

---

## TECHNOLOGY TRANSFER: SAFEGUARDING TECHNICAL DATA

By

DONALD P. OULTON

and

JAMES C. SAVAGE, III

### INTRODUCTION

More than 40 groups and organizations in the Federal Government are involved in controlling sensitive technology. Some congressmen feel that the defense budget is unnecessarily high because technology is transferred to the Soviet Union and the United States must constantly push the state-of-the-art to maintain its advantage. Many congressmen believe that the defense budget could even be significantly reduced over the next several years while enhancing our national security if US Government agencies were set up to control the export of such technology.[1]

### DOD's TECHNOLOGY TRANSFER PROGRAM

Secretary of Defense Casper Weinberger recently reported to Congress, "In its first thousand days, the Reagan Administration has reversed the tide of a decade of neglect and naivete and has made technology transfer control a key element of national security policy." The Defense Department's technology transfer control program is described in its reports to Congress, The Technology Transfer Control Program. [2] The Secretary of Defense is directed by 10 USC 138 to send to Congress an annual report [3] recommending the amount of money to be appropriated for functions relating to the formulation and execution of Department of Defense (DOD) policies on technology transfer.

During fiscal year (FY) 1985, DOD will use 184 full-time persons and will spend \$13.843 million on technology transfer activities. Employees at the Office of the Undersecretary of Defense are divided between the Office of Policy (49 positions) and Office of Research and Development (32 positions).

---

Editor's Note: This article was adapted from a paper presented by the authors to the "Symposium on the Transfer of Technology in the International Marketplace," at Boston Park Plaza Hotel on 29-30 March 1984. The Symposium was sponsored by the Federal Bar Association with the co-sponsorship of six other professional organizations. The paper was also presented at the Annual Air Force Systems Command International Programs Conference in Seattle, Washington on 8-10 May 1984. The opinions reflected in this paper are those of the authors and do not necessarily reflect the views of the Air Force's Judge Advocate General Department or any other governmental agency.

The balance of personnel are allocated to Navy (43), Army (25), and Air Force (37). While only \$182,000 and five positions were initially allocated for the Air Force, the Air Force Technology Transfer Program is being upgraded in FY 1985.[4]

General Charles A. Gabriel, Chief of Staff, US Air Force, in an address to the 1982 Air Force Association's National Convention, stated:

While we continue to rely heavily on our people, tactics, and training to offset Soviet advantages, I am increasingly concerned about the other driving element -- technology. Since the early days of air power, technological advances have been our ace in the hole. We have to stay on the frontier of technology and protect our advantages in equipment. We can't afford to let our critical technological advantages slip away or be stolen away into the armaments industries of the Soviet Union and its allies. The leakage of Western technology, through legal and illegal means, has helped the Soviets close the gap. . . . We have to do a better job of protecting the technologies and "know-how" we need to deter Soviet aggression. We cannot allow our combat capabilities to be threatened by Western technology in Soviet hands.[5]

One of the United States' greatest strengths, freedom of speech and press, paradoxically appears to be one of its greatest weaknesses. This is so since we provide our adversaries with information which may be employed to defeat these freedoms. To really understand the problem of technology transfer, it is important to note that if the United States denies US-produced information, our adversaries often obtain the same information through our allies.

An example of our denial/allied irony described above has been cited by Senator Paul E. Tsongas (D-Mass.). The Ethiopian national airline desired to purchase a Boeing 767 which had a sophisticated ring-laser gyroscope; however, the US Government (USG) did not want the gyroscope to fall into the Soviet Union's hands and refused to authorize the sale of the Boeing 767. The French instead were willing to sell their Air-Bus to the Ethiopians. Unknown to the USG's original objecting agency, the American manufacturer of the gyroscope had already sold the gyroscope for incorporation into the French Air-Bus. Because of incidents like this one, Senator Tsongas points out in effect that we sometimes lose the technology and we also lose a substantial international sale.[6]

