THE WALL STILL STANDS! COMPLYING WITH EXPORT CONTROLS ON TECHNOLOGY TRANSFERS IN THE POST-COLD WAR, POST-9/11 ERA

*Christopher F. Corr**

* Mr. Corr is a partner with White & Case, LLP. The views expressed in this article are those of the author alone. The author gratefully acknowledges the assistance of Richard Burke, Corey Norton, and Mary Featherston in the preparation of this article. This article is not and should not be regarded as legal advice.

I. INTRODUCTION

What a troublesome thing a wall is! I thought it was to defend me, and not I it!

-Henry David Thoreau[1]

Protection of capabilities and technologies readily available on the world market is, at best, unhelpful to the maintenance of military dominance and, at worst, counterproductive, undermining the industry upon which U.S. military-technological supremacy depends.

-Report of the Defense Science Board Task Force on Globalization and Security[2]

The fall of the Berlin Wall signaled the end of the Cold War and a dramatic easing of military tensions between the United States and any plausible military rival. This geopolitical watershed naturally raised expectations that the extensive restrictions on the international transfer of commercial technology and hardware had become largely unnecessary and

1. HENRY D. THOREAU, A YANKEE IN CANADA WITH ANTI-SLAVERY AND REFORM PAPERS 74 (Greenwood Press 1969) (1892).

2. *Defense Panel Recommends Cut in Export Control List, DOD Role*, WASH. TARIFF & TRADE LETTER, Feb. 14, 2000, at 1 (quoting DEF. SCI. BD., TASK FORCE ON GLOBALIZATION AND SECURITY (1999)) [hereinafter *Defense Panel Recommends Cut*].

would be lifted to a significant extent. The rationale undergirding export controls on trade in commercial goods and technology with a possible military end-use—threat of a large-scale conventional or nuclear conflict—had markedly diminished. Moreover, because U.S. dominance in technology was no longer a given, as it was during much of the Cold War, and U.S. companies had increasingly found that they must export products and technology in order to remain competitive in the global marketplace, unilateral U.S. controls became unrealistic and largely self-defeating. As the competitiveness and health of the export-dependent U.S. technology sector has a direct bearing on the U.S. ability to develop on its own new generations of "smart" defense systems, it seemed obvious that relaxing unnecessary restrictions on technology exports could well advance U.S. national security.[3]

At first, the U.S. government reacted consistently with these expectations, eliminating restrictions on the transfer of certain types of technology in the early 1990s in response to the deflation of East-West tensions. The government liberalized trade with Eastern European countries, and raised the threshold for technology subject to national security or foreign policy controls, thereby freeing exports of technology at lower levels.[4]

---

3. Many in the Clinton Administration, including the Defense Department, recognized that the military increasingly relies on technological superiority, and that the civilian commercial sector, not the military industrial sector, drives technology. Karen Alexander, *Dealing the China Card: Commerce Official at Ground Zero*, LEGAL TIMES, Mar. 22, 1999, at 1. That sector, in turn, is increasingly dependent on exports. *See id*. It is therefore tautological that for export control purposes you cannot "at once strangle and promote the source of your technological superiority." *Id*. There were many in the Clinton Administration and Congress, however, who did not share this view. *See id*.

4. TRADE PROMOTION COORDINATING COMM., TOWARD A NATIONAL EXPORT STRATEGY: REPORT TO THE UNITED STATES CONGRESS 29, 54 (1993); Export Administration Regulation: Simplification of Export Administration Regulations, 60 Fed. Reg. 25,268, 25,272 (May 11, 1995) (proposed rules); Commercial Communications Satellites and Hot Section Technology for the Development, Production or Overhaul of Commercial Aircraft Engines, 61 Fed. Reg. 54,540, 54,540 (Oct. 21, 1996) (interim final rule); Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,572–73 (Dec. 30, 1996) (interim rule). The government also liberalized trade with former Warsaw Pact countries no longer viewed as enemies or major threats to national security. *See* 15 C.F.R. pt. 738 (Supp. 1 2003); *see also* 15 C.F.R. pt. 740 (Supp. 1 2003).

Soon, however, the government reversed course on liberalization. Despite tremendous changes in post-Cold War international relations, the export control burden on U.S. business actually has *increased* in many respects since the collapse of the Soviet Union. There are still *over five* agencies enforcing an array of controls on the transfer of goods and technology to specified destinations, pursuant to *over forty* statutes.[5] The number of export license applications filed with U.S. government agencies that control technology exports actually increased after the end of the Cold War.[6] While the United States certainly continues to face threats from terrorist networks and certain countries of concern, these threats are of a different scale and magnitude than the threat posed by the organized military of the Soviet Bloc nations and do not warrant the same type of extensive technology controls.[7]

Since the events of September 11, 2001, the trend to tighten restrictions has gathered pace, casting a pall over the entire licensing process, not only anti-terrorism controls aimed at so-

---

5. U.S. INT'L TRADE COMM'N., PUB. NO. 3124, OVERVIEW AND ANALYSIS OF CURRENT U.S. UNILATERAL ECONOMIC SANCTIONS app. D (1998) [hereinafter CURRENT U.S. UNILATERAL ECONOMIC SANCTIONS]; NAT'L ASS'N. OF MFRS., A CATALOG OF NEW U.S. UNILATERAL ECONOMIC SANCTIONS FOR FOREIGN POLICY PURPOSES 1993–96 tbl. 1 (1997). *See infra* Part III (discussing agencies that enforce export regulations).

6. The number of export licenses filed with the U.S. Commerce Department in 1999 increased by roughly 15% from the year before to 12,650, the highest number in almost a decade. *Inside BXA*, EXPORT PRACTITIONER, Feb. 2000, at 24, 24–25. *See* GEN. ACCOUNTING OFFICE, GAO-01-528, EXPORT CONTROLS: STATE AND COMMERCE DEPARTMENT LICENSE REVIEW TIMES ARE SIMILAR 32 (2001) [hereinafter LICENSE REVIEW TIMES]. The Bureau also received 2,600 notifications of computer shipments, most of which were referred to the State, Energy and Defense Departments for consultations. *Inside BXA*, *supra* at 25. *See* LICENSE REVIEW TIMES, *supra* at 35. The applications in 2000 were lower, but were significant, at roughly 11,000. LICENSE REVIEW TIMES, *supra* at 2. Roughly 25% of the applications in 1999 were not approved. *Inside BXA*, *supra* at 25. Nearly 20% were turned down or returned without action in 2000. LICENSE REVIEW TIMES, *supra* at 42. License applications submitted to other agencies also increased. For example, approximately 46,000 license applications were submitted to the State Department in 2000, of which nearly 20% or 9000 were refused. *Id.* at 5, 12.

7. Given the nature of more recent threats, controls on nuclear-sensitive items under the Nuclear Suppliers Group, chemicals under the Chemical Weapons Convention, and missile technology under the Missile Technology Control Regime appear more relevant than Wassenaar dual-use technology controls aimed at the Soviet Bloc. *See* 15 C.F.R pt. 774 (Supp. 1 2003); *see also* 15 C.F.R. pt. 710 (2003).

called "rogue" states and end-users with potential terrorist connections.

This post-Cold War paradox is rooted in several causes.

- Failure to Keep Pace with Technology.
  Although remaining export controls were set at a specific technology level that may have been highly sophisticated and sensitive at the time the control level was established, the rapidly evolving pace of technological advancement often renders the delineated control levels outmoded, restricting exports of generic and freely available technology;[8]
- Expanding Unilateral Foreign Policy Controls.
  Recent U.S. administrations have embraced economic sanctions, including embargoes, as a policy tool to be used against a growing list of countries for political rather than national security purposes, motives not shared by other countries supplying similar technology;[9]
- Resistance to Change.
  Reform often requires consensus, and there are many important interests in the Executive Branch and Congress that are philosophically opposed to liberalization of the current system. Further, jurisdiction over certain types of technology has been transferred to stricter and less transparent administering agencies;[10]

---

8. The cumbersome, conflict-ridden and dilatory regulatory process often obstructs timely adjustments to the control level in order to keep up with advances in technology. For example, until the decontrol of computer microprocessors was announced in June 2000, standard commercial PCs were subject to license requirements before they could be exported from the United States to many countries. Expansion of License Exception CIV Eligibility for "Microprocessors" Controlled by ECCN 3A001 and Graphics Accelerators Controlled by ECCN 4A003, 65 Fed. Reg. 37,039, 37,039 (June 13, 2000) (to be codified at 15 C.F.R. pt. 774) (announcing an interim rule adjusting microprocessor eligibility levels).

9. For example, the sanctions imposed against India and Pakistan after their detonation of nuclear devices illustrates the volatile political nature of unilateral controls. The President was obligated by statute to impose sanctions. As it turned out, however, at the time the President invoked the statute and announced imposition of the sanctions, the agencies had not yet issued implementing regulations. It was not even clear which agencies should administer the sanctions. After several years they were largely lifted, and were generally viewed as ineffective. *See infra* Part IV.B.4.a.

10. *See infra* text accompanying notes 83–92.

- More Export Responsibility.
  Export control authorities have sought to shift some of the burden of compliance to private business, requiring them to devote more resources to export controls, particularly end-user and end-use checks;[11] and
- Emergence of E-Commerce.
  The Government is struggling to extend the traditional regulatory regime developed for brick-and-mortar business to new business models and technologies such as e-commerce-oriented internet technology transfers, globalized computer networks, and encryption software.

As the health and competitiveness of the U.S. economic base is a fundamental prerequisite to U.S. security and military preeminence, the need for reconsideration and overhaul of the burdensome patchwork of export controls is manifest. Meaningful reform of the process will require an up-to-date focus on those technologies that must be restricted for current national security purposes, tempered by the post-Cold War reality that some sensitive technologies may be available from suppliers in other countries, and by the need to reduce unnecessary administrative burdens on U.S. companies that increasingly must compete internationally.

The continued imposition of extensive export controls on U.S. industry in the post-Cold War era, despite diminished risks from other nation-states and increased international competition, has not gone without notice or criticism—even at the highest levels. For instance, an advisory board to the U.S. Defense Department called for an overhaul of U.S. export controls, including a reduction in the types of technologies controlled and a streamlined license application process, warning that over-broad controls could only hurt U.S. national security. This advisory board, the Defense Science Board's Task Force on Globalization and Security, recommended that U.S. policy be changed to "protect for the purposes of maintaining military advantage only those capabilities and technologies of which the United States is the sole possessor and whose protection is deemed necessary to preserve an essential military

11. *See infra* text accompanying notes 195–96.

capability."[12] The Task Force found that "[p]rotection of capabilities and technologies readily available on the world market is, at best, unhelpful to the maintenance of military dominance and, at worst, counterproductive, undermining the industry upon which U.S. military-technological supremacy depends.[13]

Despite these warnings, efforts toward meaningful reform of the process have failed to reach traction.[14]

Businesses, therefore, must take heed. Due diligence requires that companies engaged in cross-border transactions have an understanding of the complex post-Cold War export control requirements, and that they implement effective measures to comply with these controls. The penalties for violating export restrictions are potentially severe, including incarceration of company officials and substantial fines.[15]

Compliance with intangible technology transfer controls poses special challenges, as restricted technologies may be "exported" in a variety of ways other than the traditional physical shipment from a U.S. port to a foreign port. For instance, routine acts such as reviewing technical data with non-U.S. nationals at facilities in the United States, or sharing technical information with affiliates in foreign locations via the

---

12. *Defense Panel Recommends Cut*, *supra* note 2, at 1 (quoting the Defense Science Board's Task Force on Globalization and Security).

13. *Id.* Other commentators in the private sector issued similar warnings. For example, a congressionally appointed commission on the future of the U.S. aerospace industry called for a "fundamental shift away from the existing transaction-based licensing system," warning that the "health and competitiveness of the U.S. aerospace industry" was imperiled by "our own export control regime." *Commission Recommends "Fundamental Shift" in Export Licensing*, WASH. TARIFF & TRADE LETTER, Nov. 25, 2002, at 3 (quoting the Commission's Nov. 18, 2002 Final Report).

14. For instance, a GAO study found that "U.S. export regulations governing China contain inherent inconsistencies and are based on outdated government assessments of the availability of technology from non-U.S. sources." GEN. ACCOUNTING OFFICE, GAO-02-620, EXPORT CONTROLS: RAPID ADVANCES IN CHINA'S SEMICONDUCTOR INDUSTRY UNDERSCORE NEED FOR FUNDAMENTAL U.S. POLICY REVIEW, at Highlights (2002) [hereinafter RAPID ADVANCES]. The Departments of Commerce, Defense and State disagreed with this recommendation, and undertook no meaningful reforms in response. *See id*.

15. *See infra* Part V (discussing penalties under the various regulations).

company network or the internet are subject to export controls.[16]

This Article provides an overview of the principal regulatory controls on transfers of technology and software. It first sets out a brief history of the current regime, and summarizes the broad regulatory framework for export controls and the agencies responsible for implementing them. The Article then highlights the rules relevant to technology transfers, and goes on to discuss the reasons underlying the persistence of extensive controls. The Article closes with a discussion of procedures companies may adopt to ensure compliance with applicable regulatory controls and avoid imposition of penalties.

II. HISTORICAL BACKGROUND

> *The capitalists will sell us the rope with which we will hang them.*
>
> -Vladimir I. Lenin

> *The protection of the West's technological advantage is an essential part of our collective defence. . . . For some time it has been evident that the Soviet Union and its allies have been pursuing a far-reaching and well coordinated programme to acquire from the West advanced technology with military potential.*
>
> -Paul Channon
> former British Trade Minister[17]

> *It is my thesis that, given that the Berlin Wall has been torn down, we've liberated Eastern Europe and destroyed the Soviet Union, clearly there is a need to change the basic focus of our export administration system.*
>
> -Phil Gramm
> former Senator and Chairman of
> the Senate Banking Committee.[18]

---

16. *See* 15 C.F.R. § 734.2(b) (2003).

17. *Security Export Control*, BRITISH BUS., June 14, 1985, at i (quoting Paul Channon).

18. *Establishing an Effective, Modern Framework for Export Controls: Hearings*

A. Origins

The modern export control framework was forged in the ashes of World War II. As tensions of a global Cold War mounted, the United States and its western allies worried that, as Lenin had predicted, the Capitalist West would sell the Communist East the rope with which to hang it. According to a study at the time:

> In recent years, the United States Government has learned of a massive, well-organized campaign by the Soviet Union to acquire Western technology illegally and legally for its weapons and military equipment projects. Each year Moscow receives thousands of pieces of Western equipment and many tens of thousands of unclassified, classified, and proprietary documents as part of this campaign. Virtually every Soviet military research project—well over 4,000 each year in the late 1970s and over 5,000 in the early 1980s—benefits from these technical documents and hardware. The assimilation of Western technology is so broad that the United States and other Western nations are thus subsidizing the Soviet military buildup.[19]

B. COCOM

To forestall the West-to-East transfer of technology and hardware that would enhance Soviet Bloc military prowess, the Western allies formed the Coordinating Committee for the Control of Multinational Trade, better known as COCOM.[20]

---

on S. 149 Before the Senate Comm. on Banking, Hous., and Urban Affairs, 107th Cong. 22 (2001) (statement of Sen. Phil Gramm, Member, Senate Committee on Banking, Housing, and Urban Affairs).

19. U.S. CENT. INTELLIGENCE AGENCY, SOVIET ACQUISITION OF MILITARILY SIGNIFICANT WESTERN TECHNOLOGY: AN UPDATE (1985) (distributed by the Business Council for International Understanding pursuant to a U.S. government-industry Conference on Technology Security, National Security, Industrial Security and Competitiveness, held in Washington, D.C. on October 15, 1987) (on file with author). *See id*. (assessing Western technology transferred to the Soviet military during the 1970's and early 1980's).

20. *See* Harold J. Berman & John R. Garson, *United States Export Controls—Past, Present and Future*, 67 COLUM. L. REV. 791, 834–36 (1967); Cecil Hunt, *Multilateral Cooperation in Export Controls—The Role of COCOM*, 14 U. TOL. L. REV. 1285, 1285–87 (1983); PANEL ON THE IMPACT OF NAT'L SEC. CONTROLS ON INT'L TECH.

COCOM was a secretive, non-treaty organization located in Paris.[21] To prevent transfers to the Soviet Bloc,[22] COCOM called for controls on three categories of technology: (1) arms; (2) nuclear-related items; and (3) so-called "dual-use" technology and hardware that had both civilian and potential military applications.[23] The dual-use controls were controversial because they were broad and restricted normal commercial trade

---

TRANSFER, COMM. ON SCI., ENG'G, AND PUB. POLICY, BALANCING THE NATIONAL INTEREST: U.S. NATIONAL SECURITY EXPORT CONTROLS AND GLOBAL ECONOMIC COMPETITION 18, 123, 137 (1987) [hereinafter BALANCING].

21. *See* Hunt, *supra* note 20, at 1286; BALANCING, *supra* note 20, at 137. Membership in COCOM included as many as sixteen countries, among them Japan, Australia, and all North American Treaty Organization (NATO) countries except Iceland. *Id.* at 101 n.3.

22. *See* BALANCING, *supra* note 20, at 72. In 1985, the British Trade Minister summarized COCOM's objectives as follows:

> The protection of the West's technological advantage is an essential part of our collective defence. The alliance depends on technological, not numerical superiority. If our technological lead is eroded, it could do serious damage to our security. In addition, the Soviet Union and its allies would benefit not only from the saving in time and resources which would otherwise be spent on research and development, but they would also be better placed to devise counter measures. Their saving is also a cost; the West would lose an advantage developed at considerable expense which could only be recouped with a great deal of effort and expenditure, much of it at direct cost to the taxpayer.
>
> For some time it has been evident that the Soviet Union and its allies have been pursuing a far-reaching and well-coordinated programme to acquire from the West advanced technology with military potential. There are a number of ways in which this can be done. One important channel is through legitimate trade in high technology designed principally for civil use but which could be diverted or applied to military purposes.
>
> For these reasons the member states of NATO together with Japan have for many years controlled exports of strategically sensitive technology. The list of controlled goods are updated regularly.

Security Export Control, *supra* note 17, at i (quoting Paul Channon).

23. *See* BALANCING, *supra* note 20, at 71. The United States did not publish the COCOM list. *See* Berman & Garson, *supra* note 20, at 838 (noting the lists are classified). Instead, it incorporated the COCOM controls into domestic regulations. *See id*. at 836–40. The British government, however, released the COCOM list to the private sector through *British Business* magazine. *See Security Export Control*, *supra* note 17, at i–iii. British export controls were administered by the U.K. Department of Trade and Industry. *Id*. Controls were divided between the "Industrial List" (i.e. dual-use), the Munitions List, and the Atomic Energy List. *See id*. at iii; *see also* Hunt, *supra* note 20, at 1288–89.

provided it had some conceivable defense-related use.[24] For example, standard computer chips or telecommunications equipment could be viewed as enhancing the Soviet's command-and-control capability. COCOM developed a list of restricted dual-use products, which was subdivided into three levels of control, depending on the sophistication or sensitivity of the technology: (1) "administrative exception" technology that was freely exportable to most destinations upon notice by the member to COCOM; (2) "favorable consideration" technology that required tabling at COCOM and was freely exportable if no objection was lodged; and (3) embargoed technology that was exportable only upon general consensus or unanimous approval from all COCOM members.[25]

Although all members committed themselves to enforce the COCOM controls on dual-use technology, enforcement was uneven. The United States was the most zealous export controls enforcer. U.S. exporters bore the brunt of COCOM enforcement, and were proscribed from marketing or competing in many regions of the world.[26] This phenomenon was largely accepted by U.S. business from the 1950s through the 1970s, because the United States had a considerable technological and commercial lead over the rest of the world. If U.S. exporters were restricted from selling a particular technology to a designated region, it was quite unlikely that another country, particularly a non-COCOM country, was in a position to supply the technology.

In the 1980s, U.S. companies faced growing international competition. Uneven enforcement of export control laws put U.S. companies at a significant disadvantage as technology restricted to certain countries by COCOM and the United States nonetheless became available from non-U.S. and non-COCOM sources.[27] U.S. concerns in this area peaked in 1987, with the disclosure of a transfer by Japanese and Norwegian companies

---

24. Minister Paul Channon acknowledged these objections by businesses: "I recognise that these [dual-use] controls may be seen by some exporters as a burdensome interference with exports, on which our national prosperity depends." *Security Export Control*, *supra* note 17, at i.

25. *See* BALANCING, *supra* note 20, at 97–99.

26. *See id*. at 99–101, 123, 137–38, 140.

27. *See id*. at 137–44.

to the Soviet Navy—in violation of COCOM rules—of sophisticated milling machines and technology for making submarine propellers that were allegedly more difficult to detect.[28] Undeterred by the fact that the COCOM violation involved no U.S. technology and breached no U.S. law, Congress retaliated by passing a law punishing both companies involved in the scandal and their corporate parents,[29] and setting forth

---

28. *See* Bennett A. Caplan, *Skirmishes on Capitol Hill: The Toshiba Affair*, EXPORT TODAY, May–June 1988, at 61, 61–63. The Norwegian company, Kongsberg Trading Company, and the Japanese company, Toshiba Machine Company, were accused of selling to the Soviet Navy five- and nine-axis milling machines and related operation technology that were prohibited by the COCOM dual-use regulations. *See* William C. Triplett, II, *Crimes Against the Alliance: The Toshiba-Kongsberg Export Violations*, POL'Y REV. 8, 8–9 (Spring 1998). These machines could be used to grind large propellers to very high tolerances that would reduce cavitation noise when rotating, thereby enhancing the submarines' ability to evade sonar detection, a critical aspect of submarine warfare technology. *Id.* at 9–10. The scandal occurred at a time when military and diplomatic tensions with the Soviet Union were increasing, and trade tensions with Japan were growing as Japan's burgeoning economy and increasing trade surplus were viewed as a rising threat by many in the United States. News of the scandal during the convergence of these two trends was explosive. *See* Stephen J. Dryden, *The Battle of the Sumo Lobbyists*, REGARDIES, Sept. 1998, at 49, 49. The U.S. Congress held numerous hearings expressing outrage at the violation, and U.S. Congressmen smashed Toshiba consumer products on the steps of the Capitol. *See* Caplan, *supra* at 61–63. It became the most high-profile export control scandal in history. *See* Dryden, *supra*, at 49.

