EXPORT CONTROLS AND THE PERILS OF NONCOMPLIANCE: WHAT BUSINESSES AND UNIVERSITIES NEED TO KNOW

LEVON E. WILSON*

I. INTRODUCTION

In the interest of national security, federal export control laws have been promulgated to regulate the distribution of strategically important products, services, and information to foreign nationals and countries. These laws apply to the transfer of physical items, information, and services. The primary agencies that are responsible for implementing and managing these laws are the United States Department of State through its International Traffic in Arms Regulations (ITAR) that are administered by its Directorate of Defense Trade Controls (DDTC), and the Department of Commerce through its Export Administration Regulations (EAR) that are administered by its Bureau of Industry and Security (BIS). Additionally, the Department of Treasury enforces economic sanctions and trade embargoes through its Office of Foreign Assets Control (OFAC). The Department of Treasury prohibits transactions with countries, entities, and individuals that are the target of boycotts or trade sanctions that have been imposed by the United States. These regulations must balance the desire for free trade and globalization, which is needed for economic growth, with the need to maintain national security.[1] While federal enforcement of international trade and security regulations in nothing new, there has been renewed emphasis in the area due to concerns about terrorism, coupled with the strengthening and corresponding enforcement of corporate ethics and liability laws.[2] This article will discuss the significance of these regulations to business operations and the responsibility of corporations in pursuing global markets while preserving national security interests.

II. INTERNATIONAL TRAFFIC IN ARMS REGULATIONS

The Department of State is responsible for control of the permanent and temporary export and temporary import of defense articles (such as weapons and technical data) to foreign countries to prevent the development of arms and weapons capabilities. The Arms Export Control Act (AECA) charged the President to "control the import and the

* J.D., Ed.D., Professor of Legal Studies, Georgia Southern University

[1] K. I. Juster, Remarks at the Update 2001 Export Controls and Policy Conference, (October 4, 2001), at http://www.bis.doc.gov/News/Archive2001/Juster@Update2001.htm (last visited March 8, 2007; author retains copy).

[2] H. L. Clark & S. Jayaram, *Intensified International Trade and Security Policies Can Present Challenges for Corporate Transactions*, 38 CORNELL INT'L L.J. 391-411 (2005).

export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services."[3] This authority was delegated under Executive Order 11958 to the Secretary of State.

The AECA served as the enabling legislation that led to the implementing regulations, or ITAR, which are also administered by the Department of State. These regulations primarily address the importation and exportation of defense related trade and technology transfers. The AECA also authorized the President to designate those items that should be considered as defense articles and defense services and to develop regulations for the import and export of such articles and services.[4] This list of controlled items constitutes the United States Munitions List (USML).[5] Under the regulations, anything on the list will require a license prior to being exported.[6] Further, companies must register with the State Department if they produce, furnish, or export items that require a license.[7] The twenty-one categories of USML items are inherently military in character, and include equipment, software, and military electronics, as well as chemical and biological agents.[8] Classification is based upon the capability of the product to be used for military purposes, and not whether or not the intended use of the article after export is for military or civilian purposes.[9]

For those items that are not specifically mentioned in the other categories of the USML, but which have military application, there is a catch-all category entitled *Miscellaneous Articles.* These items may also include technical data and defense services that are directly related to the defense articles that are specifically enumerated.[10] The nature of the information that is subject to restriction under the munitions list is not subject to judicial review, although a First Amendment challenge may be subject to review.[11] As it was originally enacted, according to Busch, the AECA imposed licensing and registration requirements only on persons that were engaged in the business of manufacturing, exporting, or importing USML articles and services.[12] Busch reports that Congress expanded the category in 1996 to include persons engaged in the business of brokering activities with respect to the manufacture, export, import, or transfer of USML articles and services.[13] *Brokering activities* are defined by statute to include "the financing, transportation, freight forwarding, or taking of any other action that facilitates the manufacture, export, or import of a defense article or defense service."[14] The regulations now detail the requirements for the registration and licensing of brokers as well.[15] All exports of USML items and technical data (such as blueprints, drawings, plans, instructions, diagrams and photographs) must be licensed

