SAF/AQT-SR-90-010

Controlling Unclassified Scientific and Technical Information

Walter R. Blados

1987

Published in
Information Management Review, Volume 2 Number 4, 1987, pp. 49-60.

United States Air Force
Scientific and Technical Information Program
Management of STINFO

USAF STINFO MANAGEMENT 90/5

Secretary of the Air Force
Deputy for Scientific and Technical Information (SAF/AQT)
The Pentagon
Washington, DC 20330-1000

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1987	

4. TITLE AND SUBTITLE
Controlling Unclassified Scientific and Technical Information.

5. FUNDING NUMBERS

6. AUTHOR(S)
Walter R. Blados

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Secretary of the Air Force
Deputy for Scientific and Technical Information
SAF/AQT, Room 4D289, The Pentagon
Washington, DC 20330-1000

8. PERFORMING ORGANIZATION REPORT NUMBER
USAF-STINFO-
Management-90/5

SAF/AQT-SR-90-010

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
Published in Information Management Review, Volume 2 Number 4, 1987, pp. 49-60.

Supersedes AD-A192962

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

A substantial transfer of U.S. scientific and technical information has contributed significantly to the military potential of adversary countries, and may prove detrimental to the security of the United States. The Department of Defense has established policy and procedures to prevent further undesirable transfer of production, engineering, logistical, scientific, and technical information. The intent of the new procedures is to stem the flow of military-related technical data to U.S. adveraries without stifling technological growth, blocking the exchange of technical data that is vital to progress and innovation in the U.S., or reducing the competitiveness of U.S. industry in world markets. Properly applied, the new procedures will permit technical data to flow to government agencies and private entities that have a legitimate need. Keywords: Information [illegible]

Codes	
Dist	Special
A-1	

14. SUBJECT TERMS
Technology transfer; Security; Distribution limitation, Export control; Public disclosure; Militarily critical technical data; STINFO; Management; STINFO Program management.

15. NUMBER OF PAGES
14

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Controlling unclassified scientific and technical information

Walter R. Blados

A substantial transfer of U.S. scientific and technical information and technology has contributed significantly to the military potential of adversary countries and may prove detrimental to the security of the United States. The Department of Defense has established policy and procedures to prevent further undesirable transfer of production, engineering, logistical, scientific, and technical information.

Inf Manage Review, 1987, 2(4), 49–60

Two schools of thought on the management and sharing of scientific and technical information resulting from research and development efforts within the United States exist.

One school fosters and encourages an unrestricted, full exchange of information. Georgetown University's Center for Strategic and International Studies asserts, "International competitiveness of high technology industries is essential to long-term security . . . of the United States."[1] Another representative of this philosophy states, "Freedom of information is the life blood of scientific progress. Can we afford to restrict the flow?"[2]

Proponents of this school of thought state that only unrestricted flow and complete freedom and access to information can ensure the vital cross-fertilization of scientific results among scientists and engineers, nationally and internationally. These proponents also state that a free exchange is vital to fostering open competition and is, of course, necessary if the United States is to share results with its allies.

The other school of thought fosters the protection of information by restricting access to it. Secretary of Defense Caspar Weinberger has stated, "We are subsidizing the military build-up of the Soviet Union."[3] Malcolm Baldrige, secretary of commerce, agrees, "U.S. government agencies are tolerating a massive give-away program."[4]

Proponents of this second school of thought state that the flow of information must be restricted to control critical military technology vital to U.S. technological superiority, protect national defense, and prevent technology "drafting" (following in the tailwind of U.S. technology advances).

A good case can be made for each side. However, what is needed is a middle ground, a balanced approach, a release of information by selective process.

The Department of Defense (DOD) recognizes the necessity of information exchange and has made a commitment to interchange technology and information with the public and private sectors, including

Walter R. Blados, B.A., M.P.A., *is Scientific and Technical Information Program Manager with the U.S. Department of the Air Force.*

The views expressed in this paper are the author's and do not reflect the views of the U.S. Department of the Air Force or the United States Government.

academia. This interchange is essential to the readiness of the DOD, and technologies developed for civilian applications can be applied in the military and vice versa. Hence the DOD endorses and encourages the interchange of information between the civilian and military sectors.