29. *See* War and National Defense Export Regulation, 50 U.S.C. app. § 2410a (2000). After much debate, consideration, and reconsideration of various bills, Congress passed § 2443 of the Omnibus Trade and Competitiveness Act of 1988, which included sanctions against Toshiba Machine Company and Kongsberg Trading Company. Omnibus Trade and Competitiveness Act, Pub. L. No. 100–418, § 2443, 102 Stat. 1107, 1365 (1988) (codified at 50 U.S.C. app. § 2410(a)). These sanctions were harsh and included a three-year import embargo, with certain exceptions. *Id*. Moreover, Congress also punished the parents of these companies, Kongsberg Vaapenfabrikk, and Toshiba Corporation, despite the fact that there was no evidence Toshiba Machine's parent company was involved in the violations. Dryden, *supra* note 28, at 49. The parent companies were proscribed from participating in U.S. government procurement for a period of three years, with certain exceptions. Omnibus Trade and Competitiveness Act § 2443(b).

> The Senate Amendment applies sanctions against Toshiba Corporation, Kongsberg Vaapenfabrikk and any other firm or individual found to have violated CoCom regulations between January 1, 1980 and the date of enactment that resulted in a serious adverse impact on the strategic balance of forces. . . . [S]anctions are . . . applied . . . only to [the] guilty subsidiaries, Toshiba Machine Company and Kongsberg Trading Company, and the parent corporations themselves. Sanctions are applied to the parent corporations in

penalties for future COCOM violations.[30] The United States used the momentum from the scandal to pressure Japan and Europe to strengthen their export control systems.[31] Further, the United States assigned its intelligence gathering network to play a lead role at COCOM to prevent U.S. allies from transferring technology the United States would not allow its own companies to sell. At the close of the 1980s, the United States presided over an increasingly restive COCOM alliance,[32] as well as a business community anxious for liberalized export controls.[33]

> recognition of their responsibilities for the actions and management practices of their subsidiaries.

H.R. CONF. REP. NO. 100-576, at 831–32 (1988), *reprinted in* 1988 U.S.C.C.A.N. 1547, 1864–65. The imposition of penalties by legislation was unprecedented in three respects. First, punishment of parent companies was imposed without direct evidence of their participation in or the knowledge of the violation. Second, punishment was imposed retroactively against named persons, for prior conduct, via legislation rather than by a court or administering agency, as an apparent unconstitutional bill of attainder and *ex post facto* law. Third, punishment was for conduct that violated no U.S. law or regulation, occurred outside the United States, and did not involve U.S. products or technology subject to U.S. jurisdiction. However, the law was never challenged in court.

30. *See* Omnibus Trade and Competitiveness Act § 2444; *see also* H.R. CONF. REP. NO. 100-576, at 834.

> The Senate amendment amends Section 5 of the Export Administration Act of 1979 to require mandatory sanctions for two to five years in any case where credible evidence indicates that a foreign person has violated COCOM regulations and the violation has resulted in a serious adverse impact on the strategic balance of forces. Sanctions include both debarment from contracting with any agency or instrumentality of the U.S. Government and a ban on imports produced by the sanctioned party.

H.R. CONF. REP. NO. 100-576, at 834.

31. *See* Susan F. Rasky, *U.S. Seeks Export Assistance*, N.Y. TIMES, Oct. 17, 1987, at 49; *Business Jumps to Follow Toshiba's Example of 'Compliance Program*, ASAHI EVENING NEWS (Tokyo), Sept. 11, 1987; Takashi Kitazume, *Electronic Industries Assn. Urges Members to Control Exports Strictly*, MAINICHI DAILY NEWS (Tokyo), Sept. 22, 1987.

32. For example, European COCOM members vigorously opposed U.S. extraterritorial sanctions against Japan for the export control violation discussed above. Barbara Casassus, *Japan, W. Europe Hit U.S. Toshiba Sanctions*, J. COMMERCE, Oct. 28, 1988, at 3A. Most galling to the allies was the fact that the United States imposed extraterritorial and extra-jurisdictional penalties without heed to the judicial process and penalties imposed on the violators by the COCOM member countries who, unlike the United States, had legal jurisdiction over the violation. *See* Clyde H. Farnsworth, *Europeans Assail Bill on Export Sanctions*, N.Y. TIMES, Jan. 30, 1988, at A34.

33. *See* Caplan, *supra* note 28, at 63.

C. Wassenaar

The fall of the Berlin Wall and the end of the Cold War brought about a change in the focus of export control policies. COCOM was terminated in 1994,[34] and after tense negotiations, was replaced in 1996 by the Wassenaar Arrangement (the Wassenaar Arrangement)—a much weaker entity based in the Netherlands.[35] Unlike COCOM, Wassenaar members do not have veto power over one another's exports, do not have an agreed-upon list of embargoed or restricted countries, and do not have a requirement for notification of exports prior to shipment. The Wassenaar Arrangement merely requires an aggregate summary notification of listed exports after transfer takes place, and a notice of a license denial.[36] The stated goal of the Wassenaar Arrangement is "to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies . . . ."[37] However, the Wassenaar Arrangement controls are implemented solely at the discretion of member governments pursuant to their own national policies.

Members of the Wassenaar Arrangement more often than not fail to comply with even these watered-down requirements, further lessening the Wassenaar Arrangement's effectiveness.[38]

---

34. *History of the Wassenaar Arrangement*, *at* http://www.wassenaar.org/docs/History.html (last visited Apr. 5, 2003).

35. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies is named after a suburb of The Hague, Netherlands, where agreement was reached to establish the international arrangement on export controls. The Arrangement received final approval by thirty-three co-founding nations in July 1996 and began operations in September 1996. It is headquartered in Vienna. *The Wassenaar Arrangement*, *at* http://www.wassenaar.org/docs/talkpts.html (last visited Apr. 5, 2003).

36. *The Wassenaar Arrangement*, *supra* note 35; *see* Press Release, Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (July 12, 1996) *at* http://www.wassenaar.org/docs/press_1.html (providing initial elements adopted at the Plenary of July 11–12, 1996); Public Statement, Seventh Plenary of the Wassenaar Arrangements (Dec 7, 2001), http://www.wassenaar.org/docs/ps_7.htm (providing amendments by the plenary of December 6–7, 2001).

37. *The Wassenaar Arrangement*, *supra* note 35.

38. The U.S. General Accounting Office (GAO) issued a study that found that license denials are normally reported well behind schedule, and that roughly half of the Wassenaar members did not submit export denials on time. GEN. ACCOUNTING OFFICE,

The U.S. government has continuously sought to toughen the Wassenaar regime, without much success, given that in the post-Cold War geopolitical environment there was no provision for clear delineation of trading "blocks," and that the United States no longer was the sole source of major technologies.[39] Some members of Congress chastised the U.S. administration for not "toughening" Wassenaar, but the criticism was merely an expression of congressional frustration at the demise of COCOM, and suggested a lack of appreciation for the changes in post-Cold War geopolitical realities.[40]

In the post-Cold War era, the United States can no longer control or prevent the transfer by allies and other countries of all technologies it seeks to restrict to countries it views as unreliable or as strategic threats. This is because the United States is no longer the sole supplier of many critical technologies, and because other countries, even close allies, do not always share the U.S. view that a particular country is a strategic threat.[41] For instance, most other Wassenaar members, including some of the closest allies of the United States, simply do not share the U.S. view of China as a restricted destination.[42]

GAO-03-43, NONPROLIFERATION: STRATEGY NEEDED TO STRENGTHEN MULTILATERAL EXPORT CONTROL REGIMES 1–11 (2002). The purpose of reporting denials is to prevent unreliable purchasers from shopping from one Wassenaar member to another. *Id*. at 12–14.

39. *See Washington Gets Half a Loaf at Wassenaar: Proposals on Strengthening Regime Are Left on Cutting Floor*, EXPORT PRACTITIONER, Jan. 2000, at 17, 17–18 (noting, for instance, that the U.S. government vigorously sought a "no undercut" rule, stipulating that no Wassenaar member would approve a sale already denied by another Wassenaar member; the measure failed); *U.S. Will Accept Less Vigorous Catch-all Rules for Wassenaar*, WASH. TARIFF & TRADE LETTER, June 10, 2002, at 1 (stating the United States also sought to implement a Wassenaar "catch-all" rule under which licenses would be required for items that were not on Wassenaar's control list when an exporter knows or suspects an export would be used for illicit purposes; Wassenaar only agreed to consider a "statement of understanding," which would not impose any obligation on exporters to act on any "suspicions" with respect to a proposed export, and refused to set forth a list of countries or end-users of concern).

40. *See Senate Presses for Wassenaar Breakthrough: While Sen. Fred Thompson Reminisces About COCOM, Administration Officials Pledge More Multilateral Rigor*, EXPORT PRACTITIONER, May 2000, at 4, 4 [hereinafter *Senate Presses for Wassenaar Breakthrough*].

41. *See supra* note 13 and accompanying text. This is particularly true in the case of China. *See infra* note 44 and accompanying text.

42. *See infra* note 44 and accompanying text.

Despite the uneven enforcement of export controls on technology transfers, the United States continues to impose broad and prohibitive restrictions on U.S. business. Restricting U.S. businesses from transferring technology that their allies may transfer freely causes an obvious competitive disadvantage for U.S. business.[43] A recent General Accounting Office (GAO) study revealed that U.S. controls on semiconductor manufacturing equipment exports to China were ineffective because they were not reflected in multilateral controls by the Wassenaar Arrangement.[44]

A dramatic illustration of the shift in export control priorities away from Cold War concerns is that Russia—the main target of COCOM in its former incarnation as the center of the Soviet Union[45]—was admitted as a member of the Wassenaar Arrangement.[46] While Russia's admission to Wassenaar is widely viewed as essential, Russia nevertheless has been blamed for blocking improvements to the Wassenaar rules and for failure to enforce those rules.[47]

In the United States, the end of the Cold War was welcomed by U.S. business, which expected the shackles of past export controls would largely be removed. Although many controls on transfers to Soviet Bloc countries in East-West trade were

---

43. U.S. INT'L TRADE COMM'N., PUB. NO. 3433, COMPETITIVE ASSESSMENT OF THE U.S. LARGE CIVIL AIRCRAFT AEROSTRUCTURES INDUSTRY 8-8 (2001) ("The U.S. industry reportedly suffers a competitive disadvantage from unilaterally imposed U.S. export control laws because they are more restrictive than those of the Wassenaar arrangement . . . .").

44. RAPID ADVANCES, *supra* note 14, at 2–3.

> The multilateral Wassenaar Arrangement . . . has not affected China's ability to obtain semiconductor manufacturing equipment because the United States is the only member of this voluntary arrangement that considers China's acquisition of semiconductor manufacturing equipment a cause for concern. The arrangement deems only one type of . . . equipment to be sufficiently sensitive to warrant greater information sharing among arrangement members—no export information is shared for 97 percent of all electronics-related items covered by the arrangement.

Id.

45. *See supra* text accompanying note 20.

46. RAPID ADVANCES, *supra* note 14, at 1 n.1.

47. *Report Faults Russia's Compliance with Export Control Regimes*, WASH. TARIFF & TRADE LETTER, Nov. 4, 2002, at 3.

removed, the burden on U.S. businesses continued or even increased. Multiple U.S. agencies continue to maintain controls on the transfer of wide varieties of technology and equipment to a number of foreign countries, notwithstanding the fact that similar technology is available from other countries, including those that are not a part of the Wassenaar Arrangement or NATO alliance.[48] The fact that over five U.S. agencies enforce at least forty statutes is a striking illustration of the variety and breadth of controls in the post-Cold War and post-September 11 world.

D. September 11, 2001

Calls for reform of the process, including strongly-worded reports and recommendations urging a "thorough overhaul" of the U.S. system to eliminate unnecessary or counterproductive controls, have not been heeded.[49]

The terrorist attack of September 11, 2001 had the effect of slowing down the export clearance process and sidetracking reform efforts as the U.S. government understandably shifted resources to focus on anti-terrorism.[50] Increased security

---

48. *See infra* Part III (discussing agencies that enforce export regulations); *see also* CURRENT U.S. UNILATERAL ECONOMIC SANCTIONS, *supra* note 5, at iii; *see also supra* note 13 and accompanying text (discussing the availability of technology in other countries). Indeed, the ITC found that U.S. unilateral controls alone—setting aside multilateral controls—comprised "42 separate U.S. statutes . . . [under which] are a total of 142 federal sanctions-related provisions . . . [covering a total of] 29 countries subject to U.S. unilateral economic sanctions." CURRENT U.S. UNILATERAL ECONOMIC SANCTIONS, *supra* note 5, at iii.

49. *See* Gary G. Yerkey, *Aerospace Panel Urges 'Thorough Overhaul' of U.S. Export Controls, Cites Harm to Nation*, BNA DAILY REPORT FOR EXECUTIVES, Mar. 21, 2002, at A-15. The Commission on The Future of The U.S. Aerospace Industry called for a "thorough overhaul" of the U.S. system of controlling exports of sensitive technology, saying it has become "increasingly counterproductive" to U.S. national security interests. COMM'N. ON THE FUTURE OF THE UNITED STATES AEROSPACE INDUS., INTERIM REPORT #2 8 (2002), *available at* http://www.aerospacecommission.gov/intrpt2.pdf; *see also supra* text accompanying notes 12–13 (discussing the Defense Science Board Task Force's call for reform).

50. "[S]enior U.S. officials said that the administration's overall review of trade sanctions policy has essentially stalled since Sept. 11, when government agencies, from the State Department to the Justice Department, were mobilized to track and seek to frustrate the activities of terrorists worldwide." Gary G. Yerkey, *Review of Trade Sanctions Policy by U.S. Slows as Focus Shifts to 'Getting Terrorists'*, BNA DAILY

concerns after September 11, 2001 changed the focus of the Bush Administration and Congress from liberalization and streamlining to tightening controls and increasing scrutiny of export transactions and technology transfers.[51] The Commerce Department bureau responsible for administering export controls on dual-use technologies changed its name from the Bureau of Export Administration (BXA) to one that reflected the more cautious, post-September 11 stance of the agency—the Bureau of Industry and Security (BIS).[52]

III. EXPORT CONTROL AGENCIES

Too many bricklayers make a crooked wall.
-Chinese proverb

A number of U.S. government agencies impose and enforce a complex and overlapping system of export control regulations rooted in national security concerns and foreign policy objectives. The breadth and strictness of controls on technology and software transfers varies according to many factors, including the nature and sophistication of the technology, the

---

REPORT FOR EXECUTIVES, Mar. 22, 2002, at A-14. Bruce Williamson, Deputy Director of the State Department's Office of Economic Sanctions Policy, stated that "attention post-September 11 has shifted dramatically to 'expanding and modifying' the U.S. sanctions regime" to "get at [terrorists]." *Id.*

51. *See House, Senate Spar Over EAA*, EXPORT PRACTITIONER, Nov. 2001, at 7, 7; *September 11 Becomes New Force Driving Export Control Law*, WASH. TARIFF & TRADE LETTER, Nov. 26, 2001, at 1, 1–2.

52. Final Rule; Nomenclature Change, 67 Fed. Reg. 20,630, 20,631 (Apr. 26, 2002) (to be codified at 15 C.F.R. ch. VII). Ironically, the word "export" was dropped from its title. *See Complaints Grow About BIS Export License Handling*, WASH. TARIFF & TRADE LETTER, Aug. 5, 2002, at 1, 2 [hereinafter *Complaints Grow*]. "Even the name change to BIS from the Bureau of Export Administration (BXA) raised concerns in the trade community that the agency was moving away from its primary export-licensing role. The new name was a sign that agency managers 'have a different focus' . . . ." *Id*. The effect of the attacks of September 11, 2001 were generally described as shifting the focus of U.S. export controls from the Cold War to terrorism and nonproliferation in developing countries and countries of concern—but whatever the theoretical shift, the reality for U.S. businesses was continued tough controls on the transfer of a vast array of technologies throughout the world, and increased scrutiny.

country of ultimate destination, the identity of the end-user, and the end-use.

Thus, companies engaged in technology transfers must be able to navigate through a complex and fast-changing patchwork of regulations enforced by different agencies. Given the harsh penalties for failure, these companies must ensure they are able to determine: (1) which U.S. government agency has jurisdiction over the transfer; and (2) whether a particular transfer will require prior authorization. To make these determinations, companies must familiarize themselves with the fundamentals of the export control regulatory framework. The following surveys the agencies most relevant to technology transfer.

A. Bureau of Industry and Security

BIS, which is part of the U.S. Commerce Department, administers the Export Administration Regulations (EAR), which control exports and re-exports of U.S. origin merchandise, technology, and software principally for national security and foreign policy reasons.[53] The EAR was issued pursuant to the Export Administration Act (EAA) as supplanted by the International Emergency Economic Powers Act (IEEPA).[54]

These controls are most relevant to technology transfer because, unless the technology in question is deemed to have a primarily military or nuclear application or is intended for a country that is subject to broader political sanctions, the EAR normally will govern.[55] BIS, as a general rule, controls "dual-use" technology—technology that has civil or commercial uses, but could have military applications. BIS administers a list of items subject to licensing under the EAR known as the Commerce

53. 15 C.F.R. pt. 730 (2003).

54. *Id.* § 730.2. The EAA expired in 1994. Despite numerous fruitless initiatives by Congress, the Clinton Administration, and the private sector, Congress has tried and failed on many occasions since 1994 to enact legislation to renew or replace the EAA. *See*, *e.g.*, Gary G. Yerkey, *Sen. Gramm Blasts Lott for Moving Export Control Bill Without Banking Consent*, BNA DAILY REPORT FOR EXECUTIVES, June 20, 2000, at A-3 (discussing Sen. Gramm's criticism of proposed export control legislation). Nevertheless, the provisions of the EAR have remained applicable pursuant to the President's residual authority to issue Executive Orders under IEEPA. 15 C.F.R. § 730.2; International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701–1706 (2000).

55. 15 C.F.R. pt. 730.

Control List (CCL).[56] The EAR set forth the steps exporters must take to determine whether particular technology transfers require BIS licensing. Despite attempts at simplification, these rules remain rather complex.[57]

BIS has long been viewed as the export control agency that is most open to input from the business sector and most pragmatic in its balancing of the U.S. economic interest in free export competition with the national security interest in restricting exports. After September 11, 2001 however, BIS shifted its posture somewhat, emphasizing security and tougher export controls. It has been more reluctant to promote the interests of U.S. exporters when faced with opposition from the traditionally tougher agencies such as the Defense and State Departments.[58]

B. Office of Foreign Assets Control (OFAC)

OFAC, a subdivision of the U.S. Treasury Department, administers country-specific, politically-oriented sanctions programs.[59] At the time this Article was written, OFAC enforced twenty-four economic sanctions programs.[60] High profile trade embargoes are one aspect of OFAC sanctions programs.[61] Sanctioned "countries of concern" at the time this Article was written include Cuba,[62] Iran,[63] Iraq,[64] Libya,[65] North Korea,[66] and

---

56. 15 C.F.R. pt. 774 (2003).

57. On March 25, 1996, BIS published a final rule titled Simplification of Export Administration Regulations. 61 Fed. Reg. 12,714, 12,714 (Mar. 25, 1996) (to be codified at 15 C.F.R. ch. VII). This reorganization and clarification of the EAR became effective April 24, 1996. *Id*. Despite the rule's moniker, however, the EAR and CCL remain convoluted and nebulous.

58. *See BIS Who*?, EXPORT PRACTITIONER, Apr. 2002, at 6, 6.

59. OFAC sanctions regulations are promulgated pursuant to the Trading with the Enemy Act of 1917 (TWEA), 50 U.S.C. app. §§ 1–39, 41–44 (2000), and IEEPA, 50 U.S.C. §§ 1701–1706. *See also* International Security and Development Cooperation Act of 1985, Pub. L. No. 99-83, 99 Stat. 190 (1985); Foreign Operations, Export Financing, and Related Programs Appropriations Act, Pub. L. No. 101-513, 104 Stat. 1979 (1990); Cuban Democracy Act, 22 U.S.C. §§ 6001–6010 (2000).

60. Cuban Assets Control Regulations: Publication of Economic Sanctions Enforcement Guidelines, 68 Fed. Reg. 4422, 4423 (Jan. 29, 2003) (to be codified as appendices to 31 C.F.R. pts. 501, 515).

61. *See* 31 C.F.R. pt. 500 (2003).

62. *Id.* § 515.204.