Dr. Miles Costick, a DOD consultant and President of the Institute on Strategic Trade, a Washington DC nonprofit corporation, believes that it is still easy, although becoming more difficult, for the Soviet Union to obtain American high technology. According to Costick, approximately 80% of the Soviet Union's total effort involves economic espionage, both scientific and industrial. Dr. Costick believes that a Presidential order should be issued requiring close cooperation among all USG departments and agencies which have anything to do with intelligence and counterintelligence. He believes their work should be divided into categories of "analysis" and "anticipation" under an Office of Strategic Trade, as proposed by US Senator Jake Garn (R-UT). This office would rely on the State Department, Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), and the US Customs Ser-

vice for support. The new office would also conduct international negotiations which would curb technology transfers to the Soviets.[7]

The CIA's study "Soviet Acquisition of Western Technology" (April 1983) states that Soviet intelligence organizations:

. . . have been so successful at acquiring Western technology that the manpower levels they allocate to this effort have advanced . . . to the point where there are now several thousand collection officers at work . . . under various covers ranging from diplomats to journalists to trade officials . . . throughout the world.

Pentagon specialists have reported that early knowledge of US strategic research allows the Russians to develop countermeasures even before a US weapons system is operational. Obviously this is a major military advantage for the Soviet Union from a "cost" and "time" standpoint. A recent Parade magazine article reports that the Pentagon is convinced that, over the years, Moscow has obtained the ability to satisfy 50% of its strategic requirements by clandestine means.[8]

#### BOSTON PRESS

Boston newspapers often contain stories about Soviet spies bent on stealing high-technology and defense secrets. The Sunday Boston Herald, last year ran a series of articles on this matter.[9] Lauren MacCarthy, author of the series, reported that eight known Soviet spies posing as technical journalists, academicians, and businessmen had been approaching defense employees in Greater Boston's high-tech Mecca. The author indicates that the spies are drawn by the area's multi-billion-dollar defense industry.

Russ Gelbspan of the Boston Globe authored an extensive survey of this problem in a series of three articles: (1) "US Tightening Access to Information," January 22, 1984; (2) "Suppressing Scientific Papers," January 23, 1984; and (3) "Restrictions on the Freedom of Information Act," January 24, 1984. As in Boston, technology transfer is one of the hottest subjects in the press all over the United States.[10]

#### A BOSTON CASE

Boston courts have been well aware of local espionage activities related to US technology developments. In early 1982, US Customs officers seized several shipments of semiconductor manufacturing equipment and computer terminals plus related high-technology equipment at Logan Airport in Boston. The action capped a lengthy investigation that halted the export of extremely sophisticated equipment in violation of Commerce Department laws.

On February 18, 1982, the Massachusetts District Court grand jury returned a 30-count indictment charging a British citizen and a resident of Massachusetts with shipping US-made technological equipment to Poland, Romania, and Bulgaria in violation of the Export Administration Act. Among other things, the two were charged with illegally shipping approximately \$500,000 worth of equipment (including a Fairchild Sentry VII integrated

circuit tester valued at \$300,000) and using their respective companies as fronts to complete illegal transactions. In addition, one was also charged with falsifying statements to the US Customs Service to avoid Commerce Department licensing requirements.

On March 25, 1983 it was held by Judge Zobel of the US District Court for the District of Massachusetts, that the Export Administration Act requires that export controls be imposed only on goods and technology that would make a "significant contribution" to the military potential of any other countries or combination of countries.

In denying a motion to dismiss indictments charging the parties with violations of the Export Administration Act, the Massachusetts Federal District Court found that the Secretary of Commerce properly decided that the specific technological items involved in the case could make such a "significant contribution" when they were placed on the Commodity Control List. Moreover, the court decided the grant of authority to the Executive Branch to make such determinations was not an improper delegation of legislative power.[11]

Interesting to note, according to the Assistant US Attorney Joan Stanley, the British citizen fled US jurisdiction and is now being prosecuted in England. He was indicted in England in early September 1983 with several charges identical to those in the US case. The American pled guilty and was sentenced.

#### POLICY, REGULATIONS, AND LAW

Policy, regulation, and law are frequently changing for technology transfers. In fact, since it appears that technology is changing faster than its control mechanisms, it has been difficult to obtain a consensus between the government and its industrial suppliers.