---

[3] 22 U.S.C. § 2778(a)(1) (2008).
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] 22 C.F.R § 122 (2008).
[8] *Id*. at § 120.10.
[9] J. R. Liebman & K. J. Lombardo, *A Guide to Export Controls for the Non-Specialist*, 28 LOYOLA LOS ANGELES INTERNATIONAL & COMPARATIVE L. REV. 497-516 (2006).
[10] *Id*.
[11] Karn v. U.S. Department of State, 925 F. Supp. 1 (1996).
[12] M.L. Busch, The D.C. *Circuit Review July 2004-July 2005: Recent Decisions of the District of Columbia Circuit: Foreign Affairs*, GEORGE WASHINGTON L. REV. 810-821 (2006).
[13] *Id.*
[14] 22 U.S.C. § 2778(b)(1)(A)(ii)(II)
[15] 22 C.F.R § 129 (2008).

by the Directorate of Defense Trade Controls (DDTC) unless expressly exempted.[16] The Arms Export Control Act directs that:

> [D]ecisions on issuing export licenses under this section shall take into account whether the export of an article would contribute to an arms race, aid in the development of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements or other arrangements.[17]

DDTC maintains a fully electronic defense trade licensing system, *D-Trade*, in order to facilitate the process.[18]

Items that are already in the public domain[19] are exempt from the license requirement and can, therefore, be disseminated without government control. Fundamental research and teaching (e.g., information and technology taught in university catalogue courses) would fall within the exemptions. It is not a crime to transmit information abroad that is expressly exempted from the statutory prohibition. The public domain limitation applies to *technical data*, not to items such as firearms or weapons on the USML, as the government may still preclude their export, even though such items might be available to the public in the United States.[20] In other words, actual shipments of USML items will always require a license.

As previously noted, ITAR provides an exemption for fundamental research, which is generally classified as being within the public domain. Fundamental research is defined in the regulations as "basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls."[21] The regulations provide that "university research will not be considered fundamental research if: (i) the university or its researchers accept restrictions on publication of scientific and technical information resulting from the project or activity, or (ii) the research is funded by the government and specific access and dissemination

---

[16] 22 C.F.R §§ 123 & 125 (2008).

[17] 22 U.S.C. § 2278(a)(2) (2008).

[18] D-Trade Information Center (2006). Directorate of Defense Controls, U.S. Department of State, http://www.pmddtc.state.gov/sl_dtrade.htm (last visited March 8, 2007; author retains copy).

[19] 22 C.F.R. § 120.11 (providing that "*public domain* means information which is published and which is generally accessible or available to the public: (1) Through sales at newsstands and bookstores; (2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; (3) Through second class mailing privileges granted by the U.S. Government; (4) At libraries open to the public or from which the public can obtain documents; (5) Through patents available at any patent office; (6) Through unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the public, in the United States; (7) Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency . . . ; (8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community.")

[20] E. Lee, *The Public's Domain: The Evolution of Legal Restraints on the Government's Power to Control Public Access Through Secrecy or Intellectual Property*, 55 HASTINGS L. J. 91 (2003).

[21] 22 C.F.R § 120.11(8) (2008).

controls protecting information from the research are applicable."[22] While industry-sponsored research at an institution of higher education may qualify for this exemption, care should be taken in defining proprietary rights. For example, according to Rege, if a laser manufacturer requires a review of sponsored research prior to publication in order to ensure that patent and other proprietary rights will not be compromised, or otherwise reserves the right to withhold publication if the results are not as expected, then the research no longer qualifies for the fundamental research exception under ITAR.[23]

Export means the actual sending or taking of a defense article or technical data out of the United States in any manner (except by a person merely traveling abroad whose personal knowledge includes technical data) or transferring its registration, control or ownership. However, *export* also means what is commonly referred to as a *deemed export*—that is, disclosing (including oral or visual disclosures) any defense article or technical data to a foreign person, or performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.[24] A *foreign person* means any natural person in the United States who is neither a citizen, a permanent resident (holding a valid green card), or a refugee or alien who has been granted asylum. The definition also includes foreign corporations, business associations, partnerships, trusts, or other entities that are not incorporated or organized to do business in the United States.[25] The conclusion drawn under the deemed export rule is that ultimately the foreign national will return to the home country, and the information will then be deemed exported.