Sudan.[67] More limited investment sanctions apply to Burma.[68] Controls on exports to North Korea were significantly relaxed in 2000 as jurisdiction was transferred from OFAC to BIS, although imports are still regulated by OFAC.[69]

OFAC regulations typically are broadly worded, allowing OFAC significant interpretive discretion on a case-by-case basis. These OFAC controls often leave businesses that operate internationally in the uncomfortable position of having no clear answer as to whether a proposed transaction is permissible, forcing them to either forgo business opportunities or accept potentially unmanageable risks. Moreover, the specific controls applicable to each embargoed country, and the exceptions to these controls, vary from country to country depending on the executive order imposing them and the regulations implementing them.[70]

Whereas the scope of BIS controls normally is limited to U.S. origin merchandise, the scope of OFAC restrictions is not. OFAC chiefly restricts U.S. persons' involvement in activity in which a sanctioned country has an interest, or from which it may benefit.[71] The restrictions reach a broad range of activities, including the transfer of technology and goods, regardless of

---

63. *Id.* §§ 560.206–.208.

64. *Id.* § 575.205.

65. *Id.* § 550.209.

66. *Id.* § 500.201.

67. *Id.* § 538.205.

68. *Id.* § 537.204.

69. *Id.* § 500.586. On September 17, 1999, President Clinton announced a decision to significantly ease sanctions in place against North Korea. Foreign Assets Control Regulations, 65 Fed. Reg. 38,165, 38,165–66. The relaxation was implemented by OFAC in regulations on June 19, 2000. *Id*.

70. For example, compare the Executive Orders imposing the Iran embargo with the Executive order imposing the Iraq embargo. *Compare* Exec. Order No. 12,957, 60 Fed. Reg. 14,615, 14,615–16 (Mar. 17, 1995) (prohibiting transactions relating to Iranian petroleum resources), *and* Exec. Order No. 12,959, 60 Fed. Reg. 24,757, 24,757–59 (May 6, 1995) (prohibiting additional transactions with Iran), *and* Exec. Order No. 13,059, 62 Fed. Reg. 44,531, 44,531–33 (Aug. 19, 1997) (prohibiting additional transactions with Iran), *with* Exec. Order No. 12,722, 55 Fed. Reg. 31,803, 31,303 (Aug. 2, 1990) (prohibiting transactions with Iraq).

71. *E.g.*, 31 C.F.R. § 550.209 (listing prohibited transactions involving property in which the Government of Libya has an interest).

origin, and banking and financial transactions. OFAC normally defines U.S. persons to include U.S. citizens, permanent U.S. residents, and entities organized under U.S. jurisdiction, including foreign branches of U.S. companies.[72] However, some sanctions reach foreign subsidiaries of U.S. companies, and some do not.[73]

The Specially Designated Nationals (SDNs) program is a unique feature of OFAC sanctions. SDNs are entities or individuals determined by OFAC to be acting on behalf of sanctioned countries.[74] The regulations prohibit any transactions with such entities without a license,[75] and OFAC publishes a list of SDNs to put exporters on notice.[76]

OFAC sanctions can overlap with BIS restrictions. For instance, a transaction with an embargoed destination that is not covered by OFAC may be covered residually by BIS, and vice versa. The complexity, vagueness, and political volatility of the OFAC rules make compliance difficult. Additionally, OFAC has a significantly smaller staff than BIS. Given the "foreign affairs" basis for the restrictions that it enforces, it has not normally allowed public comment on proposed regulations or policies.[77] However, in early 2003, in an effort to increase the transparency of its enforcement deliberations, if not its substantive restrictions, OFAC issued for public comment proposed regulations providing details on OFAC's general basis for determining appropriate sanctions with respect to a particular violation.[78]

---

72. *E.g.*, *id.* § 560.314 (defining U.S. person for purposes of Iranian transaction regulations).

73. *Compare* 31 C.F.R. § 500.330 (stating a non-U.S. entity owned or controlled by U.S. persons is generally covered under foreign control assets regulations), *and* 31 C.F.R. § 515.329 (2003) (stating the same for the Cuban regulations), *with* 31 C.F.R. § 550.308 (stating that Libyan regulations do not cover foreign entities controlled by U.S. persons).

74. *See*, *e.g.*, 15 C.F.R. § 744.16 (2003).

75. *Id.*

76. 31 C.F.R. ch. V., app. A.

77. *Everything You've Ever Wanted to Know About OFAC*, EXPORT PRACTITIONER, Feb. 2001, at 8, 9.

78. Cuban Assets Control Regulations: Publication of Economic Sanctions Enforcement Guidelines, 68 Fed. Reg. 4422, 4425–26 (Jan. 29, 2003) (to be codified at 31

C. State Department

The State Department's Office of Defense Trade Controls (DTC) implements the International Traffic in Arms Regulations (ITAR)[79] to control exports of munitions-related merchandise, services, technology, and technical data. Items controlled by the State Department are included on the U.S. Munitions List (ML).[80]

As a general matter, technology and items are included in the ML when they are designed principally for military, as opposed to commercial, applications.[81] There often is a question as to whether an item is primarily commercial, and thus controlled by BIS, or primarily military, and thus controlled by DTC. In these cases, DTC has the statutory authority to decide which agency has jurisdiction, and DTC has been aggressive in asserting jurisdiction over items also claimed by BIS as within its jurisdiction.[82]

The DTC licensing process is viewed as less transparent and more restrictive than the BIS process, reflecting a chronic shortage of licensing staff, and a defense rather than business orientation.[83] DTC has a longstanding reputation in the business community as being non-transparent and inaccessible.[84] In 2000, DTC reluctantly agreed to undertake a wide-ranging reform initiative aimed at streamlining and rationalizing the licensing

---

C.F.R. pt. 501) (guidelines specific to Cuban sanctions are also listed and will be codified at 31 C.F.R. pt. 515).

79. 22 C.F.R. § 120.1.

80. *Id.* §§ 120.2, 121.1.

81. *Id.* § 120.3.

82. *Id.* § 120.4 (defining Commodity Jurisdiction); Amendments of the United States Munitions List, 67 Fed. Reg. 59,733, 59,733–34 (Sept. 23, 2002) (to be codified at 22 C.F.R. pt. 121) (determining "space qualified" items are under State Department jurisdiction).

83. *Munitions Export Licensing: Before the House Comm. On Int'l Relations*, 105th Cong. (2000) (statement of John Holmun, Senior Advisor to the Secretary of State for Arms Control and International Security).

84. *See* Maarten Sengers, *Moving Yet Standing Still: ODTC Crosses the Potomac*, EXPORT PRACTITIONER, June 2000, at 15, 15–16; *State Still Working on Reform Proposals*, EXPORT PRACTITIONER, June 2001, at 4, 4 ("Over the years, after all, State's Office of Defense Trade Controls (ODTC) had compiled an obstructionist record, stifling licensing reforms and other proposals for regulatory transparency.").

process.[85]

DTC also has been severely criticized for licensing delays despite a GAO finding that DTC processed substantially more license applications than BIS, with a significantly smaller staff, in comparable amount of time.[86] The most noteworthy criticism came in a GAO report issued at the end of 2001 in response to complaints from the U.S. defense industry and foreign government purchasers that the DTC process was "unnecessarily burdensome," and that "extended reviews of export license applications by the State Department are resulting in lost sales and are adversely affecting the nation's defense industry."[87] The GAO reported that DTC lacked important guidelines for internal and interagency review, lacked guidelines on the timing or tracking of license applications, and often viewed license reviews as low priority work.[88] DTC objected to the GAO criticism, and rejected the conclusions.[89]

A poignant illustration of the confusion caused by multi-agency involvement in the export control process is the treatment of satellites. In an effort to liberalize U.S. export controls after the end of the Cold War, in 1991 Congress transferred export licensing jurisdiction over a number of items from DTC to BIS.[90] Among the most significant items transferred were commercial encryption hardware and

---

85. *See State Announces License-Streamlining Proposals*, EXPORT PRACTITIONER, June 2000, at 11, 11–13; *State Still Working on Reform Proposals*, *supra* note 84, at 4–5.

86. LICENSE REVIEW TIMES, *supra* note 6, at 2–3.

87. GEN. ACCOUNTING OFFICE, GAO-02-203, EXPORT CONTROLS: REENGINEERING BUSINESS PROCESSES CAN IMPROVE EFFICIENCY OF STATE DEPARTMENT LICENSE REVIEWS 1 (2001).

88. *Id*. at 1–2.

89. *See id*. at 2 ("In commenting on a draft of this report, the State Department said that the report indicates a failure to comprehend how U.S. foreign policy provides the context for munitions export controls. The Department appears to have missed the point of our report."); *see also Securing the Cup*, EXPORT PRACTITIONER, Mar. 2002, at 4, 5 ("Infuriated with the GAO report, State lashed back. State complained that GAO's 'presentation of data was inflammatory and trivialized the licensing officer's role.' . . . The GAO appeared astonished by State's obstinate response.").

90. *See, e.g.*, Exec. Order No. 13,026, 61 Fed. Reg. 58,767, 58,767–68 (Nov. 15, 1996) (transferring jurisdiction over commercial encryption products from State Department to Commerce Department).

software[91] and communication satellites and "hot-section" technology.[92]

Subsequent events with respect to these two types of items illustrate the unpredictability of U.S. export controls. BIS export controls on encryption technology evolved from a highly complex and restrictive set of rules promulgated shortly after the transfer to BIS, to a liberalized and simplified framework whereby most commercial encryption can be shipped license free.[93] By contrast, as a result of a highly politicized debate regarding national security risks resulting from export control liberalization measures by the Clinton Administration, Congress reversed course and shifted jurisdiction over commercial communications satellites and related parts and technologies back from BIS to DTC.[94] In turn, this jurisdictional shift gave rise to confusion and interagency disputes regarding the scope of the re-transfer. The dispute lasted over two years.[95] In the meantime, companies whose products were affected by the interagency disputes suffered loss of business and other commercial damage because of protracted delays and confusion in the licensing procedures.[96] These delays were the result of an increased workload at DTC due to the shift, a lack of resources, and a lack of action on contested products and technology as the dispute was escalated to political levels and ultimately to the

---

91. *See infra* Part IV.

92. S*ee* Removal of Commercial Communications Satellites And Hot-Section Technology from State's USML for Transfer to Commerce's CLL, 61 Fed. Reg. 56,894, 56,894–95 (Nov. 5, 1996).

93. *See infra* Part IV.

94. Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, Pub. L. No. 105-261 §§ 1511, 1513–1514, 112 Stat. 1920 (codified as amended at 22 U.S.C. § 2778 (2000)); Amendments to the International Traffic in Arms Regulations (ITAR): Control of Commercial Communications Satellites on the United States Munitions List, 64 Fed. Reg. 13,679, 13,679–80 (Mar. 22, 1999) (to be codified at 22 C.F.R. pts. 121, 124).

95. *See* Licensing Jurisdiction for "Space-Qualified" Items and Telecommunications Items for Use on Board Satellites, 67 Fed. Reg. 59,722, 59,722 (Sept. 23, 2002) (to be codified at 15 C.F.R. pts. 740, 742, 744).

96. *See, e.g.*, Vernon Loeb, *U.S. Satellite Sales Lag Since Regulatory Shift*, WASH. POST, Mar. 28, 2000, at A21 ("U.S. satellite makers have lost significant market share to their European competitors since Congress transferred authority over export licensing from the Commerce Department to the State Department . . . .").

White House.

Another illustration of the complexity of the multi-agency jurisdiction over export controls is that the State Department, rather than OFAC, has jurisdiction over certain types of foreign-policy-oriented controls. In particular, the State Department has jurisdiction under the Iran and Libya Sanctions Act of 1996, which provides for sanctions against non-U.S. persons who knowingly make an investment over a threshold amount in the petroleum resources of Iran or Libya.[97] The State Department also has jurisdiction, under the Cuban Liberty and Solidarity Act of 1996—known as the Helms-Burton Act—with respect to the provisions requiring the U.S. government to deny U.S. entry to non-U.S. persons and entities that "traffic" in property confiscated from U.S. nationals by the Cuban government.[98]

D. Other Agencies

1. Nuclear Controls

U.S. controls on nuclear-related exports are aimed at furthering non-proliferation goals. The primary agencies that administer these controls are the Energy Department and the Nuclear Regulatory Commission (NRC). BIS and DTC also serve roles in regulating transfers of nuclear technology.

The Energy Department controls exports of technology and technical data that is directly or indirectly related to the production of "special" nuclear material outside the United States, which primarily concerns nuclear fuels such as plutonium and enriched uranium.[99] The Energy Department derives its authority from the Atomic Energy Act of 1954, as amended by Section 302 of the Nuclear Non-Proliferation Act of 1978.[100] The Secretary of Energy is authorized to permit nuclear-

---

97. Iran and Libya Sanctions Act of 1996, Pub. L. 104-172, 110 Stat. 1541 (1996); *see also* Additional Information for the Iran and Libya Sanctions Act, 61 Fed. Reg. 66,067, 66,067–68 (Dec. 16, 1996).

98. Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996, 22 U.S.C. § 6091 (2000).

99. 10 C.F.R. § 810.3.

100. *See* 42 U.S.C. §§ 2077, 2156–2158, 2201 (2000).

related technology transfers via a "general authorization" for less sensitive transactions that do not require prior approval,[101] or by "specific authorization" for more sensitive transfers.[102]

The Nuclear Regulatory Commission regulates exports of "peaceful" power-related nuclear material such as nuclear plants, nuclear reactor vessels, equipment, and components for reactors.[103] The NRC is authorized to control such transfers under the Atomic Energy Act.[104]

DTC is charged with regulating the export of technology related to nuclear weapons, and other technology deemed "classified,"[105] under authority of the Arms Export Control Act.[106] DTC's nuclear responsibilities are set forth in Category XVI of the ITAR.[107]

BIS controls exports of all other technology and technical data related to nuclear power.[108] BIS controls dual-use items enumerated on the Nuclear Referral List,[109] which sets forth commercial technology that may be used in sensitive nuclear-related end-uses. BIS also controls items for nuclear reasons even if they are not on the Nuclear Referral List if they are sold for nuclear-weapons related purposes.[110]

---

101. *See* 10 C.F.R. §§ 810.3, 810.7.

102. *Id.* §§ 810.8, 810.10.

103. *See id.* § 110.8.

104. *See* 42 U.S.C. §§ 2074, 2094, 2112, 2141 (2000). Only certain countries are eligible to receive nuclear-related exports, depending on their willingness to make and implement non-proliferation commitments. 42 U.S.C. §§ 2074, 2077, 2094, 2141; *see also* 42 U.S.C. § 2153 (2000) (explaining "terms, conditions duration, nature, scope, and other requirements"); 10 C.F.R. § 110 (explaining licensing procedures).

105. 22 C.F.R. §§ 122.1, 125.1 (2002).

106. *See* 22 U.S.C. 2751–2799aa-2; 22 C.F.R. §§ 122.1, 125.1.

107. 22 C.F.R. § 121.1 (2002). Category XVI covers nuclear weapons, design- and test-related equipment, as well as related technology and data. *Id*.

108. *See* 15 C.F.R. §§ 742.3, 744.2, 744.5.

109. BIS controls dual-use items on the Nuclear Referral List pursuant to the nuclear Non-Proliferation Act. 42 U.S.C. § 2139a(c) (2000); 10 C.F.R. § 110.2 (2002); 15 C.F.R. § 742.3. *See* 22 U.S.C. §§ 3201–3282 (2000). The Nuclear Referral List is incorporated into the CCL with the reason for control listed as "nuclear non-proliferation." BUREAU OF INDUS. & SEC., U.S. COMMERCE DEP'T, THE BXA FOREIGN POLICY REPORT TO CONGRESS (2002), *available at* http://www.bxa.doc.gov/press/2002/ForeignPolicyReport02/Default.htm (last visited Apr. 5, 2003).

110. *See* 15 C.F.R. § 742.3.

Because of the narrow and highly specialized nature of nuclear-related controls, this article will not further examine these controls.

2. Interagency Review and Consultation

Even when one agency exerts control over a particular type of technology or transaction, it often will consult with other agencies before rendering a licensing decision. This process can result in additional delay and unpredictability in the licensing process, as agencies often have different views on export control policy.

BIS license review process is subject to substantial interagency review. Executive Order 12981 states that BIS must send license applications to the Departments of State, Defense, and Energy, as well as the Arms Control and Disarmament Agency.[111] The Executive Order was designed to streamline the process by imposing time limits on interagency review that presume no objection if the reviewing agency does not take some action within thirty days. However, any questions or objections posited by any of the reviewing agencies within this thirty day time frame can substantially delay or prevent an export.

The Executive Order also established a working level Operating Committee chaired by BIS, and comprised by members of the reviewing agencies, to consider and resolve disputes and disagreements among the agencies. BIS has the deciding vote on the Operating Committee through its appointment of the chairperson, but its decisions may be appealed to the higher level Advisory Committee on Export Policy, which acts by majority vote.[112] Appeals from this body

111. Exec. Order No. 12,981, 60 Fed. Reg. 62,981, 62,981 (Dec. 5, 1995).

112. *Id*. BIS must also consult with the State Department, the Defense Department, the Energy Department, and the Nuclear Regulatory Commission in deciding on items on the Nuclear Referral List. *See* 42 U.S.C. § 2077 (2000). The Energy Department must obtain the concurrence of the State Department before authorizing certain exports of nuclear technology, and must consult with the Nuclear Regulatory Commission and the Defense Department and Commerce Department. *Id*. The Nuclear Regulatory Commission also must consult with these executive branch agencies pursuant to its licensing activities. *See* 10 C.F.R. §§ 110.40–.41 (2003). Depending on the type of technology or destination involved, other agencies can be involved in the review and consultation process. *See, e.g.*, *infra* note 127.

may be made to the cabinet level, although such appeals are rare.

3. Defense Department Involvement in the Interagency Process.

The Defense Department plays an important role in BIS and DTC licensing processes. As may be expected, the Defense Department takes a conservative, security-oriented posture, and is much less concerned with the effect of license denials on U.S. exporters.[113] Defense license reviewers can call for denial of a particular license, or can insist upon rigorous, restrictive conditions on the granting of the license. Many exporters have complained about delays in the BIS licensing process due to delays in the interagency review process, primarily review by the Defense or State Department.[114]

DTC at the State Department is a small office that often relies on, and is influenced by, the conservative views of the Defense Department, that naturally has a role in overseeing munitions exports. DTC consults with the Defense Department in reviewing the scope of the Munitions List and in setting licensing policy.[115] When there is confusion as to whether DTC or another agency is vested with authority over a particular export, DTC is empowered to determine the competent agency. Companies uncertain as to the proper authority controlling a particular technology transfer or export may submit a jurisdiction clarification request to DTC.[116] DTC will consult with the Defense Department and other agencies prior to making a decision.

113. *See* Donald H. Caldwell, Jr., Note, *The Export Administration Amendments Act of 1985: A Reassessment and Proposals for Further* Reform, 19 VAND. J. TRANSNAT'L L. 811, 848–49 (1986).

114. *See, e.g.*, *Defense Staff Claim They Meet Export Licensing Deadlines*, WASH. TARIFF & TRADE LETTER, Aug. 19, 2002, at 1.

115. 22 C.F.R. §120.2 (2002).

116. *Id.* § 120.4.

IV. CONTROLS ON TECHNOLOGY

[T]he U.S. is the most aggressive country in the world in controlling exports.

-John Holum
State Department official[117]

A. BIS Controls

1. Scope of Controls

a. Items Subject to the EAR

The scope of coverage of the EAR is extremely broad. All merchandise and technology within the scope are potentially subject to licensing requirements. The scope includes the following: (1) all commodities, technology, and software *in the United States*;[118] (2) all *U.S. origin* commodities, technology, and software *wherever located*;[119] (3) U.S. origin commodities *incorporated into foreign made products,* U.S. technology *commingled with* foreign technology, and U.S. software *commingled* with foreign software, respectively, in quantities exceeding de minimis levels;[120] (4) certain foreign-made direct products *based on U.S. origin technology or software* when shipped to certain destinations.[121]

Within this broad jurisdictional spectrum, only certain goods and technology are actually restricted pursuant to the requirements of the CCL and EAR.[122] Others are not restricted

117. *Senate Presses for Wassenaar Breakthrough, supra* note 40, at 4.

118. 15 C.F.R. § 734.3(a)(1) (2003).

119. *Id.* § 734.3(a)(2).

120. *Id.* § 734.3(a)(3). U.S. origin merchandise technology and software are excluded from controls if incorporated into non-U.S. merchandise, technology, and software, respectively, if the U.S. content is less than 25% (only 10% in the case of embargoed countries). Certain items such as encryption items and computers above specified thresholds do not qualify for the de minimis exceptions. *Id.* § 734.4.

121. *See id.* § 734.3(a)(4).

122. *See, e.g., id.* § 734.3 (detailing items subject to the EAR and those excluded

or are subject to license exceptions.[123] Controls on software and technology, which are intangibles and may be transferred or "exported" in non-traditional ways, present special challenges to exporters.[124]

Technology not subject to the EAR includes: (1) items that are exclusively controlled for export or re-export by other U.S. government agencies;[125] and (2) publications, informational materials, and "publicly available" technology and software, except for encryption software. [126] One category of publicly available technology is technology generally accessible to the public in patents and open (published) patent applications available to any patent office.[127]

b. "Exports" and "Re-exports"

An important concept in technology export control is that technology may be "exported," and thus subject to control, by transmission on the internet, by traveling abroad with software on a laptop, by allowing persons outside the United States to access data, files and libraries through the company's network, and by releasing information to foreign nationals in the United

---

from the EAR).

123. *See id.* § 734.2(a); *id*. § 730.7.

124. *See id*. § 734.2(b). The EAR define technology as specific information necessary for the "development," "production," or "use" of a product. *Id.* § 772.1. Information may take the form of technical data or technical assistance. *Id.* Technical assistance may take forms such as blueprints, plans, diagrams, formulae, tables, engineering designs and specification manuals, and instructions written or recorded on other media or devices. *Id.* Software is defined as a collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression. *Id.*

125. *Id.* § 734.3(b)(1).