There are many laws which control technical data. An excellent analysis of these laws has been presented by Mr. Americo R. Cinquergrana.[12] Based on these laws, embargoes of US technology are attempted in a world where "high technology is spreading . . . like an oil slick." [13]

Congress, in the fiscal year 1984 Defense Authorization Act, added a new statute at 10 USC §140c that permits the Secretary of Defense to:

. . . withhold from public disclosure 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 be exported lawfully outside the United States without an approval, authorization, or license under the Export Administration Act of 1979 . . . or the Arms Export Control Act . . . [14]

Implementing regulations for this statute have been drafted and are presently out for public comment.[15]

## HOW TECHNOLOGY CAN BE TRANSFERRED

In our view, export of unclassified technical data can occur under a number of rather broad circumstances. These could even include oral discussions with reporters or private citizens which result in publications that ultimately may be exported outside the United States. These publications might also be read by foreign nationals within the United States; or read by US citizens who relay the information to those not authorized to receive such information.

## INTERNATIONAL TRAFFIC IN ARMS REGULATION (ITAR) PENALTIES

It is important to note that violations of ITAR, which implements the controls of the Arms Export Control Act, can give rise to criminal and civil liability. This may result in fines, imprisonment, debarment of contractors (permanent or temporary), etc. A potential of as much as two years imprisonment and a fine of up to \$100,000 can be levied on those convicted.[16]

## DOD DIRECTIVES

Secretary of Defense Casper W. Weinberger has recently issued interim technology transfer policy to all DOD components. This guidance updates the procedures for marking and disseminating documents containing technical data and information.[17] In his memorandum on this topic Mr. Weinberger indicates that his objective is to establish a system of technology transfer controls in DOD and the defense industry which will minimize the impact of control on scientific innovation and the capability of the defense industry to compete successfully in domestic/international markets. He believes that "undesirable transfers" of US technology to the Soviet Union, through a variety of mechanisms, have "contributed greatly to the Soviet military capability, saved them millions of dollars in research and development costs, and helped them to develop countermeasures to US weapon systems."

The Air Force has designated the office of the Vice Chief of Staff for International Programs (AF/CVAIP) and has further delegated AFSC/DLXI as the point of contact[18] to assess proposed transfer cases to assure compliance with coordinated DOD policy positions. This point of contact (POC) also assists in helping to identify and assess "critical technology," and supports DOD in reviewing export control lists. That office also participates in DOD technology transfer panels and subpanels. Furthermore, the POC participates in the development and negotiation of international agreements pertaining to technology, goods, services, and munitions transfers.[19]

Transfers of technology, goods, services, and munitions are considered by the Air Force on a case-by-case basis. This process involves policy reviews, technical evaluations, operational military impact assessments, and intelligence assessments of proposed transfers. Transfers must be consistent with the US national security and foreign policy objectives. The Air Force and all other DOD components must carefully scrutinize transfers to multinational organizations in which potential adversaries participate. Recipient nations are restricted from further transferring technology unless written release is obtained from the cognizant government agency. The total effect of

contemplated transfers on US security is required to be assessed. Numerous other requirements are examined in strategic trade and munition licensing cases. DOD has a technology transfer public awareness program which is designed to inform government agencies, Congress, industry, academia, and the general public as to the danger of the loss of western technology leadership.[20]

Definitions of key words (e.g., critical technology, items of intrinsic military utility, keystone equipment, know-how, munitions, services, strategic trade cases, technical data, technology, and means of transfer mechanisms) are set forth at Enclosure 3 to DOD Directive 2040.2.[21] Technical data is defined, for example,

. . . as classified or unclassified information of any kind that can be used, or adapted for use, in the design production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of goods or munitions; or any technology that advances the state-of-the-art or establishes a new part in an area of significant military applicability in the United States. The data may be tangible, much as a model, prototype, blueprint, or an operating manual, or may be intangible, such as a technical service or oral or visual interactions.[22]

#### AIR FORCE REGULATION

The military services immediately began implementing Mr. Weinberger's guidance. The Air Force issued its formal regulation on 16 November 1983[23] which assigned responsibilities for identifying and assessing "military critical technologies" (MCT). The regulation advised Air Force offices as to the control of the transfer of technologies to foreign countries. Management of the Militarily Critical Technology Program (MCTP) was delegated to the Air Force Systems Command (AFSC). Appendix 1 [at the end of this article] identifies regulatory policy documents which government and contractor personnel must consult in these matters.

