UIC John Marshall Journal of Information Technology & Privacy Law

Volume 7
Issue 2 *Computer/Law Journal - Fall 1986*

Article 2

Fall 1986

Operation Exodus: The United States Government's Program To Intercept Illegal Exports of High Technology, 7 Computer L.J. 203 (1986)

Bruce B. Weyhrauch

OPERATION EXODUS: THE UNITED STATES GOVERNMENT'S PROGRAM TO INTERCEPT ILLEGAL EXPORTS OF HIGH TECHNOLOGY

by BRUCE B. WEYHRAUCH*

The Soviet block countries are making great efforts to obtain high technology goods manufactured or designed in the United States. The United States is making equally great efforts to stop the flow of this

* Attorney I, Alaska, Department of Law, Juneau, Alaska. J.D. 1986, Northwestern School of Law of Lewis and Clark College; B.S. 1979, California State University, Humboldt. I wish to acknowledge the assistance of Professor Leonard Duboff, Northwestern School of Law of Lewis and Clark College; Carol Emory, Attorney with Perkins Coie of Portland, Oregon; and Mr. Harvey Steele, Import Specialist with the United States Customs Service in Portland, Oregon. The views, opinions, and all representations are solely those of the author and not those of the Alaska Department of Law, nor the United States Customs Service.

technology to Soviet block countries. A key component of the United States government's effort to halt the export of high technology is a program called Operation Exodus. Operation Exodus is overseen by the United States Customs Service, which has broad authority to stem the tide of illegal technology exports. This Article will describe Operation Exodus, its impact on the illegal export of high technology, and who it affects. The Article will also assess what high technology export companies should do to comply with export licensing to avoid civil and criminal penalties under Operation Exodus.

Section I provides background on the growth of technology in the United States military, and compares the United States' advances in technology with the Soviet Union's inferior technological position. Section II discusses the quantity and quality of technology smuggled out of the United States and Soviet methods for obtaining western technology. Section III describes existing laws to stem the illegal flow of high technology and the procedures that must be followed to export technology. Section IV details Operation Exodus, what it is, how it operates, and the program's results. The section also provides an overview of the penalties exporters may face if they violate export laws, and gives an analysis of the attempted extraterritorial applications of Operation Exodus, including salient legal challenges to United States' efforts to stop certain technology exports. Section V summarizes export protocols the practitioner and the export company should follow. Exporters cannot avoid dealing with government bureaucracies and continually changing regulations, particularly in the field of high technology. Familiarity and communication with relevant agencies is critical for the successful exporter. The Article concludes that while Operation Exodus is a strong effort by the United States to stem the illegal export of high technology to eastern block nations, accurate information on the Operation's effectiveness may not be available for several years.

I. BACKGROUND

The high technology industry is a booming business, especially in the computer and laser fields because of their military applications. High technology is projected to be the growth industry, not only in the United States, but in the rest of the developing world as well.[1] A major catalyst for this growth in the United States is the emphasis on military defense spending in the government's budget.[2] In recent years, defense

1. *See* A. TOFFLER, THE THIRD WAVE (1980).

2. *See A Cost-Effective Pentagon*, Christian Sci. Monitor, Oct. 21, 1985, at 25, col. 1. "During the first four years of the Reagan administration alone Congress appropriated $1 trillion for the Nation's defense." *Id.*

spending has been the fastest growing part of the economy.[3] For example, the total 1984-85 budget for the United States Department of Defense was approximately $247 billion, with a large portion going into three aspects of defense: salaries, weapons acquisition, and weapons modernization.[4] Recent budgets continue this trend. Modernization and acquisition mean that the Pentagon purchases appropriate technology and high technology goods to give the United States military a strategic edge over the Soviets.[5]

Most commentators agree that the United States and its NATO allies presently maintain a technological advantage over the Soviet Union and Warsaw pact countries.[6] This technological edge over the Soviets is considered essential, but it is shrinking quickly.[7] Soviet scientists and engineers cannot compete with their counterparts in the United States

---

3. Cook, *Defense Budget Boosts U.S. Economy as Civilian Sector Starts to Slow*, Christian Sci. Monitor, Oct. 17, 1985, at 7, col. 1.

4. *Reagan's Mounting Deficit*, Maclean's, Jan. 17, 1983, at 20.

5. Referring to "edges," "superiority," and "inferiority" with respect to the United States' and Soviet Union's military advantages brings one into a volatile, often rhetorical (even Kafkaesque) shell game. Negotiations over the number of warheads per side seems simplistic from a military, if not a moral, point of view. Both sides, it is argued, have "enough" nuclear arms. In fact, the Union of Concerned Scientists now estimates the relative size of the world's nuclear arsenal as large enough to have a Hiroshima-size nuclear explosion every second for two weeks. In any event, whether the U.S. or the Soviet Union would ever gain military advantage over the other for any period of time is doubtful. *See* Bok, *Distrust, Secrecy, and the Arms Race*, 95 ETHICS 712 (1985). But, technological advances have moved the entire cold war dialogue onto a new plane, where talk is not of weapon strength, throw weights, and kilotonnage, but of response-time, memory capacity, and the number of bits of microchips. *See* Lautenschlager, *Controlling Military Technology*, 95 ETHICS 692 (1985). Maintaining a technological edge over the Soviets is critical from a national security point of view. It is the purpose of this Article to describe one small aspect of the government's efforts to maintain technological superiority over the Soviet Union. Operation Exodus is that aspect.

6. *See, e.g.*, Flowe, *Export Licensing of Computer Equipment and Technology—A Practitioner's Perspective*, 10 N.C. J. INT'L L. & COM. REG. 633, 640 (1985). While the U.S. has a technological edge, it is deficient in military manpower and perhaps even firepower. *Id.* For an excellent discussion of the history of technology trade between the East and West, and for a background on the wavering and waffling U.S. policies on sharing technology (hardware and software) with the Soviets, see Note, *National Security Protection: The Critical Technologies Approach to U.S. Export Control of High-Level Technology*, 15 J. OF INT'L L. & ECON. 575 (1981). *See generally* Berman & Garson, *United States Export Controls—Past, Present and Future*, 67 COLUM. L. REV. 791 (1961). For an excellent perspective on technology transfer to the Soviet Union for the practitioner, see Armstrong, *Transferring U.S. Technology to the Soviets: Some Practical Legal Problems*, 16 INT'L LAW. 737 (1982).

7. *See, e.g., infra* text accompanying notes 11-16. *See Moles Who Burrow for Microchips*, TIME, June 17, 1985, at 25, col. 2 [hereinafter *Moles*]. The TIME article makes clear that there are always persons willing to make a profit on key technology whether that technology has military applications or not. Many technology leaks are simply a process of products finding their way to the market. Both eastern European and western Eu-

in key areas of military technology, particularly in microchips and lasers.[8] While some Soviets dispute the United States' technological superiority,[9] Mikhail Gorbachev concedes the Soviet's shortcomings in the area of high technology.[10] The Soviets have instituted a multi-pronged approach to attempt to close the military technology gap. These approaches include: (1) an intensive internal development and educational program;[11] (2) espionage within the United States;[12] (3) internal spies within the United States military;[13] (4) setting up foreign corporations to make what appear to be legitimate high technology purchases;[14] (5) theft;[15] and (6) exporting high technology goods and information out of the United States without first obtaining proper government clearances.[16]

The United States Customs Service and Operation Exodus purport to stop technology that is unlicensed or controlled by law from being exported or smuggled out of the United States. The remainder of this Article concentrates on Operation Exodus and its efficacy in deterring this type of undesirable exporting.