However, this interchange of information must be tempered by controlling militarily critical technology, protecting critical defense information from unauthorized recipients, controlling information to prevent unfair competitive advantage, and adhering to the laws and regulations protecting information.

The DOD has rigorously pursued a policy of sharing scientific and technical information and data to ensure that such information and data are used to provide maximum contribution to the advancement of science and technology not only within the DOD, but in other governmental and national research and development efforts as well. This sharing of scientific and technical data has helped eliminate undesired duplication of effort and has improved the efficiency of management activities at all levels, from policymakers and staff to scientists and engineers in field activities.

DRAIN OF CRITICAL TECHNOLOGY

Considerable evidence exists that a substantial transfer and information drain of U.S. technology has contributed significantly to the military potential of countries with interests not aligned with the U.S. or its allies and has proven detrimental to U.S. national security. Because advanced technology is so important to the nation's military capabilities, its transfer to a potential adversary can destroy U.S. military advantage.

In May 1982, the U.S. Congress was given a report identifying a massive and global Soviet program for acquiring Western militarily significant technology.[5] That report described the Soviets' successes in supplementing their military research and manufacturing capabilities and in narrowing the technology gap with the West, thereby eroding the technological superiority on which U.S. and Allied security depends.

The identification of this program led the West to undertake greater efforts in counterintelligence and export control. Since then, it has become even more evident that the magnitude of the Soviet collection effort and their ability to assimilate collected equipment and technology are far greater than was previously believed.

An update of the 1982 report defines the scope of the Soviet effort, outlines how the Soviets acquire Western technology, and identifies examples of specific technologies the Soviets seek.[6] It highlights details and statistics of Soviet successes and provides much more detail than could be revealed previously. This information was obtained from intelligence sources of the United States and Allied countries. Understanding the Soviet effort is crucial to designing ways to protect Western technology from being acquired and used against Western security interests.

The Soviets use covert as well as overt and academic-related means to obtain information.

Collection of information from professional and academic conferences on applied science and technology has contributed significantly to the success of the Soviet program. In the late 1970s, at least 35 conferences worldwide were identified in the Soviet program as potential sources of specific data that would help solve military research problems. These included conferences on materiels, missiles, engines, lasers, computers, marine technology, space, microelectronics, chemical engineering, radars, armaments, and optical communications. The Soviets judged some of the data acquired from these conferences to be most significant contributions to their military projects.

However, unclassified technical documents from all countries (including engineering analyses and research results contribute most significantly to the Soviet effort because of their value to Soviet engineers seeking creative designs and alternative engineering approaches. For example, from the mid-1970s to the early 1980s, NASA documents and NASA-funded contractor studies provided the Soviets with their most important source of unclassified material in the aerospace area. Soviet interests in NASA activities focused on virtually all aspects of the space shuttle.

However, unclassified technical documents from all countries (including engineering analyses and research results) contribute most significantly to the Soviet effort because of their value to Soviet engineers seeking creative designs and alternative engineering approaches.

Documents acquired dealt with airframe designs (including computer programs on design analysis), materiels, flight computer systems, and propulsion systems. This information allowed Soviet military industries to save years of scientific research and testing time and millions of rubles as they developed their own, very similar, space shuttle vehicle.

The individual abstracts or references in government and commercial databases are unclassified, but some of the information, taken in the aggregate, may reveal sensitive information concerning U.S. strategic capabilities and vulnerabilities. Numerous unclassified DOD and contractor documents from the Commerce Department's National Technical Information Service are sought by the Soviets and other potential adversaries. Documents dealing with design, evaluation, and testing of U.S. weapon systems are in the database.

The public and private document clearinghouses, established to efficiently index and disseminate results of government and government-sponsored, military-related technical research, are a fertile ground for collectors. In recent years, the growing use of electronic databases has provided the Soviets with an even more efficient means of identifying and procuring unclassified technical information needed by Soviet designers.