These regulations list methods of transferring technology to foreign countries as follows:

- a. Sales and grants of end products, technical data, and services incident to US Government foreign military sales and commercial transactions with foreign countries.
- b. Visits by foreign nationals to US Government facilities and contractors.
- c. Visits by US Government personnel and contractors to foreign countries.
- d. Release of government or contractor produced documents (directly to foreign countries or indirectly through unlimited release to the public).
- e. Filing patents.
- f. Government-to-government agreements.

- g. Codevelopment and coproduction agreements, whether government-to-government or commercially licensed.
- h. Exchange programs.
- i. Unauthorized diversions to a third country.
- j. Direct acquisition by theft or espionage.
- k. Exploitation of captured military hardware.[24]

#### UNCLASSIFIED TECHNOLOGY

Eugene B. Skolnikoff, Director of the Center for International Studies at the Massachusetts Institute of Technology, writes, "The difficulty in controlling technology transfers is that so many unclassified technologies, if not all, are 'dual use,' that is, applicable to civilian and military use. It is those dual-use technologies that pose the contentious transfer of technology issues." [25]

Dr. Skolnikoff provided examples of the typical routes and modes of transfer of technology (direct or via a third country), as follows:

. . . licenses, sales of technology, turn-key plants, hardware sales, joint ventures, contract bids, patents, publications, textbooks, sales brochures, visits, conferences, symposia, training and education, public policy debates, loose talk, immigration, espionage, capture of weapons, and electronic communications intelligence.[26]

Measures for embargoing or controlling technology export, writes Dr. Skolnikoff, are "obviously at best difficult and perhaps impossible given the many ways by which [technology is] transferred."

Ten "typical" control measures were listed by Dr. Skolnikoff as useful with various levels of effectiveness as follows:

1. Controlling of technology sales, bids.
2. Agreement on and implementation of controls by alternative suppliers.
3. Control of overseas subsidiaries, partners.
4. Control of end use of technologies sold for civilian applications.
5. Prior review of publications.
6. Control of access by visitors to laboratories, factories, application sites.
7. Control of students and visiting faculty from abroad.
8. Control of professional visits abroad by US engineers, scientists.
9. Limitations on seminars, symposia, congressional debates.
10. Stringent counterespionage measures.

Dr. Skolnikoff commented that many of the above measures "are, and have been, in effect for many years with regard to some technologies, others have only recently become relevant. . . . "[27]

LCDR Richard A. Guida, USNR, in the January 1984 issue of the US Naval Institute's Proceedings magazine, comments that the Soviet Union is out to "beg, borrow, buy, or burgle" Western military technology, and the United States is doing little to prevent it. Guida, addressing the complex problem of technology control arising from unclassified information, contends that some unclassified information with military value has not been classified because: (1) it does not meet the strict test for classified material; (2) it is in the civilian realm and virtually impossible to control; or (3) control would tremendously increase the cost to design, build and maintain military equipment. Guida further believes that while no single approach is perfect, a reasonable compromise would (and we agree should) include these principal elements:

. . . Carefully defining and limiting the categories of unclassified information which have true military value warranting protection. . .

. . .

Establishing requirements for control of the information which are commensurate with its value. . . .

Convincing the parties who are directly involved (Congress and defense contractors) that control of the information is both necessary and achievable without significant disruption. . . .

Applying the carefully crafted categories of military sensitive technology to contractors on a case-by-case, contractor-by-contractor basis. . . . Each contractor's work should be reviewed in detail, and militarily sensitive unclassified information should be delineated. From this review, contractual requirements specifying this information and requirements for its protection can be tailored to each contractor. . . . [28]

## CONTRACT CLAUSES

While access to classified contracts is governed by a DD Form 254 and the Industrial Security Manual, until Secretary Weinberger's recent policy promulgation, no such controls existed for "distribution - limited data" resulting from unclassified contracts. This will be covered in the currently pending DOD Directive 5200.20 cited previously in Footnote 17.

In unclassified programs identified by the program manager as requiring access to sensitive or militarily critical sensitive data, the contracting officer will include certain contract clauses set forth below to assure that foreign nationals are properly cleared before a contractor assigns them to work on research and development efforts. Program managers are required to coordinate with their local critical technology focal point and foreign disclosure officer(s).