According to Rege, these regulations of deemed exports can catch the unwary business by surprise. For example, as applied, a deemed export of information that would require a license could include a foreign national witnessing any demonstration or briefing, or using controlled equipment in a corporate research laboratory. It may also include United States employees of foreign subsidiaries sending non-public information (i.e., information not in the public domain) to themselves via email while overseas.[26] Rege further argues that the regulations could restrict industrial scientist-employees of corporations submitting articles for peer-review abroad, if the corporation retains proprietary rights to keep the information private.[27] Furthermore, because of the more strict requirements under ITAR, licensing requirements apply where technical data are to be disclosed or used in the performance of defense services, even in is in the public domain.[28] Thus, disclosure even of technical data in the public domain to a foreign national may require a license as well.

There are substantial criminal penalties for failure to obtain the appropriate license. Sanctions for the violation of ITAR are set forth in 22 U.S.C. § 2778(c). According to the statute:

> Any person who willfully violates any provision of this section or section 2779 of this title, or any rule or regulation issued under either section, or who willfully, in a registration or license application or required report, makes any untrue statement of a material fact or

---

[22] *Id.*

[23] Rowena Rege, *Universities Should Implement Internal Control Programs to Monitor Compliance with Export Control Laws*, 35 J. OF LAW & EDUCATION 199-223 (2006).

[24] 22 C.F.R. § 120.17 (2008).

[25] 22 C.F.R. § 120.16 (2008).

[26] Rege, *supra* note 23

[27] Rege, *supra* note 23, at 211-215.

[28] 22 C.F.R § 142.1 (2008).

> omits to state a material fact required to be stated therein or necessary to make the statements therein not misleading, shall upon conviction be fined for each violation not more than $1,000,000 or imprisoned not more than ten years, or both.[29]

Civil penalties up to $500,000 may also be assessed for each violation.[30] In addition, violators may be prevented from exporting defense articles and technical data, or furnishing defense services for which a license or approval is required. Such a prohibition is referred to as a *debarment* under the ITAR.[31] A debarment by the State Department will generally last for a period of three years.[32] It is the general policy of the State Department to encourage the voluntary "disclosure of information to the Office of Defense Trade Controls by persons, firms or any organization that believe they may have violated any export control provision of the Arms Export Control Act."[33] Voluntary self-disclosure, according to the Act, may be considered a mitigating factor in determining the imposition of appropriate administrative penalties.[34]

III. EXPORT ADMINISTRATION REGULATIONS

While ITAR regulates military items or defense articles, technology, and services, EAR covers dual use items. This refers to items that are designed for commercial purposes, but which may have military applications. Such items might include computers, global positioning devices, or aircraft. The term *dual use* is often used to distinguish the types of items covered by EAR from those that are covered by the regulations of other United States government departments and agencies with export licensing responsibilities.[35] The EAR are issued by the United States Department of Commerce Bureau of Industry and Security (BIS) under laws relating to the control of certain exports, re-exports, and activities.[36] Re-exports are commodities, software, and technology that have been exported from the United States to be exported again from the country to which the United States export was consigned.[37] In addition, the EAR implement anti-boycott provisions that prohibit specified conduct by persons from the United States that has the effect of furthering or supporting boycotts fostered or imposed by one country against another country that is friendly to the United States.[38]

The core provisions of the export control regulations of the EAR concern exports from the United States. Some provisions give broad meaning to the term *export*, sometimes applying it to transactions outside of the United States or to activities other than exports. Commodities, software, and technology that have been exported from the United States are generally subject to the EAR with respect to re-export. Many such re-exports, on the other hand, will go to many destinations without a license or may qualify for an exception from licensing requirements depending on the countries

---

[29] 22 U.S.C. §2778(c) (2008). Section 2779 authorizes the Secretary of State to establish reporting and record maintenance requirements.
[30] *Id*. at § 2780 (2008).
[31] 22 C.F.R § 127.7 (2008).
[32] *Id*. at §127.7(a) (2008).
[33] 22 C.F.R. § 127.12(a) (2008).
[34] *Id*.
[35] 15 C.F.R. § 730.3 (2008).
[36] *Id*. at § 730.1 (2008).
[37] *Id*. at § 772.1 (2008).
[38] *Id*. at § 730.1 (2008). These boycotts or restrictive trade practices are governed by 15 C.F.R. § 760 (2008).