The United States must better organize and manage its scientific and technical information to protect its military, industrial, commercial, and scientific communities, keeping two objectives clearly in view:

1. the United States must seek to maintain its technological lead over the Soviets in vital design and manufacturing know-how, and
2. it should strictly control key dual-use products, including computer-aided design and manufacturing systems, large volumes of automatic test and inspection equipment, and, most important, the automatic test equipment that can alleviate acute Soviet qualitative deficiencies in the manufacturing of weapons and military equipment.

The ultimate goal should be to deny the Soviets access to Western documents, hardware, and technologies that will accelerate their military programs and simultaneously cause Western defense efforts and costs to increase. Soviet dependence on the West for technological innovation in military research and development and in modernizing Soviet production industries is broad.

The United States and many other Western governments have begun to better recognize that their military and dual-use equipment and technologies have been improving the performance capabilities and manufacturing standards of Soviet weapons. Several positive steps have already been taken by the United States, Western Europe, and Japan to deny the Soviets key items. Further necessary steps include

- increased awareness programs emphasizing the magnitude, tactics, and threat to Western security of the Soviet efforts,
- improved export control efforts and enhanced law enforcement capabilities, and
- better review in the prepublication or predistribution phases of government open publications.

Much of the DOD technology is military or space related and, as such, is critical to the U.S. defense posture and advantage. By acquiring this critical technology, potential adversaries are able to develop countermeasures to U.S. existing and anticipated defense systems at a much faster rate and lower cost than would otherwise be possible. Acquisition of this critical technology shortens the adversaries' research and development cycle and reduces the risks associated with the design of new weapons and defensive systems.

Policy and procedures for preventing access to classified information by unauthorized persons or countries have long existed. This classified information is not of immediate concern, but the vast amount of unclassified information of military value available to the public has been systematically exploited by the intelligence services of U.S. adversaries.

The DOD had established programs designed to protect and preserve technology—programs that reflect a balance between the principles of openness in government and the government's legitimate need to regulate the disclosure of certain information in the interest of national security. These programs have proved inadequate to the challenge posed by the extensive intelligence efforts of U.S. adversaries wishing to obtain military-related equipment and technology. The difficulty in achieving the objectives of these programs is attributed in part to conflicting legislative policy. For example, the Freedom of Information Act (FOIA) (Pub. L. 89-487, July 1966) did not provide for withholding unclassified technical data from requesters, including foreign nationals, even though export of the technical data would be other-

wise restricted by regulations implementing export control laws. Thus, the problem faced by the DOD was that any release of such data into the public domain was tantamount to uncontrolled foreign access. The DOD and other executive branch agencies presented to Congress the problem and the seriousness of its impact on national security at numerous hearings.

In September 1983, Congress included in Pub. L. 98-94, the Defense Authorization Act of 1984, authority for the secretary of defense to withhold from public disclosure certain scientific and technical data with military or space application. The DOD may now withhold from public disclosure export-controlled scientific and technical data requested under provisions of FOIA.

The new legislation defines scientific or technical data with military or space application as any research, development, test, evaluation, production, engineering, or logistics information such as formal reports, "blueprints, drawings, plans, instructions, computer software and documentation," and other scientific and "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."[7] However, secretary of defense authority to withhold such data does not extend to scientific or technical data authorized for export under a general, unrestricted license or exemption under regulations of the export control laws.

The new legislation does not apply to scientific, educational, or other data not directly and significantly related to design, production, or use in industrial processes. Therefore, the dissemination of information related to fundamental research, or the results thereof, that qualify for a general, unrestricted license under the provisions of the Export Administration Regulations is not affected.

DOD IMPLEMENTATION OF PUBLIC LAW 98-94

The provisions of Section 1217 of Public Law 98-94 were implemented by two DOD Directives: DOD Directive 5230.25, which sets forth policies, procedures and responsibilities for the withholding of unclassified technical data from public disclosure, and DOD Directive 5230.24, which establishes a new distribution marking system for technical documents.

The DOD directives provide immediate authority to deny FOIA requests for technical data that meet the criteria described in the legislation and implementing directives. In such cases, the third exemption of the FOIA is cited, which recognizes other statutes that specifically authorize withholding.