The clauses required by the Electronic Systems Division (ESD) of the Air Force Systems Command (AFSC) are as follows:[29]

a. L.62 - FOREIGN NATIONALS [for solicitations]

This is notice to the offeror that the contract which may result from this solicitation will contain and the offeror shall comply with the requirements of Clause H.79 entitled Foreign Nationals . . .

b. H.79 - FOREIGN NATIONALS [for contracts]

(a) The parties acknowledge that technical data generated under this contract may be subject to export control, including disclosure to foreign nationals, whether such data is provided orally or in written form. The contractor agrees to obtain written approval from the Procuring Contracting Officer (PCO) before assigning any foreign national to perform work under the contract or before granting foreign nationals access to data related to the following items/subject matter, whether such data is provided by the Government or generated under this contract:

(Buyer to identify items/subject matter here)

(b) For purposes of this clause, foreign nationals are all persons not citizens of, not nationals of, nor immigrant aliens to, the United States.

Nothing in this clause is intended to waive any requirement imposed by any other US Government agency with respect to employment of foreign nationals or export control.

ESD also requires use of a "Release of Information" clause as follows:[30]

A-10 RELEASE OF INFORMATION

a. It is Air Force policy to encourage publication of scientific and technological advances and information developed under its contracts. One copy of each paper planned for publication will be submitted for review and comment to the Public Affairs Office, Hq ESD (PAM), Hanscom AFB MA 01731 at least 30 days prior to submission for publication.

b. News releases and media contacts, including photographs and films, public announcements, or other forms of publicity concerning the technical content of this contract, will not be made without prior clearance from the Air Force. Requests for publicity approval should be addressed to Hq ESD (PAM), Hanscom AFB MA 01731, for the approval of the contracting officer. (DAR 1-329; AFOSR/CC Ltr, 82 Nov 17; USDR&E Memos, 82 Oct 12, 82 Sep 12, and 82 May 31)

Block 13 of the "Contract Security Classification Specification" (DD Form 254) requires that proposed public release of technical data be submitted through the local Air Force Public Affairs Office to the Directorate for Freedom of Information and Security Review in accordance with paragraph 5.0 of the Industrial Security Manual. Contractors have been cited after investigation by the Defense Investigative Service (DIS) for releasing unclassified data in violation of this contract clause for breach of contract. At ESD, minor violations have resulted in letters of admonishment to contractors, and in one case, a copy was placed in a contractor's "Past Performance" file. This file is used for evaluation purposes in awarding future contracts. Additionally, more serious breaches of contract not specifically within the scope of express statutory proscriptions can be resolved by the government through its common law contract remedies.

### SECURITY ASSISTANCE PROBLEMS

The government faces many of the same technology transfer problems summarized above in its security assistance programs with foreign governments and international organizations. Many transactions contain "hidden" security assistance problems which have the potential for conflict with US laws and regulations. According to LCDR Thomas L. Martin of the US Navy's Judge Advocate General's International Law Division,[31] many technology transfer problems are not immediately recognized in programs involving foreign personnel training in the United States. These transfer problems occur in numerous (sometimes subtle) ways. For example, personnel are exchanged between countries; the United States hosts liaison and loan personnel; courtesy visits are given to foreign VIPs; and US military units participate in combined forces exercises in foreign countries; and US equipment/technical data is loaned or transferred to host forces.

Commander Martin feels that ideally a "transfer problem checklist" could be created and distributed to all US DOD personnel for identification of technology transfer problems and coordination with appropriate DOD agencies. He acknowledges that not every "hidden" problem, or category of problems, can be listed. He believes, however, that lawyers have frequent opportunities to recognize problems that may not be immediately apparent to others. These opportunities arise through review of message traffic, correspondence, or legal queries not directly related to the security assistance field. Martin also believes members of the DOD legal community have the opportunity to point out potential pitfalls related to transfer of defense articles and services to their respective military organizations. We agree with LCDR Martin that for professionals in the security assistance community, the best advice is not only to provide assistance on that which is asked, but also to determine what additional relevant questions have not been asked.[32]

### ESPIONAGE

The DOD Information Security Program Regulation requires cases of espionage and deliberate compromise to be reported to various cognizant authorities.[33] The seriousness of these compromises must be promptly determined. Timely measures are required to be implemented to negate or

minimize the adverse effect of the compromise. For example, immediate government action must be taken to identify and regain custody of the compromised information whenever possible. Appropriate action is then taken to correct the cause of the compromise.