II. LOSS OF HIGH TECHNOLOGY GOODS FROM SMUGGLING

A. THE COST OF SOVIET ACQUISITIONS OF UNITED STATES TECHNOLOGY

Estimates of the number of high technology goods smuggled out of the United States vary. Since the late 1970's, United States intelligence experts estimate that 30,000 pieces of high technology equipment and 400,000 technical documents have been smuggled out of the United States.[17] Smuggling erodes any technological edge that the United

---

ropean merchants are willing middlemen if there is a buyer and a profit, even absent any special Soviet efforts to entice a seller, or obtain a particular product.

8. *Id.*

9. Rempel, *U.S. Deters Technology Smugglers*, L.A. Times, Apr. 15, 1985, § 1, at 3, col. 2.

10. Kempe, *Moscow's Bid to Close Its Technology Gap Will Test Gorbachev*, Wall St. J., June 6, 1985, at 1, col. 4.

11. *Id.*

12. *Moles*, *supra* note 7, at 25.

13. *See, e.g.*, the latest drama unfolding known as the "Walker family spy ring." Richey, *Walker Case Paints Rare Portrait of American Spy Family in Action*, Christian Sci. Monitor, Oct. 30, 1985, at 1, col. 3.

14. Bennett, *The Great Russian Raid on U.S. Technology*, READER'S DIG., Mar. 1984, at 57.

15. *How Soviets Steal U.S. High-Tech Secrets*, U.S. NEWS & WORLD REP., Aug. 12, 1985, at 33.

16. Rempel, *supra* note 9, § 1, at 3, col. 2.

17. *Moles*, *supra* note 7, at 25, col. 2. *See also infra* note 20 (specific examples of smuggled equipment).

States might have over the Soviet Union, and means that the Soviets do not have to spend the necessary capital for research and development of technological improvements. The Soviets can invest that money elsewhere in their admittedly stagnant economy. When the Soviet Union obtains high technology from the United States, it also means that the United States must spend more to maintain or regain a technological advantage. The Soviets save billions of dollars and years of military research and development by using stolen high technology equipment which the United States and its allies have developed to offset superior numbers of Soviet weapons.[18] This improves the military posture of the Soviets and increases defense costs to United States taxpayers as the Defense Department attempts to counter the Soviets.[19] Examples of high technology being shipped or smuggled overseas are legion.[20]

B. SOVIET METHODS OF ACQUIRING HIGH TECHNOLOGY GOODS

Since the 1930s, Soviet efforts to obtain western technology have been massive, well-planned, and well-managed.[21] In certain instances, the Soviets obtained western technology by using existing scientific or technological agreements with the West.[22] Much of the increased trade with the Soviets occurred during the period of detente in the 1970s. The impetus to this trade was the assumption that sales of technology would not only improve the United States' balance of trade but would also moderate Soviet political views.[23] Presently, the Soviets purchase

18. *How Soviets Steal U.S. High-Tech Secrets, supra* note 15, at 33.

19. *Id.*

20. For example, the Customs Service, under Operation Exodus, has seized C130 troop transport carrier aircraft parts, satellite scanners, multi-spectral electronic test equipment, a Doppler Survey System, and numerous computers and accessories with potential military application. DEP'T OF TREASURY, U.S. CUSTOMS SERVICE, OPERATION EXODUS, FACT SHEET (Dec. 1982) [hereinafter FACT SHEET]. Similarly, Customs intelligence received from other agencies indicates that this is a serious threat that is expected to increase. Investigations of attempted shipments and conspiracies reveal a broad pattern of criminal activity to export several types of technology including an advanced VAX computer valued in excess of $5 million, en route to the Soviet Union through diversion countries; a highly advanced computerized airborne spectral scanner with military potential headed for the Soviets; firearms which were stolen from the National Guard, headed for the Irish Republican Army extremists; artillery periscopes destined for Libya; and a plot to steal HARPOON anti-ship missiles and ship them to Iraq. DEP'T OF TREASURY, U.S. CUSTOMS SERVICE, OPERATION EXODUS BUSINESS ADVISORY NO. 1 (Jan. 1984).

21. CENTRAL INTELLIGENCE AGENCY, SOVIET ACQUISITION OF WESTERN TECHNOLOGY 1 (Apr., 1982) [hereinafter CIA].

22. *See* Yore, *Free Trade and National Security*, CAL. LAW, July, 1985, at 47. An often-cited example of technology trade is the Kama River truck plant in the Soviet Union. Between 1971 and 1980, the U.S. Department of Commerce issued export licenses for automotive technology and production equipment, including an IBM 370 computer. *See* Note, *supra* note 6, at 591.

23. Malley, *Technology Transfer Controls*, 23 JURIMETRICS 33, 37 (1982). *See also*

through illegal or unauthorized channels technology which is controlled by law. They also purchase legally advanced technology with military applications.[24] Before discussing how illegally exported goods are seized under Operation Exodus, a brief overview of the export process is needed.[25]

Note, *Effects of Soviet Ideology on the Legal Framework and Policy of US-USSR Trade*, 1 N.C. J. INT'L L. & COM. REG. 75 (1976). During the 1970s, President Nixon, Secretary of State, Henry Kissinger, and others in the Nixon Administration, began a policy of detente with the Soviets. Detente affected U.S.-Soviet military, cultural, and political relations. In a warming of the cold war attitudes of the 1950s and 1960s, the U.S. allowed the Soviets greater access to U.S. markets, selling them grain, technology, and other goods. Detente also allowed U.S.-Soviet military parity. Parity in military strength, it was felt, would ensure that the Soviets would not launch a first strike against the U.S. for defensive reasons, and would prevent the U.S. from launching a strike against the Soviets because the Soviets would have nuclear strength equal to that of the U.S. This equality of military strength means that if there were a nuclear war between the U.S. and the Soviets, there would be mutually assured destruction (MAD).

The policy of detente continued into the Ford and Carter Administrations. President Carter even asserted that it was time that the U.S. end its inordinate fear of the Soviet Union. It was not until the Soviet crackdown in Poland, the Soviet invasion of Afganistan, and evidence of Soviet adventurism in the Middle East, Central America, Southeast Asia, and Africa, that key policymakers in the U.S. began to reassess U.S. policies vis-a-vis the Soviets. The Western allies began seeing trucks manufactured at the Kama River truck plant, a plant using U.S. technology and equipment, enforcing martial law in Poland. Those trucks carried Soviet troops into Afganistan. The Soviets were quickly matching U.S. military technology, for example, by adding to their arsenals such weapons as stealth bombers, cruise missiles, neutron bombs, and, so-called "smart" bombs. During the 1980 Presidential campaign, candidate Reagan hit on a theme that portrayed a weak America because of a weak posture toward, and too much trust in, the Soviets. Reagan campaigned against policies that were too cozy with the Soviets and that allowed them to gain weapons superiority over the U.S., and he campaigned for a very strong defense.