The DOD directives provide immediate authority to deny FOIA requests for technical data that meet the criteria described in the legislation and implementing directives.

The DOD directives provide that scientific and technical information and data may be withheld from public disclosure when the information or data meet all of the following criteria:

- are in the possession of or under the control of the DOD (data created or received by elements of the DOD or information developed and produced for the DOD under contractual arrangements or other agreements),
- have military or space application,
- may not be exported lawfully without an approval, authorization, or license under U.S. export control laws, and
- disclose critical technology.

DOD DIRECTIVE 5230.25

DOD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, issued 6 November 1984 (see Appendix), establishes a system that accommodates transfer of export-controlled DOD technical data to persons or enterprises in the United States (and under a Memorandum of Understanding, in Canada) while retaining the protection afforded by national export control laws. These data are provided under a binding agreement and, therefore, are not considered public disclosure. This system includes a process for certifying those who need access and provides procedures for obtaining the data required.

CERTIFICATION PROCEDURES AND DATA REQUESTS

The system established by DOD Directive 5230.25 and Canada's Technical Data Control Regulations (TDCRs) requires certification by persons or enter-

prises in the United States or Canada using DD Form 2345, "Export-Controlled DOD Technical Data Agreement" (Figure 1). The form is a self-certification that the applicant will use the data only in ways that will maintain the protections afforded by U.S. export-control laws.

The Defense Logistics Agency, through the Defense Logistics Services Center, has overall responsibility for administering the certification system. Companies that are certified are assigned a certification number and are eligible to receive export-controlled DOD technical data.

The DD Form 2345 is simple to complete and, when executed by both parties, constitutes an agreement between the certifying company and the DOD and Canadian government, as applicable. If a contractor violates the provisions of the agreement, the DOD may revoke the firm's certification for access to export-controlled data. A contractor who exports the data without benefit of license or authorization may be in violation of the export control laws and subject to severe criminal penalties.

As a condition of receiving export-controlled militarily critical scientific and technical data, the individual or enterprise certifies that

- The individual designated either by name or position designation who will act as custodian of the militarily critical technical data on behalf of the contractor is a U.S. or Canadian citizen or is a person admitted lawfully for permanent residence into the United States or Canada.
- The business of the designated individual is located in the United States or Canada.
- The data are needed to bid or perform on a contract with any agency of the U.S. government or the Canadian government or for other legitimate business activities in which the contractor is engaged or plans to engage.
- The contractor acknowledges all responsibilities under applicable U.S. export-control laws and regulations (including the obligation, under certain circumstances, to obtain an export license from the U.S. government prior to the release of militarily critical technical data within the United States) or applicable Canadian export control laws and regulations.
- The contractor agrees not to disseminate militarily critical technical data in a manner that would violate applicable U.S. or Canadian export-control laws and regulations.
- The contractor will not provide access to militarily critical technical data to persons other than its employees, or persons acting on its behalf, unless such access is permitted by U.S. DOD Directive 5230.25, Canada's TDCRs, or by the U.S. or Canadian government agency that provided the technical data.
- No person employed by the contractor, or acting on its behalf, who will have access to militarily critical technical data is debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian government contracts or has violated U.S. or contravened Canadian export-control laws or has had a certification revoked under the provisions of U.S. DOD Directive 5230.25 or Canada's TDCRs.
- The contractor is not itself debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian government contracts and has not violated U.S. or contravened Canadian export-control laws and has not had a certification revoked under the provisions of U.S. DOD Directive 5230.25 or Canada's TDCRs.

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 to be void, and the contractor will either submit a revised certification or surrender all militarily critical technical data obtained under the agreement to the data-controlling offices specified on the documents.

The completed DD Form 2345 must be submitted to the U.S./Canada Joint Certification Office in Battle Creek, Michigan. This office will take the following action after review of the contents of the form:

- Accept. The U.S./Canada Joint Certification Office assigns the individual or enterprise a certification number, which will identify the individual or enterprise as a "certified contractor" as defined in U.S. DOD Directive 5230.25 or in Canada's TDCRs. The acceptance is valid for a period of five years from the acceptance date unless sooner revoked under the provisions of U.S. DOD Directive 5230.25 or Canada's TDCRs.
- Return. The submission of the DD Form 2345 did not contain all information to process the certification. Submitter must review any comments provided with the returned submission and resubmit the form in accordance with the applicable instructions.