Any person who has knowledge of the actual or possible compromise of classified information is required to report immediately the circumstances to a designated responsible official who is to evaluate the circumstances and extent of damage surrounding the actual or possible compromise. The US Code's annotated chapter on espionage and censorship[34] provides a detailed description of penalties for violations of the espionage statutes. Some years ago the death sentence was permitted[35] for serious violations.[36] Legislation to reestablish the death penalty for treason and espionage is presently nearing a final US Senate vote since the Senate broke a threatened filibuster against it on a 65-26 vote on February 9, 1984. This legislation is designed to comply with Supreme Court rulings establishing constitutional standards for use of capital punishment.[37]

As an aside, it is interesting to note that loss of classified messages through gross negligence by an Air Force member resulted in his court martial where he failed to take steps to safeguard documents by leaving them in the room of a civilian friend.[38]

#### ENFORCEMENT[39]

DOD has initiated numerous efforts to tighten export controls over strategic technologies. In FY 1983, DOD provided \$30 million to the Customs Service's Operation Exodus to strengthen its enforcement efforts in technology transfer. As a result, some 400 customs agents are now assigned in over 25 cities around the world dedicated specifically to Operation Exodus. Customs agents work closely with DOD technical experts in identifying goods to be detained.

Both Customs and Department of Commerce enforcement officials encourage businessmen and other citizens to watch for suspicious activities in relation to proposed exports. Unusual packing requirements or shipping routes, for instance, could signal a potential diversion effort. Both agencies have a 24-hour hotline phone number to receive such reports:

Customs Service  
Operations Exodus  
(202) 566-9464

Department of Commerce  
Export Enforcement  
(202) 377-4608

The following list illustrates the aspects of export transactions and shipments which may alert enforcement officials and others in international trade to the possibility that specific shipments are illicit.

#### WHAT TO LOOK FOR TO SPOT SUSPICIOUS SHIPMENTS

- End-user not familiar with the commodity.
- End-user not interested in service contracts which usually accompany sale.
- Unusual delivery location.

- Freight forwarder listed as ultimate end-user.
- Unusual packaging request.
- Evasive response to questions about domestic use.
- Reluctance to provide end-user information.
- Design incompatible with:
  - Destination.
  - End-user's line of business.
  - Usual industrial requirements for stated end-use.
- End-user willingness to pay cash for large or expensive orders.
- No business background available on end-user.

#### SUMMARY[40]

The military requirements for safeguarding technical data and controlling technology transfer is authoritatively summarized in the Secretary of Defense's annual reports to Congress. The annual report stresses Secretary Weinberger's major concerns. Secretary Weinberger calls for a halt to "erosion of our technological lead." He believes that the first objective of the United States is aggressively to improve its technology by continually and expeditiously incorporating new developments into our defense programs. Secondly, he believes that the United States must reduce access by our potential adversaries to our militarily important technological and industrial achievements.

Moreover, he recognizes the need to follow through on President Reagan's initiative to reorient the Coordinating Committee for Multilateral Export Controls (COCOM), so that technology transfer controls will be coordinated through the efforts of our allies.

Further, Mr. Weinberger has directed US policy makers to recognize explicitly the danger from transfers of "dual use" technologies. Current US policy acknowledges that recent technological innovation has been so rapid that "civilian" and "military technologies" are often impossible to distinguish. The United States, however, now systematically attempts to identify and protect those technologies essential to continuing US superiority by identifying what the Export Administration Act terms "critical military technologies," as we have previously discussed.

In conclusion, we believe substantial progress is being made by government and industry to provide sound and effective information for consistent technology transfer control methods. The objective is to stop all "undesirable technology transfers." With the major technology transfer problem identified, we believe this goal is now achievable.