When Reagan became President, new policies and programs were enacted in the area of U.S.-Soviet relations. Those included: a massive defense budget, weapons procurement, increased espionage and a greater role for the CIA, hard lines against trade with the Soviets (including a failed attempt to prevent the construction of a Trans-Siberian pipeline), and increased programs to prevent shipment of technological goods to the Soviets by tightening U.S. trade laws and policies. It is from this last point that Operation Exodus evolved.

24. Most of these legal purchases fall under the rubric of existing agreements between the United States and the Soviet Union. CIA, *supra* note 21, at 1. The law primarily responsible for controlling technology exports is the Export Administration Amendments Act of 1985, Pub. L. No. 99-64, § 1, 99 Stat. 120 (1985) (codified at 50 U.S.C. §§ 2401-2419) [hereinafter EAA Amendments]. This Act is discussed extensively in Greguras & Daunt, *Export Administration Act of 1985*, THE SCOTT REP., Aug. 1985, at 4.

25. *See* Flowe, *supra* note 6, and Greguras & Durant, *supra* note 24. *See* EAA Amendments, *supra* note 24, 99 Stat. at 120. A number of regulations deal with exporting products, especially technology, to destinations outside of the U.S. *See generally* 22 C.F.R. § 2.1 (1986), 15 C.F.R. § 400 (1986), 15 C.F.R. §§ 300-399 (1986). For another overview of all the hoops exporters must jump through and a discussion of the many specific laws Congress has enacted in this area, see Ellicott, *Trends in Export Regulation*, 38 BUS. LAW. 533 (1983).

III. UNITED STATES EXPORT LAWS AND PROCEDURES

The Export Administration Act of 1979 (EAA), as administered by the Commerce Department, controls exports of technical data and commodities, and reexports out of foreign countries of products or data with United States-origin content.[26] United States export controls under the EAA are imposed for three major reasons: to protect national security by restricting the export of militarily sensitive goods and data; to further United States foreign policy interests; and to limit the export of products in short supply in the United States.[27]

From the exporter's perspective, basic compliance with United States export regulations consists of two steps. First, a company's products must be classified according to a commodity control list to determine the type of export license that is required. This determination depends upon the nature of the product or its technical capabilities, the product's value, the country that will be the ultimate destination of the product, and the use to which the product will be put. Once these determinations are made, the second step is actually obtaining the export license. This process may involve obtaining supporting documents and assurances from the exporter's customer about the destination of the product and who the ultimate user of the equipment or data will be.[28]

The majority of goods and technical data can be exported under general licenses, such as "General Destination" ("G-DEST") licenses. Exports made with these licenses do not require individual applications, nor do they involve a specific licensing document. If technical data or high technology products do not qualify for a G-DEST license (or for another export license), then an individual validated license is required. This process requires the exporter to apply to the government for an actual export license. Most high technology exports require a validated license.

In 1979, the Secretary of Defense developed a list of "Militarily Critical Technologies" (MCT) placing emphasis upon:

> (A) arrays of design and manufacturing know-how;
> (B) keystone manufacturing, inspection, and test equipment,
> (C) goods accompanied by sophisticated operation, application, or maintenance know-how, and
> (D) keystone equipment which would reveal or give insight into the design and manufacture of a United States military system, which are not possessed by, or available in fact from sources outside the United States to, [sic] controlled countries

26. Pub. L. No. 96-72, 93 Stat. 503 (1979) (codified as amended at 50 U.S.C. §§ 2401-2420, *amended by* Pub. L. No. 99-64, 99 Stat. 120 (1985)) [hereinafter EAA].

27. 50 U.S.C. § 2401(d). (Supp. III 1985).

28. Ellicott, *supra* note 25, at 533.

> and which, if exported, would permit a significant advance in a military system of any such country.[29]

This MCT list is part of the "Commodity Control List" by which the Secretary of Commerce regulates exports.[30]

The MCT list covers a broad spectrum of "technologies that may have substantial or primarily nonmilitary applications . . . [including] computers, telecommunications, laser, and nuclear equipment."[31] After the Reagan Administration released a CIA report detailing Soviet acquisition of United States' designed and manufactured technology,[32] President Reagan announced that all high technology export license applications to the Soviet Union were suspended.[33] In 1982, the President, through executive orders, sought to limit the amount and kind of technology available to the Soviets. All information became classified if it concerned scientific or technological matters relating to national security.[34] Scientific research not clearly related to national security may not be classified, but information was classified if it "reasonably could be expected to cause damage to the national security."[35] Classification in these cases became mandatory, not discretionary, and the expectation of damage to national security did not have to be identified even if there was a reasonable doubt.[36] In addition, information could be classified even if the government did not have any proprietary interest in the research or its product.[37]

The many laws, regulations, and policies aimed at intercepting or preventing Soviet attempts to obtain high technology goods from the United States are useful only if enforced. Concurrent with the announcement of regulations designed to prevent technology exports, the Reagan Administration announced an extensive effort to control those exports. That effort is Operation Exodus.

IV. OPERATION EXODUS

In October 1982, the United States Customs Service began Opera-

29. 50 U.S.C. § 2404(d). (Supp. III 1985).

30. The most current MCT list is at 15 C.F.R. § 399.1 (1986). *Cf.* 49 Fed. Reg. 47,682 (1984) (final regulations on International Traffic in Arms Act).

31. *See* Ellicott, *supra* note 25, at 537.

32. CIA, *supra* note 21, at 1.

33. President's Statement on U.S. Measures Taken Against the Soviet Union, 17 WEEKLY COMP. PRES. DOCS. 1429, 1430 (Dec. 29, 1981).

34. Exec. Ord. No. 12,356, 47 Fed. Reg. 14,874 (1982) (national security information).

35. *Id.*, at 14,875.

36. *Id.*

37. The public's interest in disclosure is not balanced against national security needs in this case. This allows strict government control of high technology. *Cf.* Environmental Protection Agency v. Mink, 410 U.S. 73 (1973); Weissman v. Central Intelligence Agency, 565 F.2d 692 (D.C. Cir. 1977). *See generally* Ellicott, *supra* note 25, at 542.

tion Exodus in response to the Reagan Administration's mandate to stem the illegal export of strategic United States technology to the Soviet Union and Warsaw Pact countries. Operation Exodus also attempts to stop the illegal export of arms and munitions to proscribed destinations. The primary objectives of Operation Exodus are: (1) to stop the outflow of critical technology to the Soviets and to force compliance with export laws by intercepting or seizing shipments of items and data that are being exported illegally; and (2) to disrupt groups and individuals responsible for these illegal exports through arrests, prosecutions, and other legal sanctions. A secondary objective is to stem the flow of crucial merchandise to the Soviet Bloc and other embargoed nations; examples are the equipment to be used in building the Soviet gas pipeline and a water filtration system in Libya.[38]

A. How Operation Exodus Works

The Customs Service has actively intercepted arms shipments since the late eighteenth century when President Washington ordered the Customs Service to ensure the United States' neutrality in the war between England and France. The Customs Service enforces more than four hundred provisions of the law on behalf of some forty other federal agencies.