126. *Id*. § 734.3(b)(2)–(3).

127. *Id.* § 734.7(a)(3). All U.S. patent applications are screened initially by the U.S. Patent & Trademark Office (PTO) and, if necessary, by BIS, State Department, and Defense Department, to determine whether publicly available treatment could affect national security. If this determination is affirmative, a secrecy order is applied and the technology is made subject to controls even after it is patented. *See id.* § 734.3(b)(1)(v). As a separate matter, the PTO, not BIS, administers the licensing of (1) exports of technology in patent applications for filing in foreign countries, (2) technology contained in a patent application derived wholly from foreign origin technical data for execution by a foreign inventor and subsequent filing with the PTO, and (3) information in a patent application sent to a foreign inventor for his signature. *See id.* §§ 734.3(b)(3)(iv), 734.10.

States, as well as the traditional manner of shipping hardware or disks abroad.[128] Companies involved in technology transfers also need to be aware that obligations under U.S. law to comply with export control regulations do not end at the U.S. border.

In addition to controlling traditional exports from U.S. ports to foreign destinations, the EAR applies controls to many transactions outside the United States. These transactions include: (1) the re-export or further transfer of U.S. origin technology and merchandise;[129] (2) the re-export from abroad of foreign origin products, technology, and software containing more than a de minimis amount of controlled U.S. origin content;[130] and (3) the re-export from abroad of foreign products produced with any level of controlled U.S. origin technology.[131] These additional, extraterritorial controls can complicate transactions, pose liability risks for unwary exporters, and often operate as a disincentive for foreign buyers to select U.S. vendors if, as often occurs, the U.S. controls are unilateral and the technology is readily available from third countries.

Some countries that are frequent re-exporters of U.S. products have objected to the unfairness of U.S. re-export controls on the grounds that the overseas re-exporter typically lacks information as to whether the U.S. technology, product, or component is subject to re-export licensing requirements, and the U.S. exporter often does not provide sufficient information.[132]

c. Deemed Export

U.S. companies should be aware that controlled transactions may occur when they hire foreign nationals and allow them access to controlled technology. This type of transfer is termed a "deemed export" because the foreigner's access to the controlled technology is deemed to be a restricted transfer to the foreigner's

128. *See id.* § 734.2(b).

129. *Id.* § 736.2(b)(1).

130. *Id*. § 736.2(b)(2).

131. *Id*. § 736.2(b)(3).

132. *See, e.g., Japanese Companies Escalate Campaign Against Re-export Controls*, EXPORT PRACTITIONER, May 2000, at 6, 6–7 (indicating Japanese industry's frustration with U.S. re-export requirements).

country of citizenship.[133] As the demand for technologically skilled workers increases and labor shortages in critical areas such as engineering worsen, the U.S. demand for foreign-born workers will continue to grow. The deemed-export controls therefore will ensnare a growing list of companies, some of whom do not view themselves as exporters. Indeed, deemed-export applications have been on the increase,[134] as have BIS enforcement efforts.[135]

Although the EAR did not explicitly set forth a deemed-export rule until 1996,[136] BIS has traditionally taken the position that transfers of controlled technology to foreigners in the United States are subject to restriction. The transfer to any foreign national of any technology controlled by the United States for export to that foreign national's home country thus requires prior authorization by BIS (or the State Department as the case may be).[137] The deemed-export rule applies only to exports of technology or software and not to transfers of commodities. The term "foreign national" under the deemed-export rule includes temporary immigrants, including persons in the United States under H-1 and H-2 visas, but does not apply to permanent residents.[138]

Exports of technology for purposes of the deemed-export rule may take place by any means of communication including

---

133. 15 C.F.R. § 734.2(b)(2)(ii).

134. *Compare* GEN. ACCOUNTING OFFICE, GAO-02-972, EXPORT CONTROLS: DEPARTMENT OF COMMERCE CONTROLS OVER TRANSFERS OF TECHNOLOGY TO FOREIGN NATIONALS NEED IMPROVEMENT, 9 & n.8 (Sept. 2002) [hereinafter TRANSFERS TO FOREIGN NATIONALS] (noting there were 923 applications for deemed-export licenses in 2001), *with Inside BXA*, *supra* note 6, at 24–25 (noting there were 800 applications for deemed-export licenses in 1999).

135. *See Exporters Want Assurances on Deemed Export Investigations,* WASH. TARIFF & TRADE LETTER, Jan. 6, 2003, at 2–3 [hereinafter *Exporters Want Assurances*].

136. Simplification of Export Administration Regulations, 61 Fed. Reg. 12,714, 12,747 (Mar. 25, 1996) (to be codified at 15 C.F.R. ch. VII).

137. *See* 15 C.F.R. § 730.2 (2003); *see also* 15 C.F.R. § 734.2. The State Department also has a deemed-export rule. *See* 22 C.F.R. § 120.17(a) (2002) (stating that pursuant to this section of the ITAR, the definition of export includes: "(4) Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or (5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.").

138. *See* 15 C.F.R. §734.2(b)(2)(ii); *see also* 22 C.F.R. § 120.16 (2002).

telephone conversations, fax communications, training sessions, briefings, or plant tours. Providing a foreign national with access to a computer system, which may contain files or libraries with controlled technology, may also be deemed a restricted transfer, even if the foreign national's job would not involve such files. Exports of technical data also may occur through licensing or joint venture arrangements, or even a U.S. person's use of technical expertise abroad if that expertise was acquired in the United States.

The complexity of the deemed export regulation, and the intangible, amorphous nature of deemed transfers, pose special hazards and difficulties for U.S. companies seeking to develop compliance measures. One area of particular difficulty concerns the increasing use of internal company e-mail servers, or intranets, where proprietary data is shared among employees, and broad company computer networks where a foreign national may gain access to controlled data and files. To address these situations companies need to implement special screening procedures.[139] Another challenge concerns longer-term foreign nationals, who may be screened upon hiring, but then who may later gain access to additional technology through promotion or assignment to different projects.

Despite these compliance difficulties, BIS has increased its enforcement efforts, and thus, U.S. companies would be well-advised to take special measures to comply. Enforcement concerns were raised in 1999 when it was discovered that BIS processed 783 deemed-export license applications, although there were 115,000 visas issued to foreign nationals to work in the high-tech sector—raising concerns that many of the visa holders should be, but were not, operating under deemed-export licenses.[140] The GAO issued a report critical of BIS's enforcement of the deemed-export requirements, and strongly recommended that BIS significantly strengthen its enforcement of the deemed-export requirements.[141] In response, BIS has increased its

---

139. *See Deemed Export Rules Imposing Extra Burdens on Firms*, WASH. TARIFF & TRADE LETTER, Nov. 20, 2000, at 3.

140. *Report Attacks Commerce's Deemed Export Rule*, EXPORT PRACTITIONER, June 2000, at 6, 6.

141. *See* TRANSFERS TO FOREIGN NATIONALS, *supra* note 134, at 16–17.

enforcement effort, and announced that it will be conducting post-licensing inspections of deemed-export license holders.[142] BIS announced its first criminal indictment for a deemed-export violation in late 2000.[143]

When particular technology requires an export license for transfer to a foreign national's country of origin, companies must apply for an export license before controlled technology, know-how, or software is released. License applications must include information to assist BIS in deciding whether the technology at issue is likely to be transferred to the foreign national's home country, or whether it will remain in the United States.[144] As a general matter, BIS is likely to approve a license application if the technology in question would be approved for export directly to the foreign national's home country. Nevertheless, deemed-export applications are subject to interagency review, and often are plagued by delays, and by conditions that limit the work the foreign national may do.[145]

BIS created a "Special Comprehensive License" for transfers of technology to foreign nationals, as an alternative to the case-by-case approach of obtaining deemed-export licenses.[146] This special license can be issued on a company-wide basis, and sets forth the level of technology to which foreign workers at the company could have access, any nationalities that would be ineligible, and any other restrictions. Companies holding the special license would be able to hire foreign nationals without prior BIS approval, and would then submit the foreign workers' names and personal information to BIS for screening. This raises the prospect of having to transfer or terminate an employee to whom BIS subsequently denies access. The license

---

142. *See Exporters Want Assurances, supra* note 135, at 2.

143. *See BXA Gets First Indictment for Deemed Export Violation*, WASH. TARIFF & TRADE LETTER, Oct. 23, 2000, at 1.

144. *See* BXA OFFICE OF CHEMICAL AND BIOLOGICAL CONTROLS AND TREATY COMPLIANCE, GUIDELINES FOR PREPARING EXPORT LICENSE APPLICATIONS INVOLVING FOREIGN NATIONALS, *available at* www.bxa.doc.gov/DeemedExports/foreignationals.pdf (last visited Apr. 5, 2003).

145. *Deemed Export Backlog Eases, but Conditions Remain a Problem*, WASH. TARIFF & TRADE LETTER, July 22, 2002, at 1.

146. *See* 15 C.F.R. § 752.1 (2003); *BXA Plans to Move Quickly on Deemed Export Changes*, WASH. TARIFF & TRADE LETTER, June 19, 2000, at 1.

is tailored for companies that hire many foreign nationals, but imposes special burdens on them.[147]

Ironically, issuance of the deemed-export rule in written form was in response to the business community's frequent requests to BIS to issue bright-line standards for technology transfers to foreign nationals.[148] The same business community now finds the deemed-export rule hard to live with. In addition to the license delays, restrictive conditions, and compliance difficulties noted above, the rule also has had unintended effects, detrimental to business.

One such effect relates to foreign students. Publicly available technology, such as that gleaned from university research, is freely transferable to foreign nationals although proprietary business technology is not.[149] Consequently, after foreign students imbued with cutting-edge technical knowledge earn their Ph.D.s in the United States, they often are forced to take this knowledge back to their home country because U.S. businesses may have difficulty obtaining authorization to hire them due to deemed-export restrictions. It is difficult to discern how this policy serves long-term U.S. interests.

2. License Requirements and Exemptions

a. Analyzing License Requirements

In order to ensure compliance with regulatory controls, companies must make sure they understand and can apply the often arcane rules that determine whether a particular transfer requires a license. Under the amended EAR, licenses entail permission obtained after application to BIS. The EAR contains numerous "license exceptions." If a given transfer qualifies for a license exception, it is not necessary to apply for export authorization.

---

147. *BXA Plans to Move Quickly on Deemed Export Changes*, *supra* note 146, at 1.

148. The prior standard restricted "any release of technical data in the United States with the knowledge or intent that the data will be shipped or transported from the United States to a foreign country." 15 C.F.R. § 779.1(b)(ii) (1994). This provision was amended in 1994 to restrict "any release of technology or source code subject to the EAR to a foreign national." *Compare id.*, *with* 15 C.F.R. § 734.2(b)(2)(ii) (2003).

149. *See* 15 C.F.R. § 734.3(b)(3).

The first step in determining whether a license is required is to determine whether a "general prohibition" applies to a transaction.[150] If a general prohibition applies, a license is required unless a license exception applies.

b. License Exceptions

The second step is to analyze the availability of license exceptions. License exceptions permit exportation without prior authorization based upon the circumstances of a particular transaction, not the particular commodity involved or its destination.[151] It is important to check the availability of all

---

150. *See id.* §732.1(c).

General Prohibition 1: exports and re-exports of controlled items (items on the CCL) to specified countries for which a license requirement is noted explicitly on the CCL.

General Prohibition 2: re-exports of foreign-made items incorporating more than a de minimis amount of controlled U.S. content.

General Prohibition 3: re-exports of foreign-produced direct product of U.S. origin technology or software.

General Prohibition 4: exports or re-exports to parties subject to a denial order.

General Prohibition 5: *knowing* exports or re-exports to prohibited end-uses and end-users.

General Prohibition 6: exports or re-exports to embargoed or special destinations.

General Prohibition 7: activities or involvement by U.S. persons in any transaction related to the proliferation of weapons of mass destruction or missile delivery systems.

General Prohibition 8: in-transit shipments and items to be unladen from vessels or aircraft intended for specific controlled destinations.

General Prohibition 9: violation of the terms of a license or of a license exception or any other order issued pursuant to the EAR.

General Prohibition 10: proceeding with any transaction with knowledge that a violation has occurred or is about to occur.

Id. §736.2(b) (emphasis added); *see also id.* § 732.1(d)(1). General Prohibition 5 applies to exports/re-exports of all items subject to the EAR, not only those on the CCL. These are so-called "catch-all" controls. A license is required if an exporter knows that merchandise or technology is going to a weapons proliferation related end-use or end-user. In addition, BIS may "inform" exporters either individually or by public notice that certain end-users may not receive certain items without a license. The burden is on the exporter to "know" his end-user. *See id.* § 732 (Supp. 3 2003).

151. *See id.* § 740.1(a). License exceptions are set forth at Part 740 of the EAR. *See id.* § 740.1–.18.

possible license exceptions as well as any stated limitations to their availability. A number of the license exceptions specifically applicable to transfers of technology and software are referenced below.

3. Coverage of Technology and Software

The EAR defines technology to include both the tangible and intangible.[152] The term comprises tangible technical data, such as blueprints and manuals, and intangible technical assistance, such as oral instruction and the application of technical know-how. In addition to understanding the complexities of determining what is controlled, companies engaged in technology transfers also must understand what is not controlled. Technology and software are free from license requirements under the EAR if published and publicly available. This includes material released at an open conference and software that is available for general distribution free of charge or at no more than the cost of reproduction and distribution.[153]

The EAR sets out concepts and rules expressly devoted to technology and software. A number of these are discussed below.

a. The General Technology Note (GTN)

The GTN provides that the export of technology "required" for the "development," "production," or "use," of merchandise or technology on the CCL is controlled according to the specific CCL technology category that covers the technology at issue.[154] It is important to note that whereas some technology categories on the CCL may cover technology for the development, production, and use of particular commodities, others may not cover all three categories. For example, ECCN 1E001 covers technology for the development and production of certain items, but does not cover use technology. The distinctions among ECCN technology categories reflect substantive decisions to cover the defined technologies and not others.

Another important aspect of the GTN is that technology

152. *See* 15 C.F.R. § 772.1 (2002).

153. *Id.* § 734.7.

154. *See id.*

required for the development, production, or use of a controlled product remains controlled even when applicable to a proposed transfer in connection with uncontrolled products.[155] For example, an item of know-how may be necessary in the manufacturing process used to make a product that requires a license before it can be exported. The same know-how may be used in the manufacturing process to make an uncontrolled product. Pursuant to the GTN, because the technology is necessary for a controlled product, the associated know-how also will be controlled and its exportation will require a license**,** even if the recipient intends to use the know-how to make the uncontrolled product.

b. License Exceptions for Technology and Software

There are four distinct ways to qualify for License Exception Technology and Software Unrestricted (TSU).[156] The exception applies to (1) software that is publicly available; (2) technical information related to sales and operation of high-tech products; (3) technology that is necessary for the installation, operation, and repair of lawfully exported products; and (4) software "bug fixes" that do not enhance functional capacity.[157]

- *TSU for Mass-Market Software.*

This authority is available for so-called "mass-market" software that satisfies the requirements of the General Software Note to the EAR.[158] The theory behind this exception is that if software is widely available to the public, it is in fact uncontrollable. In order to qualify for mass-market software treatment under the General Software Note, software must be available to the public and be sold from stock at retail selling points, without restriction, by means of over-the-counter transactions, mail order transactions, or telephone call transactions; and designed for installation by the user without

155. *Id.* pt. 774 (Supp. 2 2003).
156. *Id*. § 740.13(a)–(d).
157. *Id*.
158. *Id.* pt. 774 (Supp. 2 2003).

further substantial support by the supplier.[159] This exception may be used for transfers to all destinations except for embargoed destinations.

- *TSU for Sales Technology*

Sales technology is data used to support a prospective or actual quotation, bid or offer to sell, lease, or otherwise supply an item.[160] Only technology that is customarily provided to potential customers is eligible. The "sales" information may not be so detailed that it will disclose design, production, or manufacturing technology, or permit buyers to reduce the technology to production.[161]

- *TSU for Operation Technology and Software*

Operation technology is the minimum technology necessary for the installation, operation, maintenance, and repair of products that have been lawfully exported either under a license or a license exception. The minimum necessary does not include technology for development or production, and includes use technology only to the extent required to ensure safe and efficient use of the product.[162] Operation technology may be exported or re-exported to any destination where the equipment for which it is intended is legally exported or re-exported. This authority does not permit the export of software that increases the performance levels of the products they support. License Exception TSU for operation technology and software permits exports or re-exports by parties other than the exporter of the related commodity.

- *TSU for Software Updates (Bug Fixes)*

This exception is intended for the correction of software errors.[163] Such bug fixes may not enhance the functional capacity of the original software previously exported. This authority

159. *Id.*
160. *Id.* § 740.13(b)(1).
161. *Id*. § 740.13(b)(2).
162. *Id*. § 740.13(a)(1).
163. *Id*. § 740.13(c).

permits all exports and re-exports to any destination where the original software was lawfully exported or re-exported.

The other principal license exception for technology and software is License Exception Technology and Software Under Restriction (TSR). This exception permits more sensitive technology, covered by national security controls, to be exported to countries in Country Group B if the exporter or re-exporter obtains a written assurance from the customer that he will not transfer the technology to a country subject to national security controls or to the nationals of such a country.[164] Country Group B includes all the principal allies of the United States as well as a number of other countries, including ex-Soviet Bloc countries, no longer considered national security threats.

c. De Minimis Exception for Technology and Software

In 1996 the EAR was amended to exempt from U.S. controls re-exports of foreign-origin technology and software with only minimal or de minimis U.S. origin technology or software content.[165] Previously, the de minimis rules applied only to commodities, not to technology and software. The U.S. formerly would control technology and software exports, regardless of the extent to which they became commingled with foreign-origin technology or software. Thus, expansion of de minimis treatment to technology and software was a liberalization of technology and software controls. Under the new rule, however, companies who wish to avail themselves of the de minimis rule for technology transfers must file a one-time report to BIS as a precondition for using the exclusion.[166] The report to BIS must disclose the methodologies for calculating the value of the U.S. origin content and the applicability of the exception. If a reporting company is not contacted within thirty days of filing this report, the company is entitled to rely on its calculations.[167]

The standards for de minimis treatment are as follows: foreign technology or software with ten percent or less controlled

164. *See id*. § 740.6.
165. *Id.* § 734.4(c).
166. *Id.* § 734(b)(1) (Supp. 2 2002).
167. *Id*. § 734(b)(5).

U.S. technology is not subject to the EAR regardless of the country of destination;[168] foreign technology or software with less than twenty-five percent but more than ten percent controlled U.S. technology by value is not subject to the EAR except for exports to countries considered terrorist-supporting countries[169] or embargoed countries;[170] and foreign technology or software with more than twenty-five percent U.S. origin content has more than de minimis U.S. content and is not exempt.[171]

The de minimis exclusion for technology and software does not apply to technology or software incorporated into foreign made hardware.[172] BIS is in the process of deriving a de minimis rule applicable in these circumstances.[173]

4. Encryption Controls

The recent attempts to regulate encryption technology and software illustrate the volatile and often unpredictable nature of export controls that affect new and evolving technologies. In the case of encryption, however, the changes provide some grounds for optimism. The trend has been decontrol rather than additional control. This is not to suggest that export controls on commercial encryption products have been eliminated entirely. Even where the requirement of an export license is dispensed, BIS will continue to impose significant pre- and post-export reporting requirements. The encryption debate provides a useful lesson to exporters: even where controls have been reduced, exporters are still subject to control, and must continue to be vigilant to ensure compliance with those requirements that remain.

---

168. *Id*. § 734.4(c).

169. *Id*. § 734.4(c)–(d); s*ee id.* § 742.1 (listing countries considered terrorist supporting countries).

170. *Id*. pt. 746 (2002); s*ee id.* pt. 734 (Supp. 2 2003) (noting the "Calculation of Values for De Minimis Rules" for calculation methodologies).

171. *See id*. § 734.4.

172. *Id*. (citing 15 C.F.R. pt. 774 (Supp. 1 2003)).

173. *De Minimis Rule for Software Gets General Approval*, WASH. TARIFF & TRADE LETTER, June 19, 2000, at 3.

a. The Original Plan

Encryption technology allows businesses and individuals to put data in code to ensure confidentiality of communications.[174] With the explosion of e-mail and e-commerce, the government's attempts to restrict transfers of encryption software were a major hindrance not only for technology companies, but also for mere users of encryption.

The Clinton Administration at first sought to heavily regulate encryption transfers, introducing on October 1, 1996 a plan to safeguard electronic communications for national security and public safety purposes. The key feature of the initial Clinton plan was its requirement of mechanisms to allow authorized law enforcement or national security agencies to decipher and otherwise "recover" the plaintext of encrypted data and communications without the knowledge of the encryption user.[175] Under this rigid plan, exports and re-exports of encryption products without these key recovery features required a license *to all destinations except Canada*.[176] "Export" means any transfer outside the United States or to a foreign national, whether physically on a disk or electronically through computer links.[177] The plan specified three licensing policies for encryption products.[178]

---

174. Encryption permits transformation of passwords or messages into a form that cannot be understood without access to special information necessary to decode the password or message. Messages are scrambled by application of a mathematical algorithm. The algorithm allows the user to select a key. The key allows the user to decrypt messages. Encryption strength increases with the length of the key. Key length is generally measured in bits. Bernadette Barnard, Note, *Leveraging Worldwide Encryption Standards Via U.S. Export Controls: The U.S. Government's Authority to "Safeguard" the Global Information Infrastructure*, 1997 COLUM. BUS. L. REV. 429, 433–35 (1997).

175. Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,574 (Dec. 30, 1996). The plan also involved the transfer to BIS of jurisdiction to administer most encryption controls which formerly was held by the State Department Office of Defense Controls. *Id*.

176. *See id*.

177. 15 C.F.R. § 734.2(b)(9).

178. *See* Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. at 68,573–74. The plan also provided exemption from normal license application requirements for various categories of products. *See id*. The three licensing policies were:

The Clinton Administration introduced the plan with much fanfare, conveying the impression of a significant liberalization of encryption export controls. It soon became apparent, however, that the new policy was not much of liberalization at all; it continued to hamstring the U.S. software industry in the global marketplace. Neither private industry, nor the government agencies actually imposing the controls, appeared to comprehend the details of how a key recovery system should or could be implemented. The software industry strongly opposed the plan, stating that it would impede the competitiveness of the U.S. industry in this sector, by favoring competitors in countries not subject to similar restrictions.[179] First Amendment advocates also challenged the restrictions.[180]

- Certain Mass-Market Encryption Software.
  Subject to a one-time BIS review, the exemption was made available for "general use" software, in other words, off-the-shelf software for self-installation with encryption less than 40 bits Data Encryption Service (DES) in key length;
- Key Escrow, Key Recovery, and Recoverable Encryption Software and Commodities.
  Exporters were required to submit a classification request to BIS spelling out: (1) a key recovery agent satisfactory to BIS; (2) satisfactory security policies to safeguard the keys or other recovery information; and (3) that government officials were permitted to obtain the encrypted data without the knowledge of the encryption user. If BIS was satisfied that the plain text of the encrypted communication was accessible to the government without the knowledge or participation of the encryption user, then the exception applied without limit to the bit length of the encryption key.
- Non-Recovery Encryption Items up to Fifty-Six Bit Key Length DES.
  The plan provided for a two-year window or transition period, but only for export and re-export of non-recovery encryption products with keys of up to fifty-six bit key length DES, after a one-time review, and only after the exporter submitted to BIS a satisfactory business and marketing plan providing a detailed explanation of the steps the company would take to adopt a key or other recovery system.

179. Rajiv Chandrasekaran, *Software Firms Call U.S. Plan on Encryption 'Unworkable'*, WASH. POST, Dec. 11, 1996, at C15; *see Encryption Policy Challenged*, CNET News.com, Dec. 4, 1996 *at* http://news.com.com/2100-1023-252068.html?legacy=cnet.

180. *See, e.g.*, Bernstein v. U. S. Department of Justice, 176 F.3d 1132 (9th Cir. 1999) (stating case of a mathematician who is challenging export controls as limiting his free speech to distribute his encryption software).

b. Confrontation and Compromise

Under withering criticism, the Clinton Administration announced in September 1998 that it was updating its encryption policy to liberalize controls with respect to certain commercial sectors and to loosen controls for recoverable encryption products.[181] The revised plan nevertheless was criticized as overly restrictive and unrealistic.

The revised plan still insisted on key recovery mechanisms and freed only low-level encryption products, those with fifty-six bit key length, from any key recovery feature requirements.[182] In particular, the plan permitted transfer of higher level encryption to a list of specified countries only if it was "recoverable" pursuant to Encryption License Agreements (ELA).[183]

The Clinton Administration finally abandoned the key recovery concept in September 1999,[184] announcing dramatic changes that BIS implemented in January 2000.[185] The January 2000 changes represented a significant liberalization and simplification of encryption controls.[186] For most standard types

---

181. Press Release, Office of the Press Secretary, The White House, Administration Updates Encryption Policy (Sept. 16, 1998), *available at* http://www.cdt.org/crypto/admin/ whousepress091698.html.

182. Encryption Items, 63 Fed. Reg. 72,156, 72,156–57 (Dec. 31, 1998) (to be codified at 15 C.F.R. pt. 750). The revised plan also provided for sectoral liberalization, decontrolling encryption transfers for encryption products associated with banks and financial institutions to certain countries, to health and medical sectors excluding biochemical and pharmaceutical producers, and subsidiaries of U.S. companies in all destinations except embargoed countries. *Id*. at 72,156–57.

183. S*ee* Encryption Items, 63 Fed. Reg. at 72,156, 72,158 (Dec. 31, 1998). ELAs are arrangements that permit exports and re-exports of encryption items and equipment to specified destinations. 15 C.F.R. § 750.7(2)(i) (2003).

184. *See* Press Release, Office of the Press Secretary, The White House, Administration Announces New Approach to Encryption (Sept. 16, 1999) [hereinafter Administration Announces New Approach], *available at* http://www.cdt.org/crypto/CESA/whousepress091699.shtml.

185. Revisions to Encryption Items, 65 Fed. Reg. 2492, 2492 (Jan. 14, 2000) (codified at 15 C.F.R. pts. 734, 740, 742, 770, 772 and 774). The revised regulations, which were issued as an interim final rule, went into effect on January 14, 2000. *Id*.

186. *See* Press Release and Fact Sheet, U.S. Dep't of Commerce, Commerce Announces Streamlined Encryption Export Regulations (Jan. 12, 2000), *available at* http://www.globalsecurity.org/intell/library/news/2000/01/000113-crypto-bxa.htm; Administration Announces New Approach, *supra* note 184; *see also* Rebecca Christie, *U.S. Limbers up for Encryption Sales: Companies Are Cheered as Rules Are*

of encryption, the regulations eliminated the restrictions on key length and the requirement of an export license.[187] The regulations also eliminated the need for a key recovery mechanism.[188] Further liberalizations of the encryption export regulations were implemented in October 2000[189] and June 2002.[190] The principal features of these liberalizations are summarized below. The complex technical details regarding implementation are contained in the corresponding Federal Register notices.

- *January 2000 Changes*[191]

Exports to Non-Government End-Users

Encryption software of any key length may be exported under a license exception to all non-government end-users, except in the seven embargoed or terrorist-supporting destinations—Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. A one-time technical review by BIS is required, however. The previous liberalization for banks and financial institutions is essentially superceded by this new broader exemption. Exports to government end-users require a license.

Eased on Exporting Privacy Software, FIN. TIMES (London), Jan. 18, 2000, at 9 (noting that regulations "mark a departure from the way encryption exports have been regulated"); Behnam Dayanim, *New Encryption Export Rules: Uncle Sam Says 'Uncle'*, LEGAL TIMES, Apr. 3, 2000, at 26; Margret Johnston, *Encryption Export Controls Are Relaxed*, INFOWORLD, Jan. 17, 2000, at 10, 10.

187. *See* Dayanim, *supra* note 186, at 26.

188. *See* Administration Announces New Approach, *supra* note 184.

189. Revision to Encryption Items, 65 Fed. Reg. 62,600, 62,600 (Oct. 19, 2000); INFORMATION TECHNOLOGY CONTROLS DIV., U.S. DEP'T OF COMMERCE, ENCRYPTION FACT SHEET (Oct. 19, 2002), *at* http://www.bxa.doc.gov/Encryption/ 19Oct2KFactsheet.html.

190. *See* Revisions and Clarifications to Encryption Controls in the Export Administration Regulations, 67 Fed. Reg. 38,855, 38,855 (June 6, 2002); *see also* INFORMATION TECHNOLOGY CONTROLS DIV., U.S. DEP'T OF COMMERCE, U.S. ENCRYPTION EXPORT CONTROL POLICY FACT SHEET (June 6, 2002), *at* http://www.bxa.doc.gov/ Encryption/EncFactSheet6_17_02.html.

191. Revisions to Encryption Items, 65 Fed. Reg. 2492, 2492–93 (Jan. 14, 2000) (codified to amend 15 C.F.R. pts. 734, 740, 742, 770, 772, and 774).

Retail Encryption Products

Retail encryption commodities and software may be exported to both non-government and government end-users, except in terrorist and embargoed destinations. BIS determines which products qualify as retail by means of a review of the products' functionality, sales volume, and distribution patterns. In the broadest sense, retail encryption products are those widely available.

Internet and Telecommunications Service Providers

Telecommunications and internet service providers are authorized to obtain and use any encryption product, under license exception, to provide encryption services. Provision of such services to government end-users will require a license.

Source Code

Encryption source code that is available to the public may be exported under license exception without the need for a formal technical review. Instead, the exporter must submit to BIS a copy of the source code or a written notification of its location on the internet. This treatment should cover most open source encryption software.

U.S. Subsidiaries

All encryption items, regardless of key length, are authorized for export or re-export to foreign subsidiaries of U.S. entities without the need for BIS technical review. Foreign nationals are authorized to work for U.S. companies on encryption issues without the need to obtain an export license. However, items produced with encryption commodities exported under this exception may require technical review.

Post-Export Reporting

Post-export reports are required for exports to non-U.S. entities of encryption products above sixty-four bits, except for finance-specific products or retail products exported to individual consumers. No reporting is required if the export is acquired through free or anonymous download, or if it is

exported from a U.S. bank, financial institution, or their subsidiaries, affiliates, customers, or contractors for banking or financial use.

Implementation of Wassenaar Revisions

The January 2000 regulation also implemented a number of multilateral changes adopted under the Wassenaar Arrangement. After technical review, fifty-six bit DES encryption is authorized for export to all users, except embargoed and terrorist destinations. Mass market encryption software of sixty-four bits or less in key length also may be exported under a license exception, but only after technical review.

- *October 2000 Liberalization*[192]

On July 17, 2000, the Clinton Administration announced further updates to the encryption policy implemented in January 2000.[193] The implementing regulation was published on October 19, 2000. The major changes were as follows:

Exports to the European Union (EU) and Eight Additional Countries

U.S. exporters are authorized to export and re-export all encryption items except cryptanalytic (code breaking) products and their related technology without a license—in other words, under a license exception—to the fifteen EU member states, Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland. Exports to worldwide offices of companies, organizations and governments headquartered in these nations and Canada are also permitted. Under this new policy, U.S. exporters can ship their products immediately after submitting a commodity classification request to BIS, rather than waiting for the review and classification to be completed.

---

192. Revision to Encryption Items, 65 Fed. Reg. 62,600, 62,600–02 (Oct. 19, 2000) (codified to amend 15 C.F.R. pts. 732, 734, 740, 742, 744, 748, 770, 772, and 774).

193. Press Release, Office of the Press Secretary, The White House, Administration Updates Encryption Export Policy (July 17, 2000) *available at* http://www.globalsecurity.org/intell/ library/news/2000/07/irp-000717-crypto.htm.

Products Incorporating Short-Range Technologies

Products that incorporate components which provide cryptographic functionality limited to short-range wireless technology can be exported to any end-user without a license—in other words, under a license exception—technical review, or reporting requirements. These include consumer products that communicate with each other via short-range wireless technologies, such as audio devices, cameras, video recorders, computer accessories, handheld devices, mobile phones and household appliances, for example, refrigerators, washing machines and microwave ovens.

Streamlined Reporting

The regulation reduces reporting requirements on U.S. distributors located overseas, including subsidiaries of U.S. companies. Additionally, post-export reporting requirements are removed for client network appliances, single processor computers (for example, PCs), laptops, and handheld devices that are preloaded or bundled with encryption software.

Encryption Source Code

Proprietary encryption source code, that is not considered publicly available, is authorized for exportation under a license exception to non-government end-users after a classification request has been filed.

- *June 2002 Revisions*[194]

Further amendments issued in June 2002 did not introduce radical changes to the regulation of encryption exports. Rather, they implemented further discrete liberalization in three key areas.

Mass-Market Encryption Products

Under the June rule, mass-market encryption commodities

194. *See* Revisions and Clarifications to Encryption Controls in the Export Administration Regulations, 67 Fed. Reg. 38,855, 38,855–57 (June 6, 2002) (codified to amend 15 C.F.R. pts. 732, 734, 738, 740, 742, 748, 770, 772, and 774).

and software exceeding sixty-four bits may be exported and re-exported following a thirty day review by BIS. These products no longer will require post-export reporting. Except for code breaking cryptanalytic products to government end-users, mass-market products may be immediately exported to the EU, Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland once the review request has been filed with BIS. For other countries, mass-market products may not be exported until thirty days after the review request has been filed.

License Exception Eligibility for Certain Encryption Equipment

These revisions clarify that—in addition to encryption software—encryption test, inspection, and production equipment are eligible for export and re-export to U.S. subsidiaries, government and non-government end-users in the EU plus eight countries, as well as to non-government end-users in all other countries, except for the seven embargoed or terrorist destinations: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

Public and Non-Public Encryption Source Code

The June 2002 revisions also clarify that publicly available encryption source and object code may be exported and re-exported to most destinations after BIS notification. Encryption code that is not publicly available, by contrast, requires more than simple notification prior to export, namely a formal review by BIS.

5. Transfer of Compliance Burden to Industry

The change in U.S. export control focus from keeping advanced technology from the Soviet Bloc countries to preventing the proliferation of arms and "weapons of mass destruction" has manifested itself in a parallel trend. This trend has been a shifting of export control responsibilities from the government to the private sector. Today's private entities have much greater responsibility for ensuring compliance with any applicable regulations. The penalties for non-compliance are

severe, and lesser involvement by the agencies on the regulatory side has made government resources available on the enforcement side. Therefore, more than ever before, private entities must make sure they have internal compliance or export management systems in place to avoid or minimize export control violations.

BIS's Enhanced Proliferation Control Initiative (EPCI) places greater emphasis on the end-use and end-users of exported merchandise and technology.[195] Under EPCI rules, technology transfers that would not normally require export licensing could require a license because of the nature of the end-use or end-user. EPCI controls impose licensing requirements on: (1) exports from the United States of chemical precursors, biological agents, and associated equipment, software, and technology specified in the CCL to specified destinations; (2) exports from the United States of any commodity, software, or technical data when the exporter knows or has reason to know that it will be used in the design, development, production, stockpiling, or use of chemical or biological weapons in or by specified countries; and (3) activities of U.S. persons, including export, re-export, or transfers of any commodities or technology, performance of contracts, service, or employment, or any action which supports such a transaction, when the U.S. person knows that such activity will assist in the design, development, production, stockpiling, or use of chemical or biological weapons in or by specified countries.[196]

The potential for liability arising from export control regulations in general, and EPCI in particular, has made it a virtual requirement for any company involved in exporting to have an internal compliance program in place. Federal

---

195. Fact Sheet, Office of the Press Secretary, The White House, Export Controls on Computers, (Aug. 3, 2000), *at* http://www.bxa.doc.gov/HPCs/WhiteHseFactSheetAug32000.html.

196. Items 2 and 3 are the so-called "catch-all" provisions under which exporters of common commercial merchandise or technologies not dedicated to weapons development still may be required to obtain export licenses, if those items are being sold to an entity believed to be involved in weapons proliferation activities. BIS indicated during the EAR revision process in 1995 and 1996 that it intended to narrow the catch-all provision by publishing a "black list" of products that would require a license. This has not yet happened.

Sentencing Guidelines refer to such compliance programs as a mitigating factor in assigning a penalty in the event of a criminal violation. Section VI of this article discusses a number of the basic elements of a compliance program.

B. Other Restrictions on Technology Transfer

1. OFAC's Country-Specific Sanctions Programs

OFAC administers a series of country-specific sanctions programs discussed in Section III.B. These programs are motivated by foreign policy considerations and are intended to punish so-called countries of concern or to alter their behavior.[197] Companies engaged in international technology transfers or that might otherwise have dealings involving countries of concern—currently including Iran,[198] Iraq,[199] Libya,[200] and Cuba[201]—should be mindful of the restrictions that apply to each sanctioned country, as well as the restrictions that do not apply. Because the controls are political in nature, they are subject to rapid change in reaction to global, political, diplomatic, or military events. Countries can quickly be added to the restrictions list[202] or be re-designated.[203] Countries can be dropped, for example, North Korea.[204] Companies should stay abreast of the frequent updates and changes to the sanctions programs.

---

197. *See* 31 C.F.R. § 500.201 (2002) (prohibiting all U.S. transactions with designated foreign countries or their nationals). The U.S. administration has changed reference to such countries to a less pejorative term—"country of concern." Steven Mufson, *A 'Rogue' Is a 'Rogue' Is a 'State of Concern'; U.S. Alters Terminology for Certain Countries*, WASH. POST, June 20, 2000, at A16.

198. 31 C.F.R. §§ 560.206–.208, .314.

199. *Id.* §§ 575.205–.206.

200. *Id.* §§ 550.205, 209.

201. *Id.* § 515.

202. For example, Burma was added as a restricted destination for new investment in 1997. *Id.* § 537.202. *See also* OFFICE OF FOREIGN ASSETS CONTROL, U.S. DEPT. OF THE TREASURY, AN OVERVIEW OF THE BURMESE SANCTION REGULATIONS TITLE 31 PART 537 OF THE U.S. CODE OF FEDERAL REGULATIONS (1998).

203. *See, e.g.*, Exec. Order No. 13,268, 67 Fed. Reg. 44,751, 44,751 (July 2, 2002) (terminating the declared emergency with respect to the Taliban in Afghanistan).

204. Foreign Assets Control Regulations, 65 Fed. Reg. 38,165, 38,165 (June 19, 2000) (to be codified at 31 C.F.R. pt. 500).

Depending on the target country, OFAC regulations may do any or all of the following: restrict exports of U.S. technology, goods, and services; restrict imports of foreign goods, technology, and services; prohibit the financing of entities in the target country; block assets of the target country; or prohibit investments in the target country.[205]

In the majority of cases, such as Cuba or, more recently, Sudan, OFAC imposes a complete commercial embargo that prohibits U.S. companies or individuals from any type of commercial dealing, including the transfer of technology, which might benefit the target country.[206] These controls apply to U.S. persons wherever they are located. Thus, a company must bear in mind that U.S. employees of a foreign subsidiary transferring technology to an embargoed country could be violating OFAC rules. In other cases, different elements of a commercial embargo are imposed piecemeal. For example, in 1987 the United States imposed an import embargo against Iran in response to aggressive Iranian action against international shipping in the Persian Gulf.[207] In March 1995 the United States expanded the sanctions, but only by adding a prohibition against involvement by U.S. companies in petroleum development in Iran.[208] Then, in May 1995 President Clinton issued an Executive Order expanding sanctions further to prohibit all trade and investment activities involving Iran, including technology transfers, by U.S. persons, wherever located.[209]

In other instances, a sanctions program might provide that it applies only to investment activity—not to trade in goods, services, or technology. The sanctions against Burma are an example.[210] However, the Burma sanctions also provide that

---

205. *See, e.g.*, 31 C.F.R. § 560.207 (prohibiting new investments in Iran); *Id.* § 560.204 (prohibiting exportation of goods, technology, or services to Iran); *Id.* § 560.201 (prohibiting importation of Iranian goods or services); *Id.* § 515.208 (2003) (restricting loans, credits and other financing in Cuba); *Id.* § 538.301 (2003) (blocking accounts and property in Sudan).

206. *Id.* §§ 515.201, 538.201.

207. Exec. Order No. 12,613, 52 Fed. Reg. 41,940, 41,940 (Oct. 29, 1987).

208. Exec. Order No. 12,957, 60 Fed. Reg. 14,615, 14,615 (Mar. 15, 1995).

209. Exec. Order No. 12,959, 60 Fed. Reg. 24,757, 24,757 (May 6, 1995).

210. 31 C.F.R. § 537.204.

technology transfers are prohibited if payment is received in the form of participation in earnings or profits of a project in Burma.[211] Consequently, the Burma program would not normally prohibit technology transfers. However, a contract calling for a U.S. company to provide technical advice and to be paid a percentage of profits could be prohibited.

Without appropriate knowledge or advice regarding the elements of a particular sanctions program, companies easily could run afoul of the regulations. Likewise, they might assume erroneously that they are not permitted to engage in certain transfers that are in fact permissible.

2. State Department Controls

Companies dealing with defense-related technology must bear in mind that although DTC's regulations, the ITAR, nominally focus on "defense articles," this term is defined to include technical data and software.[212] Such technology or software, although categorized as "munitions," may seem to be entirely commercial, for example, commercial satellite or telecom transmission technology. Technology covered by the Munitions List in the ITAR, even if it is intended entirely for commercial or civilian end-uses, will still require a license or authorization from DTC; its end-use, however, may influence whether DTC will grant a license.

Like BIS, DTC defines "export" broadly to include electronic transfers outside the United States and so-called deemed exports via transfer or disclosure to foreign persons in the United States.[213] The ITAR also broadly defines "technical data" to include information related to the design, manufacture, testing and modification of defense articles, as well as software not otherwise covered in the Munitions List.[214] Publicly available data is not covered.[215] The ITAR also restricts "defense services," which are defined to include the furnishing of technical data or

---

211. *See id.* § 537.204(b)(2).

212. 22 C.F.R. § 120.6 (2002).

213. *Id.* § 120.17.

214. *See id.* § 120.10; *see also id.* § 121.8(f) (defining "software").