#### REFERENCES

1. DOD Current News Special Edition "Technology Transfer," 8 Dec 82, No. 936, p. 1, including "Defense Spending Higher because of Lost Technology," Human Events, 12 Jun 82, p. 19.
2. C. Weinberger, Secretary of DOD, The Technology Transfer Control Program, A Report to the 98th Congress, 1st Session, Feb 1983; 2nd Session, Feb 1984.

3. Required by 1983 Defense Authorization Act which amends section 138, Title 10, US Code.
4. C. Weingerger, *Ibid.*, Feb 1984 Report, p. 66.
5. General C. Gabriel, "The Leakage of Western Technology: Working Together with the Other Services," XLIX Vital Speeches of the Day, No. 1, 15 Oct 82, pp. 1, 3, and 4.
6. J. Zonderman, "Policing High-Tech Exports," The New York Times Magazine, 27 Nov 83, pp. 100-136.
7. M. Costick, "How to Stop US Technology from Building the Soviet Military," The American Sentinel, 12 Dec 83, pp. 4-6.
8. T. Szulc, "To Steal Our Secrets," Parade magazine, 7 Nov 82, pp. 3-5.
9. L. MacCarthy, "KGB Spies Hit Hub's Hi-Tech," Sunday Boston Herald, 12 Jun 83, p. 7 (Headline/Series).
10. DOD's (Air Force as Executive Agent) Current News Branch has reprinted several hundred pages of news clippings in its five "Technology Transfer Special Editions:" (1) No. 936, 8 Dec 82; (2) No. 1001, 12 May 83; (3) No. 1033, 2 Aug 83; (4) No. 1064, 18 Oct 83; and (5) No. 1101, 19 Jan 84.
11. US vs. Moller-Butcher, 560 F. Supp. 550 (D. Mass, 1983).
12. A. Cinquegrana and J. Shepherd, Department of Justice's Office of Intelligence Policy, "The Current Legal Basis for Controls on the 'Export' of Technical Information" scheduled for publication in the Spring 1984 technology transfer issue of the Boston College International and Comparative Law Review. This article provided a short analysis of: (1) the Export Administration Act of 1979 (which has been the subject of continuing revision and debate) (50 USC App. 2401, et seq, 15 CFR 368, et seq); (2) the Arms Export Control Act, (22 USC 2751, et seq, 22 CFR 125 et seq); (3) the Atomic Energy Act, (42 USC 2011 et seq, 2139); (4) the Invention Secrecy Act of 1951, (35 USC 181 et seq, 37 CFR 5.1 et seq); (5) Trading with the Enemy Act, (50 USC App. 1 et seq, 31 CFR 500.101 et seq); (6) International Emergency Economic Powers Act, (50 USC 1701 et seq).
13. W. Guzzardi Jr., "Cutting Russia's Harvest of US Technology," Fortune, 30 May 83, pp. 102-112.
14. PL 98-94, §1217(a); 10 USC 140c (1983).
15. Draft guidance has been printed as DOD Directive 5400.XX in 48 Fed. Reg. 56603 (22 Dec 83).
16. International Traffic in Arms Regulation (ITAR), 22 CFR 121-128; penalty codified at 22 USC 2278.

17. DOD Interim Policy, "Control of Unclassified Technology with Military Application" 18 Oct 83. (Currently pending final issuance as DOD Directive 5200.20, Distribution Statements on Technical Documents.)
18. The Air Force's Office of Primary Responsibility (OPR) is Mr. McMann, Hq AFSC/DLXI, Andrews AFB, DC. The OPR for the US Army is LTC Murphy (DAMI-CIT) the Pentagon, and for the US Navy is LCDR Wheeler, Office of the Chief of Naval Operations (CNO) and Ms. Cintron, OP-623, both of the Pentagon.
19. DOD Directive 2040.2, paragraph G6, "International Transfers of Technology (IT<sup>2</sup>), Goods, Services, and Munitions," 17 Jan 84.
20. Ibid., para. E.
21. Ibid., Enclosure 3.
22. See also 10 USC 104c (b2).
23. AFR 80-5, "Research and Development: Military Critical Technology Transfer," 16 Nov 83.
24. Ibid., para. 4.
25. E. Skolnikoff, "Technology Transfer and Security," II Europe/America Letter, No. 1, Oct 82, pp. 18-26, (extracted from a speech to the Chicago Council on Foreign Relations).
26. Ibid., p. 20.
27. Ibid., p. 21.
28. LCDR R. Guida, USNR, "Protecting America's Military Technology," full cite not available, US Naval Institute, Proceedings, Jan 84.
29. ESD/PKP Contracting Policy Letter, 18 Aug 83.
30. ESD DAR Sup. 2-201(a) as revised by ESD Contracting Policy Letter 84-17, 29 Nov 83.
31. LCDR T. Martin, USN, "Unauthorized Transfers of Defense Articles and Services," Defense Institute of Security Assistance Management Newsletter, Vol. 4, No. 1 (Fall 1981), pp. 46-48.
32. Ibid.
33. DOD 5200.1-R requires reports to be made in accordance with DOD Instruction 5200.22 and DOD Directive 5210.50, and the service organization's implementing regulations. See also paras. 1-307 and 6-102, AFR 205-1.
34. Sections 792-799, Chapter 37, of Title 18, US Code Annotated.
35. 18 US Code 794.