Under Operation Exodus, the Customs Service enforces the Export Administration Act,[39] administered by the Commerce Department, and the Arms Export Control Act,[40] administered by the Department of State's Office of Munitions Control. The Customs Service uses intelligence, inspection, and investigation in their operations. Customs agents, inspectors, patrol officers, and other Customs personnel, including import specialists and regulatory auditors, focus on the illegal outflow of critical technology through ports of exit throughout the United States.[41] Inspectors and patrol officers review export documentation, determine suspect cargo, and conduct export searches. Exodus agents identify those shipments that require further investigation and then make appropriate referrals. The agents also have primary responsibility for gathering intelligence and meeting with other government agencies, both domestic and foreign.

In its first year, Operation Exodus was a "reactive program," con-

38. FACT SHEET, *supra* note 20.

39. *See supra* note 24 and accompanying text.

40. Pub. L. No. 90-629, § 38, 82 Stat. 1320 (1968), *as added* Pub. L. No. 94-329, § 212(a)(1), 90 Stat. 744 (1976), *amended by* Pub. L. No. 95-92, § 20, 91 Stat. 623 (1977) (codified at 22 U.S.C. § 2778).

41. *See* FACT SHEET, *supra* note 20, at 2.

centrating on intensive export inspections.[42] At United States ports, Customs Exodus teams—composed of Customs agents, inspectors, patrol officers, and other Customs personnel—reviewed export documents, and searched cargo.[43] In its second year, Operation Exodus shifted its emphasis to anticipatory problems by developing intelligence, selective cargo examinations, and investigations.[44] Moreover, exodus investigators now seek to discover criminal conspiracies by targeting high-risk commodities and companies through covert operations.[45]

The crackdown by Customs officials under Operation Exodus has been fairly successful. As of fiscal year 1985, there have been a total of 4420 seizures representing $302 million.[46] The Operation has been responsible for 596 arrests, 799 indictments, and 359 convictions.[47] By tightening export licensing procedures and punishing violators, Defense

42. DEP'T OF TREASURY, U.S. CUSTOMS SERVICE, OPERATION EXODUS, FACT SHEET (Jan. 1984).

43. *Id.* at 2.

44. *Id.*

45. *Id.*

46. U.S. CUSTOMS SERVICE, EXODUS STATISTICS (1985) (available from U.S. Customs Service, Washington, D.C.).

47. *Id.* The complete information is as follows:

EXODUS STATISTICS

	F/Y 82	F/Y 83	F/Y 84	F/Y 85	TOTAL
Seizures (number)	765	1444	1459	752	4420
Seizures (value)	$ 55.6 M	$ 86.3 M	$ 85.6 M	$ 74.9 M	$302.4 M
Detentions	2481	3620	2391	947	9439
Seizures/Detentions	(31%)	(40%)	(61%)	(80%)	(47%)
Arrests	195	110	121	170	596
Indictments	171	63	175	390	799
Convictions	134	80	90	55	359

The Custom's Office of Investigations was the lead in seventy-five cases and participated in three additional investigations. These seventy-eight investigations have, to date, produced the following:

Totals	Corporations	Individuals
Defendants	37	187
Fines Levied	$5,287,945	$ 967,500
Civil Penalties	$ 10,000	0
Civil Forfeitures (Value)		$1,682,000
Restitutions		$12,000,000
Years Imprisonment		133 yrs.
Years Probation		174 yrs.
Charitable/Community Service		6010 hrs.
Fugitives		24
Pending Trial		61

U.S. CUSTOMS SERVICE, SUMMARY OF SIGNIFICANT EXPORT CONTROL CASES (June 1985)

Secretary Caspar Weinberger estimates that United States taxpayers have been saved "$20 billion to $50 billion in additional future defense expenditures [that] would have been needed to counter soviet technological advances . . . ."[48]

The Customs Service does not license export shipments. Rather, it enforces the law on behalf of other agencies.[49] If Customs personnel

(available from the U.S. Customs Service, Wash., D.C.). *See also Moles, supra* note 7, at 27 (discussion of Operation Exodus in the popular press).

48. *How Soviets Steal U.S. High-Tech Secrets, supra* note 15, at 38. For additional examples of high-technology equipment being intercepted by Customs, see *Russians Are "Robbing Us Blind,"* Wash. Times, May 20, 1985, at 1. *See supra* note 20 and accompanying text. *See also* Orgeron, *Inspectors and Operation Exodus*, CUSTOMS TODAY, Fall 1982, at 13.

49. In controlling imports of various commodities, the U.S. Customs Service enforces over 400 federal laws for more than 40 federal agencies. Most of these are in the area of import control. However, the Customs Service acts as agent for seven federal agencies to enforce export controls. A "controlled commodity" can be exported only under a license granted by the primary agency having jurisdiction over that commodity. Listed below are the controlled commodities and the primary agency on whose behalf Customs enforces export controls.

CONTROLLED COMMODITY	PRIMARY AGENCY
Arms, ammunition, and implements of war	State Dep't Office of Munitions
Fish and wildlife (Endangered species)	Dep't of the Interior U.S. Fish & Wildlife Service
Gas (natural) and electric energy	Federal Power Commission
Narcotics and dangerous drugs	Dep't of Justice Drug Enforcement Administration
Petroleum and petroleum products	Dep't of Energy, Economic Regulatory Administration
Tobacco seeds and plants	Dep't of Agriculture Agriculture Marketing Service
Watercraft (includes vessels of war which are controlled for State Department, Office of Munitions Control)	Dep't of Commerce Maritime Administration
High technology items including:	State Dep't Office of Munitions Control
Computers & related-equip.	
Semiconductors	
Communications, navigation, and control systems	Dep't of Commerce
Lasers and optics materials	
Nuclear physics materials	
Microbiology materials	

NOTE: These high technology items may be controlled both by the State Department's Office of Munitions Control and by the Commerce Department, depending on their specifications and characteristics.

DEP'T OF TREASURY, U.S. CUSTOMS SERVICE, FACT SHEET (Feb. 1983).

discover commodities lacking the required export license, they notify the exporter, or the exporter's agent, and temporarily detain the shipment while the licensing agency is notified through the Exodus Command Center in Washington, D.C. The Customs Service's detention/referral procedure usually takes less than one day.[50] Licensing determinations by the Department of Commerce average twenty-two days, while those by the State Department's Office of Munitions Control average nineteen days.[51]

To minimize delays to legitimate exports, the Customs Service developed a procedure that permits the release of detained merchandise under a surety system. The procedure only applies to goods awaiting license determinations by the Commerce Department. If the situation meets certain criteria, Customs may permit an exporter to post a surety bond, letter of credit, or cash deposit. This is to ensure that funds are available if the Commerce Department denies the license and subsequently levies a penalty against the exporter. The exporter then signs a statement attesting that the commodity is not subject to the requirement for a validated license under Commerce regulations.[52]

When a shipment is seized, the Customs Service sends the exporter a Notice of Seizure telling the exporter which Customs Office will handle the case. The Fines, Penalties, and Forfeiture Officer then confers with the licensing agency to determine if a bond should be set to release the goods. Before the Customs Service will release the shipment, the exporter must post the required bond (typically ten percent of the export value of the shipment) and submit a valid license.[53]

B. PENALTIES FOR EXPORT VIOLATIONS

If a license is denied by either the Department of Commerce (DOC) or the State Department, the Customs Service cannot release the shipment. In this event, the Customs Service begins a fine, penalty, or forfeiture proceeding as it would for a violation of a Customs law.[54] The exporter may file a petition with the Customs Service for mitigation of a penalty or remission of the merchandise. Civil penalties, other than forfeiture, are assessed only by the licensing agency (DOC), not the Customs Service.[55] When an export shipment is seized, the Exodus

50. DEP'T OF TREASURY, U.S. CUSTOMS SERVICE, BUSINESS ADVISORY NO. 1 ON OPERATION EXODUS (Jan. 1984).

51. *Id.* at 3.