215. *See id.* § 120.10; *see also id.* § 120.11(a) (defining "public domain").

other assistance, such as training and repair work, to foreign entities either outside or within the United States.[216]

DTC controls are highly restrictive. Every export of technical data requires a license, subject to a few narrow exceptions. Companies may seek an individual DTC license to authorize a specific technology transfer by following the normal process of filing a license application on form DSP-5. Companies contemplating transferring technology pursuant to a project or long-term contract may obtain broader, comprehensive approval under a Technical Assistance Agreement (TAA),[217] which covers arrangements to transfer technical data or defense services, or under a Manufacturing License Agreement (MLA). A MLA can cover both a transfer of technology and the right of the foreign recipient to produce defense articles abroad based on that technology.[218]

Unlike BIS's regulations, the ITAR permits very few exemptions.[219] The ITAR has no *de minimis* exception for foreign products containing a very small U.S. component, unlike the EAR. Under the ITAR, the inclusion of U.S. origin defense articles in a foreign product, however small, renders the item subject to the ITAR.[220] Further, the ITAR does not permit any re-transfer, re-sale or re-shipment of technical data to a different end-user or destination, unless a DTC license is first obtained.[221]

Unlike BIS, DTC also requires any person who manufactures, transfers or exports defense articles and services, including technical data, to register with DTC.[222] This

---

216. *Id.* § 120.1(a); *see Id.* § 120.9 (defining "defense service").

217. *See id.* § 120.22. The TAA must contain certain clauses specified in the ITAR, must be submitted to DTC, and may not become effective until approved by DTC. *See also id.* § 124.1; *id.* § 124.8.

218. *Id.* § 120.21.

219. Exemptions are set out in Licenses for the Export of Technical Data and Classified Defense Articles, 22 C.F.R. § 125.4 (2001).

220. *See* Licenses for the Export of Technical Data and Classified Defense Articles, 22 C.F.R. § 125.1. The EAR has a de minimis exception for foreign software bundling a small component of U.S. origin. *See* Interpretations Related to Export of Technology and Software to Destinations in Country Group D:1, 15 C.F.R. § 770.3 (2003); *see also id*. § 734.4.

221. *See* 22 C.F.R. § 125.1(c).

222. *Id.* § 122.1.

requirement applies even if the company does not actually export the defense article or technology, a requirement that is often unknown to such companies. DTC must also be notified of any material changes in the registrant's ownership or business structure.[223]

3. National Security Investment Controls

U.S. law also imposes indirect restraints on the transfer of U.S. technology through national security-related restrictions on foreign investment in, or acquisition of U.S. companies. There are two primary investment-related provisions—the Exon-Florio Amendment and the National Industrial Security Program.

a. Exon-Florio Amendment

The Exon-Florio Amendment (Exon-Florio)[224] to the Defense Production Act[225] authorizes the Committee on Foreign Investment in the United States (CFIUS), an interagency committee chaired by the Treasury Department, to block any transaction that could place a U.S. corporation under foreign control in a manner that threatens U.S. national security.[226] If a transaction has been completed, CFIUS may recommend that the President order the parties to divest.[227]

In order to obtain assurances from the Government that an investment by a non-U.S. entity with potential national security implications does not run afoul of Exon-Florio, the parties to a transaction have the option of filing a notice with CFIUS, although they are not obligated to do so.[228] If the parties do not file a voluntary notice, however, the transaction may be subject to review and investigation by CFIUS for three years after the transaction's conclusion date and, in some circumstances,

---

223. *See id.* § 122.4.

224. *See* Christopher F. Corr, *A Survey of United States Controls on Foreign Investment and Operations: How Much Is Enough?*, 9 AM. U.J. INT'L L. & POL'Y 417, 421 (1994) [hereinafter *Survey of United States Control*].

225. 50 U.S.C. § 2061.

226. *See* 31 C.F.R. § 800.101 (2002).

227. *See id.* § 800.601(c).

228. *Id.* § 800.401; *see Survey of United States Controls*, *supra* note 224, at 423.

longer.[229] Within thirty days of the filing of a notice, CFIUS must either clear the transaction or open an investigation of the transaction.[230] A voluntary notice must provide information regarding the type of transaction, the operations located in the United States to which the foreign investor will gain control, the foreign investor's ownership structure, and the foreign investor's plans regarding the exercise of control.[231] The voluntary notice should be filed by all parties to the transaction.

Exon-Florio is not vigorously enforced—CFIUS has acted formally against few proposed transactions.[232] Nevertheless, given the drastic remedy, many non-U.S. acquiring companies opt to make a voluntary filing if the acquisition potentially could be viewed as national security sensitive. If pre-merger notification is made concerning the transaction for antitrust purposes,[233] CFIUS should be presumed to have knowledge of the transaction. Even where CFIUS does not act to block a transaction, the mere decision by CFIUS to question or investigate a transaction can often lead to a decision by the proposed foreign buyer to abandon the transaction. CFIUS also may seek a restructuring of the acquisition as a condition to its assent. These restrictions operate as an indirect restraint on the ability of a U.S. seller in a sector deemed national-security sensitive to transfer technology to a non-U.S. buyer.

The scope of transactions deemed potentially harmful to national security has been expanding. Traditionally, CFIUS has most closely scrutinized transactions involving businesses with some connection to the defense industry. Beginning in 2000, however, it has acted to investigate foreign acquisitions of U.S. companies in the telecommunications [234] and internet sectors.[235]

---

229. 31 C.F.R. § 800.401.

230. *Id.* § 800.404.

231. *See id.* § 800.402.

232. *See Survey of United States Controls*, *supra* note 224, at 428. Based on a review of the public record at the CFIUS Secretariat, CFIUS has blocked just one transaction, despite over 700 voluntary filings. *Id*. However, its decision to investigate proposed acquisitions more frequently has resulted in decisions by the proposed foreign investor to abandon or restructure the deal. *See id*. at 428–29.

233. *See id*. at 433. Such notices are filed under the Hart-Scott-Rodino provision of the Antitrust Improvements Act. *Id*.

234. *See, e.g.*, *Conditions Will Be Imposed on German Acquisition of*

The expansion of CFIUS' analysis into technology intensive sectors such as telecom and the internet also expands the indirect restrictions on U.S. technology transfer.

b. National Industrial Security Program

The National Industrial Security Program (NISP), which is administered by the Defense Security Service (DSS) of the Defense Department, provides that U.S. companies with classified government contracts must notify the DSS when they are acquired by or otherwise come under the control of a foreign entity.[236] DSS will impose conditions designed to prevent unauthorized disclosure of classified information to the foreign acquirer.[237]

A foreign-owned U.S. government contractor may be permitted to continue performance under existing contracts and bid for new classified contracts only if it implements a foreign-control-negating security arrangement approved by the Defense Department.[238] Such arrangements normally entail onerous structural conditions, such as voting trusts, proxy arrangements or other special security measures that bar or severely limit the

---

VoiceStream, WASH. TARIFF & TRADE LETTER, Sept. 11, 2000, at 2–3 (describing CFIUS' recent investigation of the proposed acquisition of VoiceStream, a U.S. cellular phone company, by Deutsche Telekom, a German owned company).

235. *See, e.g.*, *CFIUS and the F.B.I.*, 4 THE M&A J. 1, 1–4 (Oct. 2000). CFIUS investigated the proposed acquisition of Verio, a U.S. web-site host by Nippon Telegraph & Telephone Company (NTT). The Japanese telephone company eventually agreed to conditions that restricted its access to certain U.S. technology, among other conditions, in exchange for clearance by CFIUS. *Id*.

236. Executive Order No. 12,829, 58 Fed. Reg. 3479, 3479 (Jan. 6, 1993). NISP was established for the protection of information classified pursuant to Executive Order 12,356 (April 2, 1982). Although the National Security Council has overall responsibility for the program, the Secretary of Defense is responsible for implementing the Program rules and requirements. *Id*.

237. *Id.* The Program is implemented through the rules and guidelines set forth in the National Industrial Security Program Operating Manual (NISPOM). *Id*. The NISPOM is intended to prevent the unauthorized disclosure of classified information to parties not having proper security clearance, and in particular, non-U.S. persons ineligible for security clearance. *See id*.

238. *See* DEP'T. OF DEFENSE, DOD 5220.22-M, NAT'L INDUS. SECURITY PROGRAM OPERATING MANUAL 10-1-10 to 10-7-4 (1995) [hereinafter NIPSOM] *available at* http://www.dss.mil/isec/nispom_0195.htm; *see also* Executive Order No. 12,829, 58 Fed. Reg. at 3479.

involvement of the foreign parent in management of the contractor.[239]

Thus, the NISP requirements operate as a significant impediment to technology transfer for businesses engaged in classified government work.

4. Volatile Controls on Sensitive Countries

The discussion thus far has focused on the export control statutes and regulations that continue to apply to technology transfers in the post-Cold War setting and that require exporters to take all necessary steps to ensure compliance. A review of the way the government actually imposes restrictions on technology transfers, and the reasons for the government's action, serves to illustrate a more intangible aspect of the U.S. export control regime—the political aspect.

a. Foreign Policy Sanctions on India / Pakistan

One reason technology transfer restrictions have continued to weigh on U.S. exporters is the proliferation of economic sanctions imposed for foreign policy reasons. The economic sanctions on India and Pakistan are salient examples of the volatility and dubious effectiveness of sanctions, as well as the pain they inflict on U.S. exporters.

Under Section 102 of the Export Control Act, the President must impose sanctions if he determines that a non-nuclear weapons state has detonated a nuclear device.[240] Pursuant to this congressional mandate, President Clinton announced sanctions against India on May 13, 1998 in response to India's nuclear tests two days earlier on May 11.[241] The President announced sanctions against Pakistan on May 30, 1998, two days after Pakistan's nuclear tests on May 28.[242]

---

239. NISPOM, *supra* note 238, 10-1-1 to 10-7-4; *see* Exec. Order No. 12,829, 58 Fed. Reg. at 3479.

240. Arms Export Control Act, § 102, 22 U.S.C. §§ 2799aa, aa-1 (2000).

241. Presidential Determination No. 98-22 (May 13, 1998), 63 Fed. Reg. 27,665, 27,665 (May 20, 1998) ("Sanctions Against India for Detonation of A Nuclear Explosion"); *see U.S. Imposes Sanctions on India*, CNN INTERACTIVE, May 13, 1998, *at* http://www.cnn.com/WORLD/asiapcf/9805/ 13/india.us/.

242. Presidential Determination No. 98-25 (May 30, 1998), 63 Fed. Reg. 31,881,

The sanctions included: (1) termination of U.S. foreign assistance programs; (2) termination of military sales and financing; (3) denial of credit and credit guarantees by U.S. Government entities; (4) opposition to loans by international financial institutions; (5) prohibition against U.S. bank loans to the Indian and Pakistani governments; and (6) prohibition against exportation of certain dual-use items.[243]

The Clinton Administration indicated it wanted to avoid broad-based export restrictions, and instead wanted to tailor the sanctions to reach principally nuclear and missile related items and users through a list of proscribed products and end-users.[244]

However, after one month of confusion following the President's announcement regarding what the restrictions would be and who would enforce them, the Commerce and State Departments announced a number of sanctions against India and Pakistan that were much broader than the original intent.[245] The most significant was a policy denying all export and re-export license applications for a range of dual-use commercial items to all end-users in India and Pakistan and revoking an exception for computer exports.[246] These sanctions fell hard on U.S. exporters of purely commercial items to commercial end-users in India and Pakistan, substantially curtailing the U.S. exporters' trade and putting them at a disadvantage relative to competitors in Europe and Asia that did not have to contend

---

31,881 (June 10, 1998) ("Sanctions Against Pakistan For Detonation of a Nuclear Explosive Device"). *See*, *World Condemns Pakistan Nuclear Tests*, CNN INTERACTIVE, May 30, 1998, *at* http://www.cnn.com/WORLD/asiapcf/9805/28/pakistan.reax/ (providing international reactions to Pakistan's nuclear tests).

243. 22 U.S.C. § 2799aa-1; Presidential Determination No. 98-22 (May 13, 1998), 63 Fed. Reg. at 27,665; Presidential Determination No. 98-25 (May 30, 1998), 63 Fed. Reg. at 31,881.

244. *See* 22 U.S.C. § 2799aa-1 (indicating that U.S. sanctions were primarily targeted toward military, dual-use, and CCL items).

245. *See* Revocation of Munitions Exports Licenses and Other Approvals for India, 63 Fed. Reg. 27,781, 27,781 (May 20, 1998); *see also* Revocation of Munitions Export Licenses and Other Approvals for Pakistan, 63 Fed. Reg. 33,122, 33,122 (June 17, 1998); Indian and Pakistan Sanctions and Other Measures, 63 Fed. Reg. 64,322, 64,322 (Nov. 19, 1998).

246. *See* Indian and Pakistan Sanctions and Other Measures, 63 Fed. Reg. at 64,324–25.

with similar sanctions.[247]

Four months later, in October 1998, Congress enacted the so-called Brownback Amendment, which provided the President limited authority to waive the sanctions.[248] In November 1998, President Clinton exercised this waiver authority and announced that he would restore Export-Import Bank and OPIC programs in India and that he would not restrict the activities of U.S. banks in India and Pakistan.[249] Nevertheless, the President decided to retain the broad controls listed on U.S. commercial exports to India and Pakistan until such time as India and Pakistan demonstrate further progress on non-proliferation issues.[250]

That same month, the Commerce Department announced additional sanctions tailored to punish a specific list of Indian and Pakistani entities believed to be directly or indirectly involved with the nuclear, missile or military programs of their respective countries.[251] Although the Commerce Department stated that publishing the list would ease the burden on U.S. exporters by clarifying their responsibilities, U.S. exporters still were subject to the broad commercial sanctions announced earlier. Further, BIS later advised exporters that even if a prospective purchaser in India or Pakistan was not on the list, the U.S. exporter had a due diligence responsibility to investigate and ensure there was no relationship between the intended recipient and the listed entities.[252] What was perhaps

---

247. *See U.S. Outlines Sanctions Against India, Pakistan*, CNN INTERACTIVE, June 18, 1998, *at* http://www.cnn.com/WORLD/asiapcf/9806/18/india.pakistan.sanctions/index.html.

248. India-Pakistan Relief Act, Pub. L. No. 105-277, § 902, 112 Stat. 2681, 2690 (1998). S*ee* Press Release, Office of the Press Secretary, The White House, Easing of Sanctions on India and Pakistan (Nov. 7, 1998) [hereinafter Easing of Sanctions] *available at* http://www.mtholyoke.edu/acad/intrel/liftsanc.htm.

249. Presidential Determination No. 2000-04, (Oct. 27, 1999), 63 Fed. Reg. 60,649, 60,649 (Nov. 8, 1999); Easing of Sanctions, *supra* note 248.

250. *Compare* Indian and Pakistan Sanctions and Other Measures, 63 Fed. Reg. at 64,324–25 (restoring financial activity in India and Pakistan), *with* 22 U.S.C. § 2799aa-1 (broadening trade sanctions).

251. India and Pakistan Sanctions and Other Measures, 63 Fed. Reg. at 64,325.

252. *A Good Address Isn't Enough for Exports to India*, WASH. TARIFF & TRADE LETTER, July 24, 2000, at 1.

more troubling, the November 1998 sanctions were having no palpable effect on India or Pakistan.[253] Another concern for U.S. exporters was that there was no provision for when these sanctions would be eliminated or further modified.

Roughly one year later, in response to complaints from U.S. exporters and their allies, the Commerce Department announced the removal of over fifty Indian entities from the sanctions list.[254] Although this was announced as an easing of the sanctions, it had little commercial effect, because most of those removed were military entities or think tanks.[255] The broad-based sanctions on commercial trade continued without change.[256]

Apart from their volatility and punitive effect on U.S. exporters, the India-Pakistan sanctions also highlight other peculiar features of the foreign policy sanctions—they are self-reinforcing and difficult to remove. In the summer of 2001, President George W. Bush was approached by executives from over eighty U.S. companies, and told that failure to remove the sanctions would cost U.S. businesses hundreds of millions of dollars that would go to their non-U.S. competitors.[257] All efforts to remove the sanctions were resisted by the State Department and Congress due to concerns that any relaxation would send the wrong signal to countries such as Brazil and South Africa—namely that the U.S. opposition to nuclear proliferation had weakened.[258]

Eleven days after September 11, 2001, President Bush announced the immediate suspension of the sanctions against India and Pakistan.[259] Thus, as quickly as they came, the

253. *See id*.

254. Press Release, Bureau of Industry and Security, Commerce Department Will Remove 51 Indian Entities from Sanctions List (Dec. 16, 1999), *available at* http://www.bxa.doc.gov/news/ archive99/51entities2beremoved.html.

255. *BXA Eases Indian Sanctions*, EXPORT PRACTITIONER, Jan. 2000, at 13, 13.

256. *See id*.

257. *Opposition Mounts to Easing of India Sanctions*, FIN. TIMES (London), Aug. 16, 2001, at 8.

258. *Id*.

259. Presidential Determination No. 2001-28 Memorandum on Waiver of Nuclear-Related Sanctions on India and Pakistan (Sept. 22, 2001), 66 Fed. Reg. 50,095, 50,095 (Oct. 2, 2001); *Bush Lifts India, Pakistan Sanctions*, CNN.com/WORLD, Sept. 22, 2001, *at*

sanctions were gone. The political event that gave rise to them gave rise to another that had no longer made them expedient. The sanctions had no evident effect on the actions of Pakistan or India,[260] although they certainly had a negative effect on U.S. exporters.

b. Pressure on China Trade

In 1996, jurisdiction over export control of commercial communications satellites and related merchandise was transferred to the Commerce Department from the State Department.[261] China had become an important market for satellite-related items for U.S aerospace companies, mainly because of China's burgeoning space launch capabilities. China was able to offer more launch slots at lower cost than the launch services of Western nations. The transfer in jurisdiction was intended to carry forward the policy of the Clinton Administration to engage China.[262]

This policy provision was overtaken in 1998 by a scandal relating to technical assistance two U.S. companies provided to China in connection with a failed satellite launch.[263] Although it was not clear whether a violation had occurred, news of the actions set off a firestorm that had a lasting effect on controls and transfers to China.

The scandal gave rise to a criminal investigation of the companies involved[264] and to a special congressional investigation, by the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's

---

http://www.cnn.com/2001/WORLD/asiapcf/south/09/22/ret.sanctions.pakistan/index.html.

260. *BXA Eases Indian Sanctions, supra* note 255, at 13. Neither India nor Pakistan signed the comprehensive test ban treaty, nor did they commit to a moratorium on production of weapons-grade material.

261. *See* Alexander, *supra* note 3.

262. *See id*.

263. *See* John Mintz, *Two Executives Defend Hughes's China Deals*, WASH. POST, July 30, 1998, at A6; *see also* John Mintz, *How Hughes Got What It Wanted on China*, WASH. POST, June 25, 1998, at A1 [hereinafter Mintz, *How Hughes Got What it Wanted*].

264. Mintz, *How Hughes Got What it Wanted*, *supra* note 263. Loral reached a settlement in early 2002. *Unequal Justice on Tech Transfer Enforcement*, EXPORT PRACTITIONER, Feb. 2002, at 6, 6.

Republic of China, chaired by Republican Representative Christopher Cox of California, the Cox Committee. The Cox Committee Report (the Cox Report), issued in January, 1999,[265] concluded that more damage to U.S. national security actually resulted from Chinese espionage at U.S. nuclear facilities than lax compliance and enforcement of U.S. export controls.[266] Nevertheless, the Cox Report roundly criticized the export control record of the Clinton Administration with respect to China, and set forth thirty-eight recommendations for changes to that policy.[267]

Many of the Cox Committee's recommendations were manifestly reasonable, and align with the recommendations of this author for reforms of the export control process, including: (1) expediting the processing of license applications;[268] (2) increasing transparency in license processing;[269] (3) focusing on technologies of the greatest national security importance;[270] and (4) implementing procedures for reviewing the reasons for controlling technologies for national security purposes.[271] However, the report also recommended changes aimed at "toughening" export controls that would likely lead to increased delays and denials, such as providing for longer interagency review times,[272] allowing for mid-level departments involved in interagency review to veto license applications,[273] and calling for overseas on-site pre- and post-license inspections without notice to the host government.[274]

The Cox Report set off cries of alarm from the Clinton Administration and U.S. business, who objected to some of the

---

265. H.R. SELECT COMM. REP. No. 105-851 (1999), *available at* http://www.gpo.gov/congress/house/hr105851-html.

266. *Chinese Espionage—Not Trade—Hurt U.S. Security*, WASH. TRADE DAILY, May 26, 1999, at 1.

267. *See id.* at 1–4; *see also* H.R. SELECT COMM. REP. No. 105-851.

268. H.R. SELECT COMM. REP. No. 105-851, vol. III, at 175.

269. *Id.*

270. *Id.* at 174.

271. *See id.*

272. *Id.*

273. *See id.* at 173.

274. *Id.*

recommendations.[275] Despite these objections, the Cox Report gave momentum to those wishing to clamp down on trade with China, and led to a number of other calls for such a clampdown. Jurisdiction over satellites was transferred back to the State Department from the Commerce Department.[276] Former Senator Thompson introduced a series of bills to restrict trade with China, calling for automatic sanctions against foreign governments found to be transferring security-sensitive technologies to China, notwithstanding the fact that these foreign countries might not share the U.S. view of China as a strategic threat.[277] None of these bills was enacted. The GAO also issued a report criticizing the effectiveness of U.S. restrictions on technology transfer to China with respect to the semiconductor industry, calling for an overhaul of U.S. restrictions.[278] A few months later, the U.S.-China Security Review Commission released a report calling for tougher licensing policies on trade with China.[279]

---

275. *See* John Mintz, *Clinton: Panel's Export Rules May Delay Deals,* WASH. POST, Feb. 2, 1999, at A10. (expressing the White House's concern that some of the Cox Committee's recommendations "could resurrect Cold War-type export rules and gum up overseas deals with layers of bureaucracy"); s*ee also*, *Cox Report Fuels Fears of Return to Cold War*, EXPORT PRACTITIONER, Jan. 1999, at 17, 17–18 (discussing the American Electronics Association's counterproposal for multilateral export controls that focuses on "controllable" and "chokepoint" products, technologies critical to the national security, policies responsive to frequent advancements in technology, and policies that regularly assess the effect of controls on U.S. exporters).