involved.[39] Getting authorization to ship technology from the United States will, in some instances, be subject to additional assurances that items produced abroad as a byproduct of that technology will not be exported to certain countries without first obtaining authorization from BIS.[40] To counter the proliferation of weapons of mass destruction, EAR restrict the involvement of United States persons anywhere in the world in exports of foreign-origin items, or in providing services or support that may contribute to such proliferation. The EAR also restrict technical assistance by United States persons with respect to encryption commodities or software.[41]

Certain actions that might not be regarded as an export in other contexts do constitute an export under the EAR.[42] For example, technology or software is *released* and deemed to be an export if it falls within one of the three broad categories defined in the regulations.[43] If a United States researcher sends an electronic transmission of data that is not *public*, yet will be received outside of the United States, it may be considered an export. In the case of research sponsored by the federal government, some material may be prevented from being disseminated. Thus, a researcher violating these restrictions may be subject to sanctions under the export control laws.[44] When an item is controlled, a license may be required before the technology can be exported. Other examples of exports under the EAR include the return of foreign equipment to its country of origin after repair in the United States, shipments from a United States foreign trade zone, and the electronic transmission of non-public data that will be received abroad.[45] A *foreign national*, as used in these provisions, is any person who is not a: 1) United States citizen or national, 2) United States lawful permanent resident, 3) person granted asylum, 4) person granted refugee status, or 5) temporary resident. Persons in the United States in non-immigrant status and persons unlawfully in the United States would be deemed foreign nationals.[46] A relatively small percentage of exports and re-exports subject to EAR require an application to the BIS for a license. Many items are not on the Commerce Control List (CCL).[47] In some instances, even if they are on the CCL, they may require a license to only a limited number of countries. Other transactions may be covered by one or more of the license exceptions to the EAR. In such cases, no application need be made to the BIS.[48] License requirements under EAR are dependent upon an item's technical characteristics, the destination, the end-user, and the end-use. The exporter must determine whether or not an export requires a license. When making that determination, consideration must be given to: 1) what is being exported, 2) where it is being exported, 3) who will receive the export, and 4) for what purpose the export will be used.[49] The BIS maintains the CCL, which includes

---

[39] *Id*. at § 730.5(a) (2008).
[40] *Id*. at § 730.5(b) (2008).
[41] *Id*. at § 730.5(d) (2008).
[42] *Id*. at § 734.2(b)(3) (2008).
[43] *Id*. The regulations provide that "technology or software is released for export through: (i) visual inspection by foreign nations of U.S.-origin equipment and facilities; (ii) oral exchanges of information in the United States or abroad; or (iii) the application to situations abroad of personal knowledge or technical experience acquired in the United States."
[44] Rege, *supra* note 23.
[45] 15 C.F.R. § 730.5(c) (2008).
[46] *Id*. at § 734.2(b)(2) (2008).
[47] *Id*. at § 774.1, Supplement No. 1 (2007).
[48] *Id*. at § 730.7 (2008).
[49] Introduction to Commerce Department Export Controls, 2007, Bureau of Industry and Security, U.S. Department of Commerce, http://www.bis.doc.gov/licensing/esportingbasics.htm (last visited April 6, 2008; author retains copy).

items (e.g., commodities, software, and technology) subject to its authority. The CCL is divided into 10 categories,[50] numbered as follows:

0 – Nuclear Materials, Facilities and Equipment and Miscellaneous
1 – Materials, Chemicals, Microorganisms, and Toxins
2 – Materials Processing
3 – Electronics
4 – Computers
5 – Telecommunications and Information Security
6 – Lasers and Sensors
7 – Navigation and Avionics
8 – Marine
9 – Propulsion Systems, Space Vehicles and Related Equipment

Within each category, items are arranged by group. Each category contains the same five groups.[51] Each group is identified by the letters A through E as follows:

A – Equipment, Assemblies and Components
B – Test, Inspection and Production Equipment
C – Materials
D – Software
E – Technology

In order to determine if an item is on the CCL, an exporter should begin with a review of the general characteristics of the item to be exported. This will usually guide the exporter to the appropriate category within the CCL. Once the appropriate category is identified, the exporter should match the particular characteristics and the functions of the item to a specified Export Control Classification Number (ECCN). Within each group, individual items are identified by an ECCN. A brief description is provided for each ECCN. There is also information relating to *License Requirements*, *License Exceptions*, and *List of Items Controlled*. The CCL identifies all possible reasons for control, in order of restrictiveness, and the extent to which each applies. The accompanying country chart identifies almost every country in the world and contains licensing requirements based on destination and reasons for control.[52] Export controls under EAR rely almost entirely on self-regulatory behavior by exporters. This is a result of the regulations themselves, as well as the lack of enforcement resources available to BIS and the small percentage of exports that require a license.[53] Morris reports that ninety-six percent of

---

[50] 15 C.F.R. § 738.2(a) (2008).

[51] *Id*. at § 738.2(b) (2008).

[52] *Id*. at § 738. Regulations regarding license exceptions are promulgated in 15 C.F.R. § 740 (2008). The EAR contains a number of exceptions to licensing requirements. In addition to the main categories of exemptions, the EAR also provides for comprehensive licenses for multiple exports and re-exports, as well as special exemptions for some encryption exports. *See* George W. Bowman, *Emails, Servers and Software: U.S. Export controls for the Modern Era*, 35 GEO. J. INT'L L. 319 (2004). No license is required for the export of public information and software. 15 C.F.R. § 734.7(a)(1)(2008). Information is considered to be public or in the public domain if it has been published and is generally accessible to the interested public in any form. *Id*. at § 734.7(a). Examples of information in the public domain include periodicals, books (both print and electronic), and any other media that is available for general distribution to members of the public. It also includes information available at public libraries, patents and published patent applications available at any patent office, and information that is released at open conferences, meetings, seminars, trade shows, or other similar public gatherings. *Id*. at § 734.7(a)(1)-(4).

[53] M.G. Morris, *The Executive Role in Culturing Export Control Compliance*, 104 MICHIGAN L. REV. 1785-1808 (2006).

exports do not require licensing, which, he suggests, forces BIS to economize the use of its enforcement resources. While BIS provides some level of enforcement of violations of the regulations, according to Morris, the preferred method is to prevent violations through education and guidance.[54] Sanctions for violation of EAR are set forth in 15 C.F.R. § 764.3. Whoever willfully violates or conspires to violate any provision of the EAR will be subject to a fine of "not more than five times the value of the export or re-export involved or $1,000,000, whichever is greater; and, in the case of an individual, shall be fined not more than $250,000, or imprisoned not more than 10 years, or both."[55] There are also administrative sanctions for civil violations that include monetary penalties, denial of export privileges, and exclusion from practice.[56] The regulations further indicate that "items that have been, are being, or are intended to be exported or shipped from or taken out of the United States in violation of the EAA, the EAR, or any order, license or authorization issued thereunder, are subject to being seized and detained as are the vessels, vehicles, and aircraft carrying such items."[57]

BIS strongly encourages disclosure of any violations of the EAR to the Office of Export Enforcement (OEE).[58] If a person learns that an export control violation of the EAR has taken place, he or she may provide notification to the appropriate authorities.[59] Voluntary self-disclosure is a mitigating factor here just as it was in reporting ITAR violations to the Department of State.[60] While voluntary self-disclosure may be considered as a mitigating factor in determining the administrative sanctions that might be sought by the OEE, it is only one among all factors that will be considered in the case. The mitigating aspect of voluntary self-disclosure may be outweighed by the other factors. The amount of weight to be attributed to this factor is within the sole discretion of the OEE.[61]

IV. OFFICE OF FOREIGN ASSETS CONTROL

The third category of export controls is administered by the Office of Foreign Assets Control (OFAC), which is located in the United States Department of Treasury. The office is responsible for enforcing economic and trade sanctions that are in the best interests of United States foreign policy and national security. The Department of

---

[54] *Id.*

[55] 15 C.F.R. § 764.3(c)(2)(i) (2008).