Figure 1

INSTRUCTIONS FOR COMPLETION OF DD FORM 2345

INSTRUCTIONS FOR COMPLETION OF DD FORM 2345

Privacy Act Statement

AUTHORITY: For 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 6, 1984 (32 CFR Part 250).

For Canadian individuals and enterprises: Defence Production Act.

PRINCIPLE PURPOSE: To identify individuals and enterprises eligible to receive military critical technical data.

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

DISCLOSURE: Voluntary; however, failure to provide the information may result in a denial of access to militarily 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

SPECIFIC INSTRUCTIONS

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 militarily 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 (FSCNM) 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.

   e. Show telephone number of the certifying official identified in Item 6. Include the area code.

3. Show the name, address, phone number (including area code) and title of the individual who will receive militarily 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 militarily critical technical data which 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 in 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 to be void, and the contractor will either submit a revised certification or surrender all militarily critical technical data obtained under this agreement to the data controlling offices specified on the documents.

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

   c. REJECTED. Reasons for rejection include, for example, debarment, 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.

ABBREVIATIONS

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

DD Form 2345 Reverse, APR 86

Figure 1 *continued*

MILITARILY CRITICAL TECHNICAL DATA AGREEMENT

(Please read Privacy Act Statement and Instructions on reverse before completion.)

Form Approved OMB No. 0704-0207 Expires Dec 31, 1987

1. TYPE OF SUBMISSION *(X one)* — ☐ INITIAL SUBMISSION ☐ RESUBMISSION ☐ REVISION ☐ 5-YEAR RENEWAL

2. INDIVIDUAL OR ENTERPRISE DATA *(Referred to as a "certified contractor" upon acceptance of certification by the U.S./Canada-JCO)*

a. NAME	b. ADDRESS *(Street, City, State/Province and Zip/Postal Code)*
c. NAME OF SUBSIDIARY/DIVISION	
d. FSCM/FSCNM/CAGE/DSS VENDOR CODE	e. PHONE NO.

3. DATA CUSTODIAN

a. NAME OR POSITION DESIGNATION *(See Instructions)*	b. ADDRESS *(Street, City, State/Province and Zip/Postal Code)*
c. PHONE NO.	
d. TITLE	

4. DESCRIPTION OF RELEVANT BUSINESS ACTIVITY

5. AS A CONDITION OF RECEIVING MILITARILY CRITICAL TECHNICAL DATA, THE INDIVIDUAL OR ENTERPRISE CERTIFIES THAT:

a. (1) Citizenship/Residency Status.
The individual designated either by name or position designation in Item 3, who will act as custodian of the militarily critical technical data on behalf of the contractor, is: *(X one — (a), (b), (c), or (d))*

☐ (a) a U.S. citizen ☐ (b) a Canadian citizen
☐ or a person admitted lawfully for permanent residence into:
☐ (c) the United States ☐ (d) Canada

(2) Business Location. Business of individual listed in Item 3 is located in *(X (a) or (b))*: ☐ (a) the United States ☐ (b) Canada

b. The data are needed to bid or perform on a contract with any agency of the U.S. Government or the Canadian Government or for other legitimate business activities in which the contractor is engaged, or plans to engage.

c. It (1) acknowledges all responsibilities under applicable U.S. export control laws and regulations (including the obligation, under certain circumstances, to obtain an export license from the U.S. Government prior to the release of militarily critical technical data within the United States) or applicable Canadian export control laws and regulations, and

(2) agrees not to disseminate militarily critical technical data in a manner that would violate applicable U.S. or Canadian export control laws and regulations.

d. It will not provide access to militarily critical technical data to persons other than its employees, or persons acting on its behalf, unless such access is permitted by U.S. DoDD 5230.25, Canada's TDCR, or by the U.S. or Canadian Government agency that provided the technical data.

e. No person employed by it, or acting on its behalf, who will have access to militarily critical technical data, is debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian Government contracts or has violated U.S. or contravened Canadian export control laws or has had a certification revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR.

f. It is not itself debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian Government contracts, and has not violated U.S. or contravened Canadian export control laws, and has not had a certification revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR.