276. *See* Amendments to the International Traffic in Arms Regulations: Control of Commercial Communications Satellites on the United States Munitions List, 64 Fed. Reg. 13,679, 13,679–02 (Mar. 22, 1999) (to be codified at 22 C.F.R. pts. 121 and 124); *see also* Removal of Commercial Communications Satellites and Related Items from the Department of Commerce's Commerce Control List for Retransfer to the Department of State's United States Munition List, 64 Fed. Reg. 13,338, 13,338 (Mar. 18, 1999).

277. The Administration and many in Congress objected to the bills. *See e.g., Thompson Scales Back China Bill*, EXPORT PRACTITIONER, Aug. 2000, at 13, 13 (emphasizing that "[the Thompson bill] is still entirely objectionable . . . . There is no other country that is going to follow us, so the only real effect would be to cut off U.S. exports and investments.").

278. *See* RAPID ADVANCES, *supra* note 14, at Highlights (summarizing the GAO's report to the U.S. Senate).

279. *See* U.S.-CHINA SECURITY REVIEW COMM'N, DEP'T OF STATE, THE NAT'L SECURITY IMPLICATIONS OF THE RELATIONSHIP BETWEEN THE UNITED STATES AND CHINA (2002), *available at* http://usinfo.state.gov/regional/ea/uschina/comisrpt.htm; *see also China Report Foreshadows Tougher Licensing and Legislatio*n, WASH. TARIFF & TRADE

Although the Clinton Administration and BIS objected to many of the more extreme calls for tightening China export controls, BIS nevertheless responded to the pressure by announcing various provisions to strengthen the licensing process with regard to China and to enforce license conditions, and it implemented a substantial curtailment of high-tech transfers to China, particularly satellites.[280] The most significant effect on U.S. exporters was that the processing time for license applications increased dramatically.[281] In addition to the lengthy interagency consideration of China applications, the increasing imposition of conditions requiring pre- and post-license inspections in China caused significant delays.[282]

The treatment of trade with China between 1998 and 2002 reveals the tension of the disparate interests at work in the export control process, as well as the ever-changing tilt of the pendulum between those promoting U.S. exports and those promoting restrictions in the name of national defense. In the case of China, the balance of power unquestionably shifted to

---

LETTER, July 22, 2002, at 1 (indicating that the report made "21 recommendations aimed at tightening controls on the flow of economic resources and technology to China"). The report was widely criticized in the export community. *See id.* The former Undersecretary of the Commerce Department for Export Administration stated that the report "reflects a Cold War mentality that ignores both the spread of these technologies over the past decade and their importance in bringing freer communications and information to the Chinese people. *Id*. at 2.

280. *See* David S. Cloud et al., *U.S. Says China-Satellite Rejection Was One-Time Event, but Chill May Result*, WALL ST. J., Feb. 24, 1999, at A4; *see also* Stephen Fidler & Tony Walker, *US Satellite Sale to China Under Threat*, FIN. TIMES (London), Feb. 22, 1999, at 3.

281. *See License Processing for China Gets Harder, Longer*, WASH. TARIFF & TRADE LETTER, July 26, 1999, at 1. Processing times between 1998 and 1999 increased from roughly fifty to roughly sixty days, with a significant increase in the number of applications returned without action. *Id*. By 2002, the average processing time had increased to over seventy-five days. *Export Licensing Remains Slow for Sensitive Destinations*, WASH. TARIFF & TRADE LETTER, Oct. 28, 2002, at 1. The backlog of pending China applications soared from six cases in the Clinton Administration to almost 300 under the Bush Administration. *Agencies Slow on China License Applications*, EXPORT PRACTITIONER, Nov. 2001, at 5, 5.

282. *Little Progress Made with Chinese on Post-Shipment Inspections*, WASH. TARIFF & TRADE LETTER, Oct. 28, 2002, at 1 (discussing a backlog of some 700 post-shipment verification requirements).

those who would curtail transfers of technology.[283]

More specifically, and more troubling, is the inability, or unwillingness, on the part of those who would restrict U.S. sales to China to acknowledge that China often can buy the same technology from suppliers in other countries. Unlike the days of the Cold War when there was a common view among the United States and its allies regarding the threat posed by the Soviet Bloc, other countries who supply comparable technology and merchandise to China often do not agree with the United States that China is a strategic threat.[284] Consequently, many such third-country suppliers, including close U.S. allies, refused to restrict exports to China.[285] In these circumstances, restricting U.S. exporters from shipping to China does not prevent China from acquiring the technology it desires, and only hurts U.S. exporters. A national security policy that is ineffective towards perceived strategic threats and harms the U.S. technological competitiveness that it relies on makes no sense.[286] Although

---

283. *See supra* note 281 and accompanying text; *see also* Alexander, *supra* note 3, at 1 (discussing the different interests along the export control spectrum, and the ever-shifting balance of power "from the Commerce Department during the Carter Administration to the Defense Department in the Reagan era, and on to State in the Clinton Administration").

284. *See Differing Views of China at Heart of Export Control Dilemma*, WASH. TARIFF & TRADE LETTER, Feb 12, 2001, at 1.

285. *See* RAPID ADVANCES, *supra* note 14, at 2–3; *see also* U.S.-TAIWAN BUSINESS COUNCIL, SEMICONDUCTOR REPORT 15 (Third Quarter, 2002) The report discusses the fact that European suppliers of 0.18-micron semiconductor production equipment were shipping to start-up China factories, whereas the U.S. companies are prohibited from doing so.

> Unless the U.S. can rein in its European counterparts, there appears to be no reason not to allow U.S. companies to take advantage of [the China] market. The European Commission has said that it has no control over licenses for chip making equipment—it allows individual member nations their own say. The result is chaos, and individual European nations are allowing 0.18-micron equipment into China at a growing rate.

Id.

286. Even where licenses to China ultimately are approved, the delays that U.S. exporters must deal with places them at a distinct disadvantage. *See, e.g.*, *Complaints Grow*, *supra* note 52, at 1 (noting that "[t]he slow reviews and extra conditions particularly hit licenses for China . . . . Although most cases eventually get approved, U.S. exporters face an unlevel playing field against foreign competitors who can get approvals in weeks or days from their export licensing agencies.").

this flagrant shortcoming has been expressed repeatedly,[287] it is surprising that none of the export control agencies affords meaningful import to foreign availability in the licensing process.[288]

V. PENALTIES

> *[BIS] has become one of the prime beneficiaries of Washington's new enthrallment with homeland security, and tougher enforcement of export control regulations will be a central focus of the agency's increased budget*.[289]

> *In light of the [post 9/11] paradigm shift . . . [BIS] might be out for blood.*[290]

It goes without saying that corporations and individuals should comply with export control requirements out of dedication to law-abiding conduct and cooperation with the government on issues of national security. However, principles of self-preservation also impel companies to take measures to

---

287. *E.g.*, *Defense Panel Recommends Cut*, *supra* note 2, at 1. The Defense Science Board Task Force on Globalization and Security warned that "protection of capabilities and technologies readily available on the world market is, at best, unhelpful to the maintenance of military dominance and, at worst, counterproductive, undermining the industry upon which U.S. military-technological supremacy depends." *Id*.

288. *See* RAPID ADVANCES, *supra* note 14, at 4. Specifically, "[a] U.S. Government foreign availability analysis of semiconductor manufacturing equipment has not been completed since 1987." *Id.* In the one instance known to this author in which a license decision was made on the basis of foreign availability, both the European competitor of a U.S. exporter and the European government explicitly stated that they had and would continue to ship competing merchandise that the U.S. exporter had been repeatedly denied the right to export to China. Despite clear, documentary evidence of such foreign availability, supported by the foreign government—evidence which typically would not be available to a U.S. exporter—it took the U.S. exporter over ten months to overturn the license application denial and receive permission. *See* Letter from William A. Reinsch, United States Department of Commerce, to Christopher F. Corr, Partner, White & Case LLP (Dec. 6, 1999) (on file with author).

289. *Homeland Security Concerns Boost BXA Enforcement Budget*, WASH. TARIFF & TRADE LETTER, Feb. 11, 2002, at 1.

290. *Unequal Justice on Tech Transfer Enforcement, supra* note 264, at 6.

comply with export controls. Violations can result not only in negative publicity and enhanced scrutiny from regulators, but also in severe civil and criminal penalties, including imprisonment of company directors, officers and employees, and substantial fines. Violations broadly encompass not only direct participation in unauthorized transfers, but also indirect involvement via support for or facilitation of any aspect of illicit transactions.

For instance, in January of 2003, BIS announced the imposition of civil and criminal sanctions, including $1 million in criminal fines, against a U.S. company that pled guilty to two felony charges of violating U.S. export controls.[291] BIS also announced that it was holding another company liable for export violations committed by an entity it had acquired several years previously. The purchaser agreed to a settlement calling for a $1.76 million civil fine, following a BIS demand for $3.76 million.[292] The State Department often imposes even more severe penalties, including three cases in 2002 in which it imposed fines ranging from $13–14 million.[293]

The State Department is authorized to impose more severe sanctions for violations than is BIS, and in practice this has been the case.[294] However, after September 11, 2001, BIS announced plans to substantially enhance its enforcement efforts, including a significant budget and staff increase for its

---

291. Press Release, Bureau of Industry and Security, Silicon Graphics Settles Criminal and Civil Charges That Computer Shipments Violated U.S. Export Controls (Jan. 7, 2003). Silicon Graphics, Inc. pled guilty to two felony charges related to exporting computers to Russia. *Id*. In addition to the $1 million in criminal fines, Silicon Graphics also agreed to civil fines. *Id*.

292. *BIS Seeks to Impose Liability on Firms That Acquire Exporters*, WASH. TARIFF & TRADE LETTER, Nov. 11, 2002, at 1. The purchaser, Sigma Aldrich Corp. agreed to pay $1.76 million in civil fines to settle charges that Research Biochemicals Limited Partnership, a company it had acquired in 1997, had violated the EAR restrictions before and after the acquisition. *Id*.

293. *See Unequal Justice on Tech Transfer Enforcement*, *supra* note 264, at 6 (discussing a fine against Loral Space & Communications for $14 million, a fine against Boeing for $13.8 million, and a fine against Lockheed Martin for $13 million, all for alleged ITAR violations).

294. *See id.* at 6–7; s*ee also infra* Parts III.A, III.C. Violations of munitions controls may be viewed as more serious than violations of dual-use controls, thereby warranting harsher sanctions.

Office of Export Enforcement, and legislation was introduced in Congress to allow it to impose more severe sanctions.[295] The discussion below summarizes the penalty authority of the various agencies.

A. BIS

Under the EAR, it is a violation to "engage in any conduct prohibited by or contrary to, or refrain from engaging in any conduct required by the EAA, the EAR, or any order, license, or authorization issued thereunder."[296] Penalties for EAR violations include both criminal and civil/administrative penalties.[297]

1. Criminal Penalties

There are different levels of criminal penalties for "knowing violations" and "willful violations." A knowing violation is one where the act is committed intentionally, but there is no specific intent to break the law.[298] The potential penalties for knowing violations include imprisonment of up to five years, and fines of up to $50,000 or five times the value of the exports involved, whichever is greater.[299] Willful violations are defined by BIS as instances in which the violator has knowledge that the items at issue will be used for the benefit of, or that the destination or intended destination of the items is, any country to which exports are restricted for national security or foreign policy reasons.[300] The potential penalties for each willful violation by an individual range from fines of up to $250,000 to imprisonment of up to ten years, or both. For companies, the penalty for each violation can be up to $1 million or up to five times the value of

---

295. *Homeland Security Concerns Boost BXA Enforcement Budget*, *supra* note 289, at 1; Export Administration Act of 2001, S. 149, 107th Cong. (2001) (proposing legislation to provide "authority to export control exports"); *see Unequal Justice on Tech Transfer Enforcement, supra* note 264, at 7–8 (discussing S. 149, which would permit BIS to impose more severe sanctions).

296. 15 C.F.R. § 764.2(a) (2002). This authority is delegated by the Export Administration Act. *See* War and National Defense, 50 U.S.C. §§ 2401–2420 (2000).

297. 15 C.F.R. § 764.3(a), (b).

298. United States v. Haldeman, 559 F.2d 31, 114 n.226 (D.C. Cir. 1977).

299. 15 C.F.R. § 764.3(b)(1).

300. *Id.* § 764.3(b)(2).

the exports involved, whichever is greater.[301]

2. Administrative Penalties

The EAR also provides for a litany of administrative sanctions including: revocation of export licenses held by the violator; general denial of the violator's export privileges; exclusion of the exporter from export practice—the so-called "death sentence"; and the imposition of fines for each violation.[302]

As discussed previously, Congress and the Bush Administration have introduced legislation to strengthen BIS's authority to impose penalties.[303]

3. Legal Standard

Unlike criminal sanctions, which commonly require willful or knowing violations, civil penalties may be assessed on a strict liability basis for violations of the EAR.[304] However, a strict liability standard does not apply to all civil or administrative violations, but only to those for which the regulatory standard does not require a finding of knowledge or "reason to know" as a prerequisite to a violation.[305]

---

301. *Id*.

302. *Id.* § 764.3(a)(1). Fines range from up to $10,000 per violation, or up to $100,000 per violation in case of violations of national security export controls. *Id*. However, the maximum civil penalty allowed by law under the authority of the IEEPA is $10,000 per violation. *See* 50 U.S.C. § 1705(b).

303. *Supra* note 295 and accompanying text. Senate Resolution 149 would increase criminal sanctions on individuals for willful violations to $1 million and imprisonment up to 10 years, and to $5 million for entities. Export Administration Act of 2001, S. 149, 107th Cong. § 1 (2001). Civil penalties would be raised to $500,000 per violation. *Id*.

304. *See* Iran Air v. Kugelman, 996 F.2d 1253, 1259 (D.C. Cir. 1993). The Court ruled that "the language of the statute and the pertinent regulations adequately indicated that civil sanctions could be assessed on a strict liability basis." *Id*. The Court went onto emphasize a key distinction between civil or administrative violations, on the one hand, and criminal violations, on the other, stating that, "[i]t is not unusual for Congress to provide for both criminal and administrative penalties in the same statute and to permit the imposition of civil sanctions without proof of the violator's knowledge. " *Id*. at 1258.

305. *Compare* 15 C.F.R. § 764.2(e) (providing for administrative sanctions in the case of "acting with knowledge of a violation"), *and* 15 C.F.R. § 764.2(f) (providing for administrative sanctions in the case of "possession with intent to export illegally"), *with*

With respect to both criminal sanctions and those administrative sanctions requiring a finding of knowledge, the inquiry into the state of mind of a reasonable exporter, rather than a focus on the defendant's actual knowledge, effectively shifts the burden of screening export transactions to the exporter.[306] Under the regulatory definition, it is sufficient for BIS to show that the exporter should have been aware that the transaction would be a violation of the EAR without hard evidence of actual knowledge. This more nebulous standard results in greater uncertainty and consequent pressure on accused exporters to settle claims, given that settlement has tactical attractions apart from questions of guilt or innocence. These inducements include minimizing litigation risk and the possibility of harsher penalties, minimizing damage to reputation and good will as a result of drawn-out public proceedings, and reducing legal costs. In terms of risks, exporters must bear in mind that sanctions imposed by BIS cannot be challenged, only findings regarding liability.[307]

B. OFAC

Violations of the OFAC regulations also are punishable by criminal and civil sanctions. Criminal penalties for OFAC violations include up to ten years imprisonment, up to $1 million in corporate fines per violation, and up to $100,000 in individual fines per violation.[308] Fines for criminal penalties may be increased pursuant to 18 U.S.C. § 3571. Civil penalties for OFAC violations include fines of up to $11,000 per violation and

---

15 C.F.R. §§ 764.2(a)–(d) (defining violations as simply engaging in prohibited conduct, to which the strict liability standard would apply).

306. *See* 15 C.F.R. §§ 764.2(f), 772.1 (clarifying that, because the regulatory definition of "knowledge" includes not only actual knowledge but also "reason to know" or "reason to believe," evidence of something less than actual knowledge may be sufficient to prove liability).

307. *See* 50 U.S.C. § 2412(c)(3) (2000); *see also* Moller-Butcher v. U.S. Department of Commerce, 12 F.3d 249, 252 (D.C. Cir. 1994) (indicating that "[t]he plain language of 2412(c)(3) confers and defines our jurisdiction, clearly limiting it to questions concerning the liability which occasioned the sanction at issue, not the sanction itself").

308. War and National Defense, 50 U.S.C. § 5 app. (1917). Penalties under the Trading with the Enemy Act are much stronger than penalties under the International Emergency Economic Powers Act. *Compare* 50 U.S.C. § 5, *with* 50 U.S.C. § 1705 (2000).

are imposed administratively.[309]

On January 29, 2003, OFAC promulgated proposed rules for enforcing the sanctions programs.[310] The rules address prior criticism that OFAC's deliberative process was not transparent and provide significant detail regarding OFAC's enforcement process, indicating factors bearing on the choice of sanctions in a particular case and consideration of mitigating and aggravating factors.[311]

C. State Department

Similarly, violations of the State Department ITAR rules carry both criminal and civil penalties. Willful violations of ITAR rules may result in criminal fines for corporations or individuals of up to $1 million for each violation.[312] Violations also are subject to civil penalties for corporations or individuals of up to $500,000 per violation.[313] Under ITAR, violators may also be debarred from exporting defense articles or defense services.[314]

D. Other Agencies

Penalties for violating nuclear-related controls of the Energy Department include fines up to $10,000 and imprisonment up to ten years, or both.[315] If done with intent to injure the United States or to aid a foreign country, penalties are more severe, including life imprisonment and higher fines. Violations of NRC controls also carry criminal and civil penalties.[316]

---

309. *See* 31 C.F.R. § 560.701 (2002). The legal standard of review for OFAC violations also differs from the standard for the EAR.

310. Reporting and Procedures Regulations; Cuban Assets Control Regulations: Publication of Economic Sanctions Enforcement Guidelines, 68 Fed. Reg. 4422, 4422–29 (Jan. 29, 2003) (to be codified in 31 C.F.R. pts. 501, 515).

311. *Id*.

312. *See* 22 C.F.R. § 127.3 (2002); *see also* Foreign Relations and Intercourse, 22 U.S.C. § 2778(c) (2000).

313. *See* 22 C.F.R. § 127.10 (2002); *see also* 22 U.S.C. 2778(e).

314. 22 C.F.R. § 127.11.

315. 10 C.F.R. § 810.15 (2003).

316. 10 C.F.R. §§ 110.60, 110.64, 110.67.

VI. COMPLIANCE MEASURES

Every wall is a door.

-Ralph Waldo Emerson

Because export control rules are broad, complex, and subject to periodic change, and because violations of the rules can be punished severely, companies involved in technology transfer should—as a matter of due diligence—assess and implement measures to ensure compliance. Industry best practices call for the development of an internal compliance program, tailored to the structure and operations of the company concerned, that institutes checks and safeguards on transactions and minimizes possible violations of export control laws. Should a violation occur, existence of a compliance program should serve as a mitigating factor in an investigation.

This section outlines the general compliance measures that all companies engaged in international business should consider. It then addresses specific compliance issues related to technology transfer, encountered through use of a company-wide computer network or information system and through employment of foreign nationals in the United States or abroad.

A. General Compliance Measures

There are certain basic elements that all competent corporate internal compliance programs (ICP) should include. BIS has recognized and encouraged exporters to embrace these elements. These elements also apply with respect to exports under jurisdiction of other agencies such as OFAC and DTC.[317] Whereas the precise scope and details of the program will depend on the nature and structure of a company's operations,

317. *See* BUREAU OF INDUSTRY AND SECURITY, ELEMENTS OF THE EXPORT MANAGEMENT SYSTEM GUIDELINES *available at* http://www.bxa.doc.gov/exportmanagementsystems/emsguidelines.html (last visited Apr. 5, 2003). The Hughes Electronics Corporation commissioned a study on best practices for complying with U.S. export controls. Press Release, Hughes Electronics, Nunn-Wolfowitz Task Force Establishes Best Practice Guidelines for Export Compliance (July 25, 2000), *available at* http://www.hughes.com/news/pr/00_07_25_report.asp.

the fundamental elements include the following:

1. Corporate Policy Statement

A written corporate policy statement discussing the importance of compliance with all export control laws and regulations is a fundamental starting point. The statement should: (1) send a clear signal from top management of the importance of compliance; (2) identify personnel ultimately responsible for export control compliance and for carrying out responsibilities, delegating authority as appropriate with a clear chain of command; (3) identify all regulations relevant to the company's current and potential business activities; and (4) establish notification procedures and punitive measures for failure to abide by the compliance program.

2. Product and Technology Classification

A threshold task in determining the types of compliance measures to be adopted is determining the regulatory classification of the products and technology that may be transferred by the company. Companies normally are best served by creating a chart or matrix that sets forth the controls applicable to the various products/technology produced, sold, or transferred by the company, by category and by destination. There must be close interaction between engineering and sales personnel so that the company correctly identifies applicable controls. Informed personnel must ensure that mechanisms are in place to keep current with regulatory changes over time.