[56] *See* 15 C.F.R. § 764.3(a)(1)(i) (providing that "a civil penalty not to exceed $10,000 may be imposed for each violation, except that a civil penalty not to exceed $100,000 may be imposed for each violation involving national security controls imposed under section 5 of the EEA").

[57] 15 C.F.R. § 764.3(c)(2)(i) (2008). Any seized items would be subject to forfeiture under the regulations.

[58] 15 C.F.R. § 764.4 (2008).

[59] *Id.* at § 764.4 (a) (2008). (The actual addresses, as well as telephone, and facsimile numbers of the offices to which these reports should be made are provided in the regulations.)

[60] *Id.* at § 764.5 (2008).

[61] Voluntary self-disclosure will not prevent transactions from being referred to the Department of Justice for criminal prosecution. *See* 15 C.F.R. § 764.5(4) (2006). If a person learns that an export control violation of the EAR has occurred or may occur, that person may notify the OEE, which is a division of the U.S. Department of Commerce, Bureau of Industry and Security. Notification of violations of anti-boycott provisions of the EAR should be sent to the Office of Antiboycott Compliance, which is a separate division of the U.S. Department of Commerce, Bureau of Industry and Security.

Treasury imposes economic sanctions against various countries from time to time.[62] When economic sanctions are imposed, United States persons are prohibited from engaging in economic interactions with the target country. These provisions may also restrict dealings with designated persons (e.g., foreign nationals) and entities, such as persons who are affiliated with a sanctioned country. These restrictions may include parties who are connected to terrorist activities, or those who may be involved in international drug trafficking.[63] Additionally, the property of certain persons or entities from other countries with questionable domestic or foreign policies, such as The Congo, Belarus, The Cote d'Ivoire, Zimbabwe and the Balkans, may be frozen from time to time, and trading privileges suspended. It is important for businesses to remain abreast of such foreign policy developments, and to monitor OFAC's list of *Specially Designated Nationals* (SDNs), which can be front companies, parasitical entities, or individuals determined to be owned or controlled by, or acting for or on behalf of, targeted countries or groups, as well as *Blocked Persons*, who are specially identified individuals, such as terrorists or narcotics traffickers. United States entities are prohibited from engaging in any transactions with them, and must block any property in their possession or under their control in which the targeted counties, groups, or blocked persons have an interest.

In addition to violating sanctions against SDNs, economic sanctions can be violated by United States firms in several non-obvious ways, for example, 1) by purchasing an approved foreign firm's assets, which happen to include supply contracts with a sanctioned entity, 2) by investing in a joint venture if other participants include sanctioned parties or sanctioned entities, or 3) by acquiring even a minority interest in the shares of an approved company that engages in significant sales to a sanctioned customer.[64] Of course, licenses may be obtained from OFAC to engage in a transaction that otherwise would be prohibited. There are two types of licenses: general licenses, which authorize a particular type of transaction for a class of persons without the need to apply for a license, and specific licenses, which is a written document issued by OFAC to a particular person or entity, authorizing a particular transaction in response to a written license application.[65] For example, the Clinton Administration authorized commercial sales of food, medicine, and medical equipment to Iran on a case-by-case basis to approved buyers with certain payment restrictions.[66] Compliance with the regulations enforced by OFAC can be challenging because they are broad, ambiguously drafted, and often interpreted by the Treasury Department in a far-reaching and undocumented manner.[67] OFAC does not provide any lists or detailed regulations that are comparable to the USML or the CCL. There are, however, various provisions in the Code of Federal Regulations that outline the available sanctions against certain target countries or entities.[68] Therefore, transactions with any of these targeted countries, or other entities identified as proliferation risks, should be handled with extreme caution,[69] as failure to comply with trade sanctions can prove to be very costly. Fines for

---

[62] Author's commentary: The Department of Treasury has imposed economic sanctions against a variety of countries, including Burma (Myanmar), Cuba, Iran, Sudan, Libya, North Korea, and Syria.

[63] Clark & Jayaram, *supra* note 2.

[64] Clark & Jayaram, *supra* note 2.