52. *Id.*

53. DEP'T OF TREASURY, U.S. CUSTOMS SERVICE, BUSINESS ADVISORY NO. 2 ON OPERATIONS EXODUS (Jan. 1984) [hereinafter ADVISORY 2].

54. *See id.* The procedures are detailed in 19 C.F.R. pt. 171 (1986). *See* 22 U.S.C. § 401 (1984).

55. 19 C.F.R. pt. 171.

team's final step is to notify the Office of Investigations in Customs headquarters. The Customs Service investigates those exporters it believes may be intentionally violating provisions of export control statutes.[56]

Non-compliance with export laws, or even attempting or conspiring to violate export laws or regulations, subjects the violator to harsh penalties. Penalties range from fines to imprisonment.[57] An exporter may

---

56. ADVISORY 2, *supra* note 53, at 1. Congress, in its most recent amendment of the EAA, gave specific, strong authority to the U.S. Customs Service to rout out high technology export violators and to enforce its provisions. The new law provides in part:

> (1) To the extent necessary or appropriate to [enforce] this Act . . . any department or agency exercising any function thereunder (and officers or employees of such department or agency specifically designated by the head thereof) may make such investigations [inside or outside the United States] and obtain such information from, require such reports or the keeping of such records by, make such inspection of the books, records, and other writings, premises, or property of, and take the sworn testimony of, any person. . . .
> The Secretary and [others so designated] . . . may conduct, outside the United States, pre-license investigations and post-shipment verifications of items licensed for export, and [enforcement] investigations . . .
>
> (2)(A) the United States Customs Service is authorized, in the enforcement of this Act, to search, detain (after search), and seize goods or technology at those ports of entry or exit from the United States where officers of the Customs Service are authorized by law to conduct such searches, detentions, and seizures, and at those places outside the United States where the Customs Service, pursuant to agreements or other arrangements with other countries, is authorized to perform enforcement activities.
> (B) An officer of the United States Customs Service may do the following in carrying out enforcement authority under this Act:
>
> (i) Stop, search, and examine a vehicle, vessel, aircraft, or person on which or whom such officer has reasonable cause to suspect there are any goods or technology that has been, is being, or is about to be exported from the United States in violation of this Act.
>
> (ii) Search any package or container in which such officer has reasonable cause to suspect there are any goods or technology that has been, is being, or is about to be exported from the United States in violation of this Act.
>
> (iii) Detain (after search) or seize and secure for trial any goods or technology on or about such vehicle, vessel, aircraft, or person, or in such package or container, if such officer has probable cause to believe the goods or technology has been, is being, or is about to be exported from the United States in violation of this Act.
>
> (iv) Make arrests without warrant for any violation of this Act committed in his or her presence or view or if the officer has probable cause to believe that the person to be arrested has committed or is committing such a violation.

Pub. L. No. 96-72, § 12, 93 Stat. 530 (1979), *amended by* Pub. L. No. 99-64, § 113, 99 Stat. 148, 149 (1985) (codified at 50 U.S.C. app. 2411(a)). Thus, the Customs Service is given authority to check on shipments of high technology goods, both inside and outside the U.S., and may make such checks before, during, and after the sale of the goods to make sure high technology goods do not fall into Soviet hands.

57. *See* 50 U.S.C. § 2410 (1982), *as amended by* Pub. L. No. 99-64, § 112, 99 Stat. 146 (1985)). The new law adds "attempt" to violation provisions. Section 2410, provides in part:

> whoever knowingly violates or conspires to or attempts to violate any provision

also be denied export privileges. For high technology corporations dependent on export sales, this last penalty could mean bankruptcy as well as lawsuits for breach of contract. Even if harsh penalties are not imposed, detentions, delays, or seizures of products may result in additional costs to the exporter, bad publicity, or severed business relationships with overseas customers, and distributors.

---

of this Act or any regulation, order, or license issued thereunder shall be fined not more than five times the value of the exports involved or $50,000, whichever is greater, or imprisoned not more than 5 years, or both.

(1) Whoever willfully violates or conspires to or attempts to violate any provision of this Act or any regulation, order, or license issued thereunder, with knowledge that the exports involved will be used for the benefit of, or that the destination or intended destination of the goods or technology involved is, any controlled country to which exports are controlled for national security or foreign policy purposes, shall be fined not more than five times the value of the exports involved or $100,000, whichever is greater, or imprisoned not more than 10 years, or both.

(2) Any person who is issued a validated license under this Act for the export of any good or technology to a controlled country and who, with knowledge that such a good or technology is being used by such controlled country for military or intelligence gathering purposes contrary to the conditions under which the license was issued, willfully fails to report such use to the Secretary of Defense, shall be fined not more than five times the value of the exports involved or $100,000, whichever is greater, or imprisoned for not more than 5 years, or both.

(3) Any person who possesses any goods or technology—

(A) with the intent to export such goods or technology in violation of an export control imposed under this Act or

(B) knowing or having reason to believe the goods or technology would be so exported, shall . . . be subject to the penalties set forth . . . this subsection. . . .

(4) Any person who takes any action with the intent to evade the provisions of this Act or any regulation, order, or license issued under this Act shall be subject to the penalties set forth [here].

(5) Nothing in this subsection or subsection (a) shall limit the power of the Secretary to define by regulations violations under this Act.

(1) The Secretary . . . may impose a civil penalty not to exceed $10,000 for each violation of this Act. . . .

(2)(A) The authority under this Act to suspend or revoke the authority of any United States person to export goods or technology may be used. . . .

(a) Any person who is convicted under subsection (a) or (b) shall, in addition to any other penalty, forfeit to the United States —

(A) any of that person's interest in, security of, claim against, or property or contractual rights of any kind in the goods or tangible items that were the subject of the violation;

(B) any of that person's interest in, security of, claim against, or property or contractual rights of any kind in tangible property that was used in the export or attempt to export that was the subject of the violation; and

(C) any of that person's property constituting, or derived from, any proceeds obtained directly or indirectly as a result of the violation.

(h) No person convicted of a violation . . . shall be eligible, at the discretion of the Secretary, to apply for or use any export license under this Act for a period of up to 10 years from the date of the conviction. The Secretary may revoke any export license under this Act in which such person has an interest at the time of the conviction.