3. Customer and End-User Screening

Both BIS and DTC significantly increased scrutiny of non-U.S. customers and end-users due to heightened concerns regarding terrorism and proliferation after September 11, 2001.[318] Customer screening is therefore a critical element of any

318. *See End-User Checks Playing Larger Role in State, BIS Enforcement*, WASH. TARIFF & TRADE LETTER, Jun. 17, 2002, at 2. In 2001, pursuant to its "blue lantern" inspection program, State conducted over 400 end-use investigations, finding that end-users were unfavorable in roughly 17% of the cases. *Id*. BIS investigated over 1,000 end-users through pre- and post-license checks in 2001. *Id*. at 3.

compliance program, notwithstanding the burden it may impose on the exporter.[319]

A company's technology base and customer profiles will determine its need to screen proposed transactions in order to avoid dealing with "prohibited" customers on a relevant agency's denial or specially designated national list.[320] Screening may be on a transaction-by-transaction basis or against a list of customers.

Proliferation controls require prior authorization if the exporter "knows" or has "reason to know" that the transaction is linked to restricted activity, namely weapons proliferation, even if the export is otherwise free from licensing requirements. There is a due diligence requirement associated with the knowledge standard that imposes a burden on exporters.[321] Exporters should determine whether there are any "red flags" when interacting with customers. Criteria for such red flags should be provided to sales and project personnel. Red flags include: (1) reluctance by the customer to offer end-use information; (2) inconsistencies between the sophistication of technology being transferred and the customer's capabilities; or (3) refusal by the customer to accept installation or routine maintenance. If a concern arises, exporters should assume that they have a duty to determine the actual use of the export. Companies should not "self-blind"—that is, they should not deliberately avoid information that could reveal a prohibited end-use.[322] As a general matter, exports of technology in intangible form often require a closer assessment of possible proliferation end-uses than transfers in tangible form.

Thus, exporters not only must screen customers against the denial lists published by relevant administering agencies, but

---

319. *See, e.g.*, *BXA to Provide New Batch of Guidance on Customer Screening*, EXPORT PRACTITIONER, Oct. 2000, at 5, 5 (stating that BIS's guidelines would require roughly eight hours of staff work plus $850 of online charges to screen a single customer).

320. *See, e.g.*, 31 C.F.R. ch. V, app. (listing blocked persons, specifically designated nationals, specifically designated terrorists, foreign terrorist organizations, and specially designated narcotics traffickers).

321. *See* 15 C.F.R. pt. 732 (Supp. 3 2003).

322. *Id.*

also must investigate customers not falling on such lists for any "red flags." BIS issued a partial list of such unverified end-users who were not subject to denial, but who were subject to thorough investigation.[323] It is unclear how much assistance such an "unverified" list will be to exporters, since it does not operate as a denial list. Exporters can take advantage of customer screening to comply with other U.S. regulatory requirements, such as anti-boycott and anti-bribery rules.[324]

4. Monitoring Activity of U.S. Persons and Entities Abroad

Under OFAC regulations, U.S. companies and U.S. persons in those companies may risk liability if their overseas affiliates engage in transactions with embargoed countries and OFAC decides the U.S. companies or persons participated. Likewise, in the EPCI context, BIS could arguably impute liability to U.S. companies or persons if an overseas affiliate ships to a prohibited end-use or end-user, and BIS decides the U.S. persons should have known. Companies should implement systemic measures to insulate U.S. persons from liability stemming from their foreign affiliates' conduct.

5. Clearance and Record Keeping

Compliance managers must ensure that proper screening procedures are undertaken on an order-by-order and transaction-by-transaction basis, with respect to the technology, the destination, the customer, and the end-use individual. When a license is required, the manager must ensure the application is completed and submitted, the license is received, and the company adheres to the license quality and value limits and to other license conditions. The manager also must ensure that, prior to shipment or transfer, applicable "choke point" controls

---

323. List of Unverified Persons in Foreign Countries, Guidance to Exporters as to "Red Flags," 67 Fed. Reg. 40,910, 40,910 (June 14, 2002). *See End-User Checks Playing Larger Role in State, BIS Enforcement*, *supra* note 318, at 2.

324. *See* 15 C.F.R. pt. 760 (listing anti-boycott rules); *see also* Commerce and Trade Securities Exchanges, 15 U.S.C. §§ 78dd, 78m (2000) (listing anti-bribery rules); *see also* Christopher F. Corr & Judd Lawler, *Damned If You Do, Damned If You Don't? The OECD Convention and the Globalization of Anti-Bribery Measures*, 32 VAND. J. TRANSNAT'L L. 1249, 1255–95 (1999) (discussing the anti-bribery rules).

are enforced and documented and that destination control statements accompany the transfer. For shipments of products and technology in tangible form, the manager must be sure that the shipper's export declaration is properly completed, and for transfers of technology in intangible form, that other special requirements are observed.[325] The manager also must ensure hard copy or electronic records of all relevant aspects of the export transaction are maintained. These records include purchase orders, invoices, and other sales documents, as well as regulating documents such as licenses, applications, end-use certificates, shipper's export declarations, and internal compliance records.

6. Training and Auditing

Companies should ensure relevant personnel receive ongoing, periodic, up-to-date training regarding applicable rules, the regulatory process, company policy, and changes that take place in the control regime. Training should be hands-on, and include more than the simple distribution of written materials. Training should extend not only to in-house export control managers, but also to in-house personnel who may be involved in technology transfer or export transactions.

Companies should arrange for periodic audits, either by in-house personnel or outside consultants, to investigate and verify whether the company is in compliance with regulatory controls on technology transfer. Management should review the results and make any necessary modifications to the system.

---

325. *See Customs Cites Fatal Exporter Mistakes*, EXPORT PRACTITIONER, May 2000, at 15, 15. Exports under a State Department DTC license have special requirements at the port, including mandatory lodging of the licenses with Customs, along with any amendments, and the provision of contact information for Defense Department officials when classified information is involved. The ITAR have other special requirements, including the recording of all exports of technical data under an exception with the relevant ITAR certification, the keeping of a detailed log of all transfers of technical data in intangible form (i.e., by visual, oral or electronic means), and forwarding to the DTC a copy of the duly executed shipper's export declaration. 22 C.F.R. §§ 123.22, 125.66 (2002).

7. Notification and Enforcement

The compliance program also should make clear to all officers and personnel involved in technology transfer and export controls the critical issues and circumstances that would require consultation with or notification to the in-house export control compliance manager. Such occasions would include orders for transfers of controlled technology abroad, the observation of any possible red flags in the order or delivery process, launches of new products and technology, the hiring of non-U.S. personnel, or visits by non-U.S. persons who may be given access to controlled technology.

The compliance system also should anticipate procedures for handling suspected violations of the program or the regulations. Employees should be encouraged to report all concerns regarding inconsistencies or violations to the in-house manager. There should also be established procedures for investigating any suspected violations and for taking appropriate follow-up measures, including external reporting and disclosure, appropriate sanctions, and cessation of any transactions or activities of concern pending resolution.

8. Due Diligence in Corporate Transactions

As discussed previously, BIS announced in late 2002 that "corporations will be held accountable for violations of U.S. export control laws committed by companies that they acquire."[326] This warning makes clear that, although the focus of export compliance programs is on day-to-day operations, the breadth and scope of U.S. export controls also may reach larger, higher-level corporate transactions. Multinational corporations, as well as financial companies such as commercial and investment banks, are well-advised to implement due diligence compliance measures in connection with mergers, acquisitions, and joint ventures, as well as distribution, licensing, and sales agreements.

---

326. *See BIS Seeks to Impose Liability on Firms That Acquire Exporters*, *supra* note 292, at 1. The BIS announcement was made in connection with a settlement in which an acquiring company agreed to pay a civil fine of $1.76 million to settle charges that a company it had purchased violated U.S. export controls. *Id*.

In addition to the threshold question of whether the contemplated transaction itself involves controlled technology transfers, due diligence checks on corporate acquisitions include an assessment of (1) whether the company to be acquired is involved in transfers of controlled technology and products, (2) whether the company has in effect an internal compliance program, (3) whether any of the target's customers or affiliates are listed as denied parties or are located in restricted countries, and (4) whether the company has been involved in any export control violations. Due diligence measures for other types of transactions such as joint ventures and distribution, licensing, and sales agreements include examining whether any other parties to the transaction are on an agency denial list or are located in restricted or embargoed countries. Other compliance measures may include the insertion of clauses in contracts and other documents disclaiming any express or implied assumption of liability for export control violations, as well as structural changes to the management or operations of an acquired company to limit liability.

B. Systems Compliance

As companies expand their global operations, they must integrate the worldwide workforce across timelines through use of the company computer network. Integrated, electronic communications and information sharing has its hazards, however. The possible transfer of controlled technology via a company's computer network raises special export control concerns and calls for special compliance measures.

Many U.S. companies operate networks that can be accessed through terminals in the United States, at the companies' subsidiaries and affiliates abroad, and through remote dial-in facilities in other countries. An effective compliance program must ensure that the computer network, particularly information-processing, operates consistently with U.S. export laws regulating the transfer of technology, software, data and other information to persons outside of the U.S. and to foreign persons within the United States. Given the many ways in which technology can be transferred, this is a difficult undertaking.

Under U.S. law, the term "export" is construed broadly to encompass technology transfers in many forms, as previously discussed.[327] Understandably, many business people find this broad definition to be counterintuitive. The term "export" includes: (1) transmission of data and software by email or otherwise over a computer network to foreign access points; (2) posting or storing information on a computer network such as a company intranet site or a shared library, folder, or database, if persons outside the United States have access; and (3) access of foreign nationals both abroad, and on-site in the United States, to network data and software.[328] Special compliance measures to prevent unlawful technology transfers via a company's computer network are discussed in the following sections.

1. Identification of the Technical Data and Software on the Network

A crucial initial step in compliance is for the company's technical personnel—normally from the information systems and engineering departments—to review all technical data and software on the network and to identify all technology and software subject to export controls. Technology subject to DTC and BIS restrictions generally is defined as information necessary for the development, design, production, use, or maintenance of hardware items subject to control.[329] Technology

---

327. *See supra* Part IV.A.1.b–c; *see, e.g.*, 15 C.F.R. § 734.2(b) (defining the export of technology or software as any release of technology or software subject to the EAR in a foreign country, or any release of technology or source code subject to the EAR to a foreign national); 15 C.F.R. § 734.2(b)(3) (specifying that under the EAR, technology is deemed to be "released" for export through visual inspection by foreign nationals of U.S. origin equipment, facilities, and technical specifications—such as reading technical specifications, plans, blueprints, etc.—oral exchanges of information in the U.S. or abroad, or the application to situations abroad of personal knowledge or technical experience acquired in the U.S.); 22 C.F.R. §120.17 (2002) (defining "export" to include disclosure—including oral or visual disclosure—or the transfer of technical data to a foreign person, whether in the U.S. or abroad); 31 C.F.R. § 500.310 (2002) (defining the term "transfer" in the context of OFAC regulations).

328. *See supra* Part IV.A.1.c (discussing deemed exports); s*ee also infra* Part VI.C (discussing compliance with controls on deemed exports).

329. *See* 22 C.F.R. § 120.10 (defining "technical data" subject to the ITAR as information "which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles");

subject to OFAC embargo restrictions is controlled with reference to the country to which the technology relates or is transferred.[330] After the technology, data, and software on the system are classified in this manner, the company should ensure that on an ongoing basis, it implements procedures to ensure that all future data put onto the system is reviewed and classified in a similar manner.

2. Segregation of Technical Data and Software Subject to Export Controls

The next compliance step is to segregate and protect the technical data and software found to be subject to export controls. This can be done by creating separate controlled files, folders or limited access databases, or by annotating or labeling the information. Controlled technical data and software should be subcategorized based on the types of controls applicable—for instance, whether ITAR or EAR controls apply and whether there are restrictions on all transfers outside the United States, or only transfers to embargoed countries.

3. Restriction of Transfers of Controlled Technical Data and Software

The most difficult compliance measure is to ensure that controlled technical data and software are not transferred to unauthorized non-U.S. citizens or non-U.S. locations, and to do so in a manner that does not disrupt or impair company communications. One threshold restriction is to limit who is given access to the company's computer system, and, within the system, who has access to protected databases and files. The system must restrict access not only from overseas terminals, but also from non-U.S. nationals who may be located in the United States.

Company information systems specialists, working with the

---

see also 15 C.F.R. § 772.1 (defining technology subject to the EAR in relation to items listed on the Commerce Control List at 15 C.F.R. pt 774 (Supp. 1 2003).

330. *See, e.g.*, 31 C.F.R. § 550.202 (2003) (sanctions against Libya); 31 C.F.R. §§ 575.315, 411 (2003) (sanctions against Iraq); 31 C.F.R. § 515.311 (2003) (sanctions against Cuba); *see also infra* Part VI.B.2–4 (discussing further how technology is defined and controlled).

export compliance manager, must develop a system of user identification and authentication that reflects export control priorities. One common measure is to correlate the use of passwords and log-in codes with a user's nationality or location, and to program the computer access system to cross-reference the nationality and location with specific restrictions in determining whether a particular user is entitled to a particular level of access. The log-in-authentication-safeguard system should provide for traceability, so that all information transfers on the system are recorded and can be identified later to demonstrate compliance or to investigate potential breaches. The overall aim is to prevent overseas users from having unregulated access on the U.S. network to controlled information that would require a license if it were actually exported to the user's destination, and limit unauthorized access by non-U.S. nationals to controlled technical information, regardless of the non-U.S. nationals' location. The system also should be programmed to prohibit transfers to customers or other parties who have been designated as subject to denial of export privileges.

An important screening measure is to restrict the country to which the technical data can be transferred. The network could be configured so that terminals outside the United States could not have access to certain categories of technical data and software absent additional screening steps in order to ensure all regulatory requirements were satisfied. The network also could be programmed to screen the address of each user requesting network access or a transfer of technical data, in order to verify that the user and the location of the user are permissible.

4. Direct Requests for Access to Controlled Technologies to Designated In-House Compliance Managers

When the system denies access pursuant to user or country screening measures, the request for access or transfer should be routed to the in-house compliance manager. The manager then can assess the facts and circumstances relating to the request, and can make a final determination as to whether access may be granted, the conditions under which access may be granted, and whether prior authorization from the relevant controlling

agency must be obtained. If it is determined that controlled technology may be transferred to a non-U.S. user or to a user outside the United States, the manager, or network itself, may attach a notice to the technical data or software indicating that it is subject to U.S. export control laws and that anyone having access to the data or receiving a transfer is subject to regulatory requirements, including restriction on re-transfer without prior authorization.

These special procedures for network compliance are in addition to the general measures discussed above in section A, including training and record keeping.

C. Compliance in Transfers to Foreign Nationals

In their quest to assemble the most talented workforce, U.S. companies increasingly hire foreign nationals in the United States and abroad. The hiring of skilled foreign personnel, particularly in areas of sensitive research and development, raises unique export compliance challenges, as a consequence of U.S. enforcement of the "deemed-export" rule. This rule restricts transfers to certain foreign nationals, wherever they are located, of technology that would be controlled if transferred to their country of citizenship.[331]

On the one hand, companies have an interest in hiring talented foreign nationals and allowing them access to modern tools of communication and analysis without excessive monitoring or oversight. On the other hand, as a matter of self-preservation, companies must undertake compliance with the deemed-export rule. As previously discussed, the administering agencies have committed to toughening their enforcement of the deemed-export rule. Toughened enforcement means increased investigations of companies in sensitive fields that employ a significant number of foreign nationals. It also means increased audits of companies that have obtained deemed-export licenses for foreign nationals in the United States, including an assessment of the companies' compliance programs and of their actual compliance with license conditions.

---

331. 15 C.F.R. § 734.2(b)(2)–(3); *see supra* Part IV.A.1.c (discussing the "deemed export" rule).

It is therefore incumbent on companies employing foreign nationals to implement due diligence measures, supplemental to the general compliance measures discussed in Section A above, to prevent unauthorized transfer of controlled data or technology to ineligible foreign nationals. For instance, one of the conditions for obtaining a deemed-export license is a description of the company's internal compliance program. These measures should be tailored to a company's organizational and technology structure to reduce the administrative burden and increase effectiveness. Given the many intangible ways in which information may be imparted to a foreign employee—verbally, electronically, or through physical access to controlled technology or areas—the implementation of effective compliance measures is a daunting challenge. The remaining subsections discuss key compliance measures.

1. Hiring and Identity Proofing

For companies that are involved with controlled technology or technical data, an important place to commence compliance with the deemed-export rule is at the time of hiring. The export compliance manager must work in coordination with the personnel or human resources office to ensure that when foreign nationals subject to the deemed-export rule[332] are hired, they are screened for export compliance purposes. These screening measures include identity-proofing through trusted documentation such as passports, licenses, etc. Depending on the foreign national's country of citizenship, the compliance manager must determine whether restrictions apply to the prospective employee's access to any technology and technical data at the company. If the applicant is hired, then the personnel office should provide credentials and authentication that reflect any legal technology restrictions.

---

332. Not all foreign nationals are subject to the deemed-export rule. For instance, green card holders, students and scholars are exempt. *See supra* text accompanying note 138.

2. Screening and Restricting Access

The most difficult task for the export manager is to ensure that ineligible employees are restricted from access to controlled technical data and technology at the company. Access to technical data and technology stored electronically on the company's computer network can be controlled through user authentication and log-in restrictions, as discussed above in Part VI.B. Depending on the job description of the ineligible foreign national, it also may be necessary to designate restricted areas within the company, such as research and development centers, where controlled technology and technical data are otherwise widely accessible. Such areas could be controlled by walling them off from generally accessible areas and restricting access to eligible employees through a guard, key, badge or fingerprint scan system.[333]

3. Licensing and Compliance with Licenses

Where it is determined that an employee's access to company technology or technical data is legally restricted, that no exception applies, and that the employee must have access to the technology to carry out the job functions, the compliance manager should ensure that the company applies for and receives a deemed-export license prior to granting the employee such access and adheres to all license conditions. Employees for whom a license has been obtained also may be requested to sign a certification that they will abide by the license conditions and report any unauthorized disclosures.

When submitting applications to the State Department and BIS, compliance staff can follow the same procedures and use the same forms as the normal export license process. However, deemed-export license applications typically must be supported by different or additional information and documentation including: evidence of the applicant's immigration status and country of citizenship; information regarding how the controlled technology received by the foreign national will be used

333. *See Safeguarding Instant Exports: Avoiding Deemed Export Violations with Technical Controls*, EXPORT PRACTITIONER, Oct. 2002, at 4, 5–6 (discussing screening procedures for deemed-export compliance).

pursuant to the employment; a letter of explanation providing further background on the applicant, the technology involved, and the job or project; an explanation of the company's need for the license and the benefit to be derived therefrom; a description of the company's internal compliance program to adhere to the conditions and prevent unauthorized access; and a detailed resume for the employee, including technical skills.

When deemed-export licenses are issued, they often are subject to conditions, such as restrictions on the foreign national's access to high-performance computers, advanced microprocessors, or certain semiconductor production equipment. The compliance manager should ensure that measures are undertaken to prevent unauthorized access.

In order to stay abreast of the restrictions applicable to different non-U.S. national employees, as well as the various licenses and license conditions under which these employees may operate, company compliance staff may maintain and update a folder for each such employee setting out the restrictions to which the employee is subject, the employee's job description, a copy of any deemed-export license, and a description of applicable compliance measures. Given the normal rate of employee turnover, as well as promotions and transfers within a company, the compliance staff must stay current on all restrictions.

In view of the difficulty of implementing deemed-export controls, the general compliance measures such as employee training and periodic audits, discussed above in Section A, take on added significance.

VII. CONCLUSION

> *Before I built a wall I'd ask to know what I was walling in or out, and to whom it was likely to give offense.*
>
> -Robert Frost

Despite the realignment of global security concerns in the new millennium and the reality that the United States alone no longer can control the flow of technology around the world, U.S. businesses continue to be subject to a vast array of export

controls with which their international competitors often need not comply. The controls can be futile because their target often can obtain the same technology from a non-U.S. source. By impeding the ability of U.S. high technology companies to compete in export markets, these controls too often prove counterproductive, harming elements of the U.S. high technology sector whose health is critical to the maintenance of the national defense.

This author believes that the case has been made for an overhaul of the U.S. export control regime with a view towards streamlined, rationalized controls on technologies that truly are critical to national security, and which either can be meaningfully controlled unilaterally by the United States without undercutting by third-country suppliers, or are subject to effective multilateral controls. The agencies charged with implementing national security and foreign policy controls must not lose sight of the fact that a robust, competitive, and technologically advanced U.S. industry is a fundamental prerequisite for a preeminent, self-reliant, and "smart" U.S. military.

Some questions merit careful consideration in devising a better system. If a technology or product is not critical to the national security, then why should controls be imposed on it? Given the importance of export controls to U.S. national security, the burden that these controls impose on U.S. exporters, and the evolving pace of geopolitical change and technological advancement, why are there no routine systemic assessments of U.S. security needs for restricting the transfer of particular technologies to particular countries? If a restricted country is able to obtain a technology or item from suppliers in a third country, then why should U.S. businesses be restricted from selling similar technology to the same end-user? Why should other agencies need to review a license application for security concerns when it has been established that the same technology is available to the intended recipient from other sources? Must export control licensing responsibilities be divided among multiple agencies?

Despite the need for export control reform in the post-Cold War era, it is evident that there will be no fundamental change

in the foreseeable future. As a consequence, U.S. businesses must learn to live with the current export control regime. Violations can be severely punished.

Companies involved in the transfer of technology and in international commerce would be well advised, as a matter of due diligence, to assess whether export controls apply to their business operations. If so, they should develop and implement internal compliance measures to ensure they adhere to all legal requirements in the simplest and least burdensome manner.