36. See for example, Rosenberg vs. US, Sup. 1953, 73 S. Ct. 1152, 346 US 273, 97 L. Ed. 1607, reconsideration denied, 73 S. Ct. 1178, 346 US 324, 97 L. Ed. 1634.
37. "Senate Nears Federal Crime Death Penalty," The Middlesex News, 30 Feb 84.
38. US vs. Gonzales, AFCMR 1981, 12 M.J. 747, which affirmed the finding of guilty for four violations of Articles 92 and 134, Uniform Code of Military Justice (UCMJ), 10 USC 892 and 934. Paragraph 6-102 of AFR 205-1 also was held to be a punitive authority.
39. C. Weinberger, Secretary of Defense, The Technology Transfer Control Program, A Report to the 98th Congress, 2nd Session, Feb 1984, pp. 55-56. This section is reprinted as presented.
40. C. Weinberger, Secretary of Defense, The Technology Transfer Control Program, A Report to the 98th Congress, 1st Session, Feb 1983.

Mr. Donald Oulton is Chief of the Foreign Military Sales (FMS) Branch, Contract Law Division, Office of the Staff Judge Advocate, Electronic Systems Division (AFSC). Mr. Oulton's FMS Branch provides legal support for over \$10 billion in international contracts. He has a B.S. in Business Management from Boston University, and in 1969 he received a Juris Doctor (JD) degree from Suffolk University Law School. Mr. Oulton has over 22 years experience in defense contracting as a contract negotiator. In 1976 he was appointed as the only fulltime FMS attorney then serving with the Air Force. Mr. Oulton is a member of the Federal Bar Association, the American Society of International Law, and is licensed to practice law before seven courts, including the Supreme Court of the United States. He received AFSC's "Outstanding Civilian Attorney of the Year Award" in 1980 and the USAF's "Wrightson Award" after being competitively selected as the "Outstanding Civilian Attorney Serving with the Judge Advocate's Department for the Year 1980." Recently, he was selected as the recipient of the Air Force's 1983 Harold Wright Award for "outstanding achievement and service in support of the Command, Control, Communications, and Intelligence (C<sup>3</sup>I) mission" of the Electronic Systems Division.

Mr. Jim Savage is an FMS government contracts attorney for the Office of the Staff Judge Advocate, Electronic Systems Division (AFSC), and a Major with the US Army Reserve Judge Advocate General's Corps. He is a member of the Tennessee, District of Columbia, and Maryland Bars and holds the following degrees: JD, Memphis State University; LLM, John Marshall Law School; LLM, Georgetown University; BS, Austin Peay State University; and an MS in Criminal Justice, Troy State University. After law school, Mr. Savage served as an Army trial counsel (prosecutor), defense counsel, and claims attorney in Germany and Georgia. He has also worked as a procurement attorney and has taught numerous legal and para-legal courses as an adjunct faculty member at various colleges/universities. Since 1979 he has served as Vice-Chairman of the International Procurement Committee of the Federal Bar Association. He is the current President of the Boston Chapter of the Federal Bar Association, President of the New England Civil Affairs Chapter and State Junior Vice-President (Army) of the Reserve Officers Association.