6. CONTRACTOR CERTIFICATION

I certify that the information and certifications made by me are true, complete, and accurate to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. *(For U.S. Contractor see U.S. Code, Title 18, Section 1001 and for Canadian Contractor see Section 21 of the Defence Production Act.)*

a. TYPED NAME *(Last, First, Middle Initial)*	b. TITLE	c. SIGNATURE	d. DATE SIGNED

7. CERTIFICATION ACTION *(X one)*

☐ a. CERTIFICATION ACCEPTED: This certification number, along with a statement of intended data use, must be included with each request for militarily critical technical data. NUMBER:

☐ b. RETURNED—Insufficient information:

☐ c. REJECTED—Does not meet eligibility requirements of DoDD 5230.25 or of Canada's TDCR.

8. DoD OFFICIAL		9. CANADIAN OFFICIAL	
a. TYPED NAME *(Last, First, Middle Initial)*		a. TYPED NAME *(Last, First, Middle Initial)*	
b. TITLE		b. TITLE	
c. SIGNATURE	d. DATE SIGNED	c. SIGNATURE	d. DATE SIGNED

DD Form 2345, APR 86 *Previous editions are obsolete*

- Reject. Reasons for rejection include, for example, debarment, a business activity that does not fall within the scope of U.S. DOD Directive 5230.25 or Canada's TDCRs, or failure to make all of the required certifications.

A certified contractor obtains export-controlled technical data from the DOD by submitting a request and a statement of intended use to the appropriate repository or controlling agency. Before releasing the data, the repository or controlling office determines whether the requester is a certified contractor and whether the intended use of the technical data falls within the scope of the business purpose for which the company is certified.

Export-controlled technical data released to certified contractors include a notice cautioning the recipient that export of the data without approval or license may constitute a violation of law, penalties for unlawful export range from imprisonment to substantial fines or combinations of both, and unauthorized dissemination of the data is prohibited and may result in disqualifications.

DOD DIRECTIVE 5230.24

To identify technical data covered by DOD Directive 5230.25 and to facilitate dissemination of scientific and technical data within the defense community, DOD Directive 5230.24, Distribution Statements on Technical Documents, was issued 20 November 1984. The distribution markings have two basic purposes: (1) to identify documents that contain export-controlled information whose dissemination is controlled by statute or regulation, and (2) to indicate the extent of secondary distribution that is permissible without further authorization or approval of the originator.

It is now mandatory within the DOD that all newly created technical documents, if they are likely to be disseminated outside the DOD, be marked with an "export control notice" if the document contains export-controlled data and any one of the seven distribution statement markings prescribed by DOD Directive 5230.24. The authorized distribution statements provide options ranging from unlimited distribution to no secondary distribution without specific authority of the originator. Distribution statements are not in themselves authority to withhold unclassified technical data from public disclosure. Such determinations are the responsibility of the originator and are made in accordance with the FOIA.

EXPORT-CONTROL WARNING NOTICE

The following warning notice is authorized for use on DOD technical documents. An abbreviated form may be used on documents that cannot contain the entire warning notice.

> *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.[8]

DISTRIBUTION STATEMENTS

The following distribution statements and notices are authorized for use on DOD technical documents.[9]

Distribution statement A

> Approved for public release; distribution is unlimited.

This statement may be used only on unclassified technical documents that have been cleared for public release by competent authority.

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.

Technical documents resulting from contracted fundamental research efforts will normally be assigned distribution statement A, except for those rare and exceptional circumstances where a high likelihood exists 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.

This statement may not be used on technical documents that formerly were classified unless such documents are cleared for public release.

This statement shall not be used on classified technical documents or documents containing export-controlled technical data.

Distribution statement B

> Distribution authorized to U.S. government agencies only (reason) (date of determination). Other requests for this document shall be referred to (insert controlling DOD office).