C. LEGAL ANALYSIS

Enactment of the EAA, and other United States government attempts to intercept the illegal exports of high technology, have been subject to many legal challenges. One major aspect of the EAA is the extraterritorial jurisdiction of the law: that is, the law gives federal authorities the power to enforce export controls in other countries.[58] Also, the federal government's interception of high technology exports under the EAA provisions have been challenged under various constitutional theories such as the rights of due process, the commerce clause, the fourth amendment's search and seizure provisions, and the first amendment.

1. *Extraterritorial Application*

The EAA authorizes export controls on "goods, technology, other information subject to the jurisdiction of the United States, or exported by any person subject to the jurisdiction of the United States."[59] Congress intended that the Customs Service play a major role in the extraterritorial enforcement of the EAA.[60] "Extraterritoriality" refers to the application of the EAA to transactions or activities outside the United States' borders. Generally, principles of international law give each state sovereignty within its boundaries and prohibit other states from acting unilaterally in another state's territory.[61] However, under cer-

58. Report Administration Amendments Act of 1985, Pub. L. No. 99-64, § 113, 99 Stat. 148. The EAA is not the only federal legislation that has extraterritorial elements. Several other statutes either regulate activities outside the U.S. or control conduct in the U.S. that affects foreign nations. *See* 50 U.S.C. app. § 1-44 (1982); 22 U.S.C. § 2778 (1982); 42 U.S.C. § 2011 (1982); 15 U.S.C. § 22 (1982); 15 U.S.C. § 1 (1982); 50 U.S.C. § 1701-06 (1982).

59. EAA, *supra* note 26, § 6, 93 Stat. at 503 (codified at 50 U.S.C. § 2405).

60. *See* H.R. REP. NO. 80, 99th Cong., 1st Sess. 62-63, *reprinted in* 1985 U.S. CODE CONG. & ADMIN. NEWS 124-25.

61. *See* Comment, *Extraterritorial Application of United States Law: The Case of Export Controls*, 132 U. PENN. L. REV. 355, 366-72 (1984). *See also* Fazzone, *Business Effects of the Extraterritorial Reach of the U.S. Export Control Laws*, 15 INT'L L. & POL. 545 (1983). Samie, *Extraterritorial Enforcement of United States Antitrust Laws: The British Reaction*, 16 INT'L LAW. 313 (1982). Tittman, *Extra-territorial Application to U.S. Export Control Laws on Foreign Subsidiaries of U.S. Corporations: An American Lawyer's View from Europe*, 16 INT'L LAW. 730 (1982). Note, *Extraterritorial Application of the Export Administration Act of 1979 Under International and American Law*, 81 MICH. L. REV. 1308 (1983). *See generally* Dam, *Economic and Political Aspects of Extraterritoriality*, 19 INT'L LAW. 887 (1985); Feinberg, *Economic Coercion and Economic Sanctions: The Expansion of the United States Extraterritorial Jurisdiction* 30 AM. U.L. REV. 323 (1981); Gollieb, *Extraterritoriality: A Canadian Perspective*, 5 NW. J. INT'L L. & BUS. 449 (1983); Jackson, *United States-EEC Trade Relations: Constitutional Problems of Economic Interdependence*, 16 COMMON MKT. L. REV. 453 (1979); Kastenbaum & Olson, *Federal Amicus Intervention in Private Antitrust Litigation Raising Issues of Extraterritoriality: A Modest Proposal*, 16 INT'L LAW. 587 (1982).

tain circumstances, extraterritorial application of another country's law is accepted as an exception to the basic sovereignty rule.[62]

The EAA legislates extraterritorial jurisdiction in several instances. No person may reexport a technology that was originally exported from the United States, nor can they export with the knowledge that the product will be reexported.[63] Unless authorized by the Office of Export Administration, "no person in the United States or a foreign country may: Reexport any technical data imported from the United States" nor export or reexport any foreign-produced product if the product contains a major portion of United States technical data.[64]

The purpose of the EAA's extraterritorial jurisdiction is to stop exporters from getting around the law by indirect export. If the EAA did not grant this power, United States exporters could export to an authorized location and then arrange for a reexport to the desired unauthorized location.[65] The alternatives to extraterritorial jurisdiction are either to stop high technology exports, or to place stringent controls on exports and allow them only to those countries that are friendly to the United States.[66] To further the United States' foreign policy objectives, the President is authorized to control exports.[67] The President has power to apply the EAA extraterritorially by regulating the export of "goods, technology, or other information subject to the jurisdiction of the United States," and exports by "any person subject to the Jurisdiction of the United States."[68] Although Congress authorizes extraterritorial application of the EAA, authorization under international law is disputed.[69]

Two cases have tested both the legality and the efficacy of the EAA's extraterritorial controls. In 1981, the United States responded to the imposition of martial law in Poland by imposing economic sanctions and by tightening the trade restrictions on exports to the Soviet Union.[70] In order to obstruct Soviet efforts to construct a trans-Siberian oil and gas pipeline, the United States sought western European co-

62. *See* Comment, *supra* note 61, at 369. A state may have jurisdiction to govern its own citizens, even if they are in a foreign location, under the nationality principle.

63. 15 C.F.R. § 374.1 (1986).

64. *Id.* § 379.8(a)(1).

65. Moyer & Mabrey, *Export Controls as Instruments of Foreign Policy: The History, Legal Issues, and Policy Lessons of Three Recent Cases*, 15 LAW & POL'Y INT'L BUS. 1, 108 (1983).

66. *See* Comment, *supra* note 61, at 382.

67. 50 U.S.C. app. 2405(a)(1) (Supp. III 1985).

68. *Id.*

69. *See* Moyer & Mabrey, *supra* note 65; Note, *In the Wake of the Pipeline Embargo: European-United States Dialogue*, 12 FLA. ST. U.L. REV. 73 (1984).

70. 47 Fed. Reg. 27,250-52 (1982). *See Legislation and Regulations*, 21 INT'L LEGAL MATERIALS 864 (1982).

operation to halt oil and gas production equipment going to the Soviets. In June 1982, the United States began to require prior written authorization from the Department of Commerce for the export of all oil and gas related technology or data by any person subject to the jurisdiction of the United States, including technology not originating from the United States.[71] Regulations defined "persons subject to the jurisdiction of the United States"[72] to include foreign subsidiaries of the United States firms, foreign firms using United States technology, and foreign firms owned by United States shareholders.[73]

Europeans strongly objected to United States' pipeline regulations. The European Economic Community (EEC) filed a formal diplomatic protest with the Department of State,[74] and other European nations either ordered or strongly encouraged their companies to ignore the United States' regulations.[75] Faced with this pressure and outright hostility, the United States finally backed down and lifted the pipeline restrictions before any judicial ruling on the lawfulness of the United States regulations could assess either the domestic or international legal implications of these extraterritorial restrictions.[76]

One case did arise out of United States' attempts to embargo construction of the Soviet trans-Siberian pipeline. Dresser Industries (United States) and Dresser (France) lost a three million dollar parts contract with General Motors because, under the United States directive, the parts were to be used for the Soviet oil and gas pipeline.[77] The French government served Dresser (France) with a "Requisition Order for Services" to complete delivery of the Soviet-bound parts.[78] Dresser Industries loaded the parts onto ships but the United States Department of Commerce issued orders denying Dresser export privileges for the oil and gas parts.[79]

In an equity action in federal district court, Dresser sought to enjoin the United States government from enforcing sanctions on Dresser for shipping the parts to the Soviets.[80] In denying injunctive relief, the court wrote that there was a "potential for profound harm" if the government were enjoined from halting Dresser's shipment.[81] The court

71. 47 Fed. Reg. at 27,250. More detailed discussions of the pipeline controversy can be found in Comment, *supra* note 61, at 364-66 and in Note, *supra* note 69, at 73.