This statement will be used on unclassified and classified technical documents.

Distribution statement C

Distribution authorized to U.S. government agencies and their contractors (reason) (date of determination). Other requests for this document shall be referred to (controlling DOD office).

Distribution statement C will be used on unclassified and classified technical documents.

Distribution statement D

Distribution authorized to the DOD and U.S. DOD contractors only (reason) (date of determination). Other requests shall be referred to (controlling DOD office).

Distribution statement D will be used on unclassified and classified technical documents.

Distribution statement E

Distribution authorized to DOD components only (reason) (date of determination). Other requests shall be referred to (controlling DOD office).

Distribution statement E will be used on unclassified and classified technical documents.

Distribution statement F

Further dissemination only as directed by (controlling DOD office) (date of determination) or higher DOD authority.

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

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 DOD Directive 5230.25 (date of determination). Controlling DOD office is (insert).

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 export-controlled technical data.

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

Reasons for assigning distribution statements include

- Foreign government information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information.
- Proprietary information: To protect information not owned by the U.S. government and protected by a contractor's "limited rights" statement.
- 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.
- 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 patentable 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.
- Specific authority: To protect information not specifically included in the above reasons and discussions but that requires protection in accordance with valid documented authority such as executive orders, classification guidelines, DOD or DOD component regulatory documents.
- 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 U.S. military advantage.

• • •

The intent of the new procedures is to stem the flow of military-related technical data to U.S. adversaries without stifling technological growth, blocking the exchange of technical data that is vital to progress and innovation in the United States, or reducing the competitiveness of U.S. industry in world markets. Properly applied, the new procedures will keep critical technology from U.S. adversaries and permit technical data to flow to government agencies and private entities that have a legitimate need.

REFERENCES

1. *Securing Technological Advantage: Balancing Export Controls and Innovation*. Washington, D.C.: Center for Strategic and International Studies, Georgetown University, 1985.
2. Chalk, R. "Continuing Debate Over Science and Secrecy." *Bulletin of the Atomic Scientists* (March 1986).
3. Weinberger, C. Statement read at press conference, 18 September 1985.
4. Baldrige, M. Letter to Secretaries of State, Defense, Energy; Assistant to the President for National Secretary Affairs; and Administrator, National Aeronautics and Space Administration, 16 January 1985.
5. U.S. Congress. Senate. Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, *Soviet Acquisition of Western Technology*, April 1982. Exhibit number 1. 97th Cong., 2d sess., 1982.
6. *Soviet Acquisition of Militarily Significant Western Technology: An Update*. Released by the Secretary of Defense, September 1985.
7. 10 U.S.C. §140c(b)(2).
8. U.S. Department of Defense. Directive Number 5230.25, 6 November 1984.
9. U.S. Department of Defense. Directive Number 5230.24, 20 November 1984.

Appendix

DEPARTMENT OF DEFENSE DIRECTIVE

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 1

A. PURPOSE

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

B. APPLICABILITY AND SCOPE

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 which 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. This Directive:

a. 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 (hereinafter referred to collectively as "DoD Components").

b. 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)).

c. 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 C.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.

d. 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 3) or for general exemptions under subsection 125.11 of the ITAR (reference (g)) (see enclosure 4).

e. 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 (h)) or which are authorized to be withheld from public disclosure under 5 U.S.C. 552(b)(4) (reference (i)).

f. 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.

g. Does not apply to classified technical data. After declassification, however, dissemination of such data that are within the scope of subsection B.1., above, is governed by this Directive.

C. DEFINITIONS

1. Except for the definition in subsection C.2., terms used in this Directive are defined in enclosure 2.

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:

a. 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.

b. 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 subsec-

tion E.4.b., above, are related properly to such business purpose.

c. 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.

d. The U.S. contractor also agrees that, unless dissemination is permitted by subsection E.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.

e. 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.

f. 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 C.2.e. and f., above, cannot be made truthfully, the U.S. contractor may request the certification be accepted based on its description of extenuating circumstances.

D. POLICY

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 3 and 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.

3. Notwithstanding the authority provided in subsection D.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. 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.

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.

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)).

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)).

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.

---

[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.