72. 50 U.S.C. app. § 2405(a)(1) (Supp. III 1985).

73. *Legislation and Regulations, supra* note 70, at 866.

74. *Id.* at 891.

75. Note, *supra* note 69, at 79.

76. Note, *supra* note 61, at 1310.

77. Fazzone, *supra* note 61, at 573-74 n.4.

78. Ellicott, *supra* note 25, at 553.

79. *Id.*

80. Dresser Industries, Inc. v. Baldridge, 549 F. Supp. 108 (D.D.C. 1982).

81. *Id.* at 110.

noted that United States regulations were a major foreign policy exercise designed to prevent the construction of the Soviet pipeline and that the regulations were "essential to the accomplishment of important foreign policy objectives."[82]

The experience with Dresser signals a trend in the Department of Commerce that should extend to the Customs Service operating under Operation Exodus, namely, that a broad application of extraterritorial jurisdiction will be applied to further United States foreign policy goals of keeping technology out of the Soviet Union's hands. This jurisdiction will not be exerted without straining relations with those countries that might be affected.[83] Foreign demand may be shifted away from United States technology manufacturers if the foreign buyers are leary of United States law. Because of the uncertainty surrounding high technology sales overseas, contracts should be carefully drawn to recognize a myriad of contingencies, including: (1) risk allocation among parties for the impossibility of performance; (2) contingency plans for substitute products; (3) excuse of performance if the government intervenes; and (4) no liability if a party is unable to obtain a license or if a license is revoked. Moreover, contracts should specify which country will have jurisdiction over any possible mediation, arbitration, or litigation arising out of the transaction.[84]

2. *Legal Challenges*

Operation Exodus is a relatively new program, but the effort to control technology exports from the United States is really old wine in a new bottle. Throughout the Nation's history, import and export controls have been in effect.[85] When the United States government has intercepted high technology exports in the past, those actions have been challenged on several legal theories. No doubt such challenges will be pondered in the future if Operation Exodus is successful in fulfilling its goal of stopping the outflow of high technology to the Soviets. This subsection discusses several court cases that have raised legal challenges to the government's interception of high technology goods.

In *United States v. Brumage*, the defendant's electronics company was prosecuted for willfully exporting electronic and technical equipment to Hungary and East Germany without a valid export license.[86]

---

82. *Id.*

83. *See* Tittman, *supra* note 61, at 733. Several foreign governments have reacted by enacting legislation to prevent foreign subsidiaries of U.S. companies from complying with various U.S. directives.

84. *See* Fazzone, *supra* note 61, at 579-87.

85. *See* Berman & Garson, *supra* note 6, at 791. *See also* Note, *supra* note 6 at 575.

86. 377 F. Supp. 144 (E.D.N.Y. 1974). The defendant was charged specifically with violating § 6(b) of the EAA, 50 U.S.C. app. § 2405(b).

The defendant argued that the EAA was unconstitutionally vague because the EAA proscribed certain exports to "Communist-dominated nations," and that reasonable men could differ as to which countries would be covered.[87] The court rejected this argument primarily because regulations promulgated under the EAA identified which nations were "Communist-dominated."[88] Today, a void-for-vagueness challenge for Exodus seizures would similarly fail because foreign nations to whom exporting is illegal are noted by statute.[89]

In *United States v. Spawr Optical Research, Inc.*,[90] the defendants were convicted of violating provisions of the EAA because they unlawfully exported laser mirrors to the Soviet Union. After inventing a superior process for polishing laser optics and mirrors, the Spawrs, the owners of Optical Research, explored international markets through a business arrangement with a West German national, named Weber, who promoted and distributed Spawr mirrors in several communist block nations, including the Soviet Union.[91] In January 1976, Weber obtained the Spawrs' authorization to accept an order for mirrors from a purchasing agency of the Soviet government.[92] The Spawrs shipped the order to Weber in West Germany who then forwarded the entire order to Moscow.[93] The Spawrs never obtained a validated export license for the mirrors that were exported.[94]

In April 1976, when Weber notified Spawr that Weber had received a second Soviet order for Spawr mirrors, Spawr filed an application with the Commerce Department for a validated export license to ship some of the mirrors to the Soviets.[95] The Commerce Department de-

87. 377 F. Supp. at 147.

88. The regulations cited were at 15 C.F.R. § 370.11. The court listed several other reasons to reject the vagueness challenge, including the proposition that an act of Congress is presumptively valid, and that Congress has broad powers to regulate trade with foreign nations under U.S. CONST. art. I, § 8. 377 F. Supp. at 1480. *See also* United States v. Zheng, 768 F.2d 518 (3d Cir. 1985), *cert. denied*, 106 S. Ct. 806 (1986). In *Zheng* the defendant was charged with unlawful purchase and export of high technology equipment. Zheng challenged the statute on the grounds of vagueness, arguing that the Arms Export Control Act, which addressed "items" that were prohibited from export, was too vague. The court, extensively discussing congressional intent surrounding "items," struck down the challenge. *Cf.* United States v. Moller-Butcher, 560 F. Supp. 550 (D. Mass. 1983), *appeal dismissed*, 723 F.2d 189 (1st Cir. 1983) (where the defendants were charged under the EAA with making misleading statements to the Customs Service; the statute was not void-for-vagueness).

89. *See supra* notes 25, 29, 30, and accompanying text.

90. 685 F.2d 1076 (9th Cir. 1982), *cert. denied*, 461 U.S. 905 (1983).

91. *Id.* at 1079.

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.*

nied the application on October 7, 1976 pursuant to Executive Order 11940[96] and existing export regulations, because the mirrors were found to have "significant strategic applications" which posed a potential threat to national security.[97] In February 1977, however, Spawr shipped mirrors to a freight forwarder in Switzerland. Weber then relabeled the packages containing the mirrors and shipped them to Moscow.[98]

The Spawrs did not dispute the government's authority to prosecute them for exporting mirrors to fill the first Soviet order. The Spawrs, however, asserted that the government lacked authority to prosecute them for exporting mirrors for the second Soviet orders because (1) there was no genuine national emergency, (2) the regulations were not rationally related to any emergency then in existence, and (3) the lapse of the EAA shows that Congress intended to terminate the regulations.[99] The court struck down all three contentions.

The court declined to address the "national emergency" question, holding that it was a political question. Further, the court held that regulations limiting the export of high technology goods were rationally related to various national emergencies.[100] The court cited Presidential Proclamation Number 2914 which declared a national emergency based in part on events that "imperil the efforts of this country and those of the United Nations to prevent aggression and armed conflict."[101] The court held that this effort to limit the exportation of strategic items "clearly had a rational relationship to the prevention of aggression and armed conflict."[102]

Finally, the court rejected the Spawrs' argument that Congress intended to terminate these export regulations by allowing the EAA to lapse. The court noted that various presidential and congressional actions taken when the EAA had previously lapsed were taken to maintain the export regulations.[103] Congress "conferred on the President the rulemaking authority necessary to maintain the regulations [which reflects] concern for preserving existing regulation imposed under emergency authority, including . . . the transaction control regulations, which prohibit U.S. persons from participating in shipping strategic

96. 50 U.S.C. app. § 2403 (1976) (Ex. Ord. No. 11940 was revoked by Ex. Ord. No. 12,002, July 7, 1977, 92 Fed. Reg. 35,623).

97. 685 F.2d at 1079.

98. *Id.*

99. *Id.* at 1080. The EAA had lapsing dates incorporated into it, but has continually been reenacted.

100. *Id.* at 1081.

101. *Id.* at 1081, *citing* 3 C.F.R. §§ 99, 100 (1949-53 compilation).

102. 685 F.2d at 1081.

103. *Id. See* Exec. Ord. No. 11940, 3 C.F.R. § 150 (1976), *reprinted in* 50 U.S.C. app. § 2403.

goods to . . . the Soviet Union."[104] Using *Spawr Optical* as an example, the Customs Service's rules implementing Operation Exodus may or may not be in response to a "national emergency." This may be of no consequence because the court deems this a political matter. Even if it were not a "political question," there are a plethora of presidential and congressional directives supporting any agency actions designed to intercept high technology exports going overseas.[105]

Other challenges to the EAA have involved the fifth amendment rights to due process[106] and illegal search and seizure under the fourth amendment.[107] However, these attempts to thwart conviction under the EAA do not relate to actions by the Customs Service or other agencies in intercepting high technology goods. Rather, they are challenges generally used to avoid conviction. What is clear from the limited amount of existing case law is that Operation Exodus has enough legal precedent behind it to be a strong tool in the government's efforts to stem illegal exports to Soviet block countries.

V. STRATEGIES FOR THE HIGH TECHNOLOGY CORPORATION AND THE PRACTITIONER TO AVOID OPERATION EXODUS LIABILITY

When preparing to ship high technology orders overseas, a shipper should identify orders for products, parts, or technology which are likely to be shipped abroad and see that they are handled by personnel

104. 685 F.2d at 1081, *citing S. Rep. No.* 466, 95th Cong., 1st Sess. 3, *reprinted in* 1977 U.S. CODE CONG. & ADMIN. NEWS 4540, 4542. It should be noted that the President continually extends export controls under the EAA. *See* Exec. Ord. No. 12,444, 19 WEEKLY COMP. PRES. DOC. 1436 (Oct. 14, 1983); Message to Congress Reporting on the Continuation of Export Control Regulations, *id.* at 1437; Exec. Ord. No. 12,470, Continuation of Export Control Regulations, 20 WEEKLY COMP. PRES. DOC. 452-54 (1984). *See* Announcement Concerning Licensing and Enforcement Procedures [under the EAA], 20 WEEKLY COMP. PRES. DOC. 420-21 (1984). For other older examples, see Exec. Ord. No. 11810, 3 C.F.R. 905 (1971-75 compilation) (covering 29-day lapse; revoked by Exec. Ord. No. 1181, 3 C.F.R. 924 (1971-75 compilation)); Exec. Ord. No. 11796, 3 C.F.R. 888 (1971-75 compilation) (covering 14-day lapse; revoked by Exec. Ord. No. 11798, 3 C.F.R. 890 (1971-75 compilation)); Exec. Ord. No. 11677, 3 C.F.R. 719 (1971-75 compilation) (covering 28-day lapse; revoked by Exec. Ord. No. 11683, 3 C.F.R. 724 (1971-75 compilation)).

105. *See supra* notes 25, 30-37.

106. Trane Co. v. Baldrige, 552 F. Supp. 1378 (W.D. Wis. 1983), *aff'd*, 728 F.2d 915, *cert. denied*, 105 S.Ct. 105 (1984) (corporations doing business with Arab States challenged portions of the EAA and implementing regulations, but it was held that the prohibitions did not infringe on plaintiffs' first amendment right of free speech, fifth amendment substantive or procedural due process rights, or rights under the ninth amendment).

107. United States v. Whiting, 781 F.2d 692 (9th Cir. 1986) (regarding suppression of evidence under the "good faith" exception to the fourth amendment's exclusionary rule). *See* United States v. Moller-Butcher, 560 F. Supp. 550 (D. Mass. 1983) (search and seizure issues).

experienced in export matters.[108] Companies manufacturing high technology products should ensure that corporate personnel know current export regulations and that appropriate screening and license procedures are followed. On both foreign and domestic purchases, many companies notify a purchaser in writing that a validated export license is required and this is built into standard contract language.[109] Similarly, company employees living abroad or traveling internationally should be informed about United States government restrictions on the movement of high technology out of the United States. Any questions relating to licensing requirements and potential problems should be directed to the appropriate agency or to corporate counsel.[110]

To expedite legitimate exports, all requests by the Customs Service for specifications on items that are being detained for examination should be filled promptly. Often licensing determinations can only be made after the licensing agency (the Department of Commerce or the Department of State, Office of Munitions Control) receives adequate specifications from the manufacturers.[111] The exporter should be sure that product specifications are written by a technical engineer, not the marketing manager who may exaggerate.

To prevent illegal exports, altered shipping schedules, and fines, corporate policies must include an aggressive in-house program stressing regulatory compliance. To effect the policies, the company's export licensing procedures should be checked routinely to ensure accuracy and effectiveness. This requires commitment to an effective export control program from top management; this commitment should be regularly communicated to the company's employees, contractors, and buyers. Also, a centralized export licensing staff should be designated. Within this staff, there should be procedures to ensure communication between the export licensing staff, the marketing department, customer relations, and shipping personnel. This staff should maintain clear lines of communication not only within the office, but between licensing agencies and the Customs Service to help speed up various administrative processes.

VI CONCLUSION

Operation Exodus represents a strong effort by the United States Customs Service to intercept illegal exports of high technology products to Soviet bloc countries. While the number of seizures has increased

108. DEP'T OF TREASURY, U.S. CUSTOMS SERVICE, BUSINESS ADVISORY NO. 3 ON OPERATION EXODUS (Jan. 1984).

109. *Id.*

110. *Id.*

111. *Id.*

since Operation Exodus was implemented, it is difficult to know what percent of the total amount of illegal exports these seizures represent.[112] The real test of the effectiveness of Operation Exodus will probably occur five to ten years from now when a proper intelligence survey of the balance sheet (seizures versus losses) can be made. Until then, to prevent penalties, heavy fines, or imprisonment, corporate officers and practitioners working with high technology companies should maintain tight export licensing procedures and practices.

112. See *supra* note 47 for information on seizures.