[65] 31 C.F.R. § 501.801 (2008)).

[66] J.H. Donboli & F. Kashefi, *Doing Business in the Middle East: A Primer for U.S. Companies*, 38 CORNELL INTERNATIONAL L. J. 413-458. (2005).

[67] Clark & Jayaram, *supra* note 2.

[68] Liebman & Lombardo, *supra* note 9.

[69] *Id*.

violations often can be substantial. Depending on the program, criminal penalties can include fines ranging from $50,000 to $10,000,000 and imprisonment ranging from 10 to 30 years for willful violations, while civil penalties range from $11,000 to $1,000,000 for each violation.[70] In determining a settlement amount or penalty assessment, OFAC considers whether or not the institution made a deliberate effort to conceal the violation, along with any useful enforcement information provided during an OFAC audit, investigation, or penalty proceeding.[71]

V. IMPLICATIONS FOR UNIVERSITY RESEARCH

These export controls provisions are particularly challenging to colleges and universities because they require balancing concerns about national security and economic vitality against the academic traditions of unrestricted freedom and the unfettered publication and dissemination of research findings and results.[72] Much of what universities do is covered by one or more of the exemptions that fall under the classification of fundamental research, official use, teaching, or public domain.[73] University based research normally will be considered fundamental research unless the research results are subject to prepublication review.[74] If a university or its researchers accept restrictions or limitations on the publication of scientific or technical information resulting from a research activity, that activity will not be considered fundamental research.[75] As long as the research results are not shielded from public access, it will not be subject to the EAR licensing requirements; thus, foreign national employees need not be licensed prior to the release of such information to them.

The EAR includes a very helpful set of questions and answers relating to technology and software that is subject to the EAR. It provides guidance in interpreting

---

[70] Most recently, Vesper Corporation remitted $23,800 to settle allegations of violations of the Cuban Assets Control Regulations and Iranian Transactions Regulations, Tyco Valves & Controls Middle East, Inc., remitted $450,905.50 to settle allegations of violations of the Iranian Transactions Regulations, EMD Chemicals, Inc., remitted $8,250 to settle allegations of violations of the Iranian Transactions Regulations, and Encore Medical, L.P., successor by merger to Chattanooga Group, Inc., remitted $3,241.20 to settle an alleged violation for disregarding licensing requirements for the export of physical therapy equipment to Iran . *See* OFAC Enforcement Information, 2007, Office of Foreign Assets Control, U.S. Department of Treasury at http://www.treas.gov/offices/enforcement/ofac/actions/20070213.shtml.

[71] C.A. Wray & R. K. Hur, *Corporate Criminal Prosecution in a Post-Enron World: The Thompson Memo in Theory and Practice*, 43 AMERICAN CRIMINAL L. REV. 1095-1188 (2006).

[72] *Export Controls and Universities: Information and Case Studies*, Council on Governmental Relations (2004). http://www.cogr.edu/docs/export%20controls.pdf (last visited April 6, 2008; author retains copy).

[73] The fundamental research exception under the EAR protects basic and applied research in science and engineering where the resulting information is ordinarily shared through publication within the scientific community, but it does not protect proprietary research that is restricted for proprietary research or because of specific national security reasons. 15 C.F.R. § 734.8(a).

[74] 15 C.F.R. § 734.8(b)(1). There are several similarities between the EAR exceptions and the ITAR exemptions relating to fundamental research. Under the ITAR, fundamental research is included under the public domain exception. There is not a separate category, as there is under the EAR. The fundamental research exception under the EAR also includes publicly available technology and software that arises during or results from fundamental research. 15 C.F.R. § 734.3(b)(3)(ii) (2008).

[75] *Id*. at § 734.8(b)(5). It is permissible to conduct a limited prepublication review without losing the exception if it is limited to ensuring that the publication does not compromise proprietary rights in the information or that it does not violate patent rights.

the scope of the EAR licensing requirements. These questions and answers provide guidance relating to publications, conferences, instruction, research, consulting, and other matters that will be helpful to those working within universities and colleges.[76] The fundamental research exemption under ITAR is more limited than under EAR. As previously noted, the EAR is concerned with dual use items, whereas the focus of ITAR is with items that are inherently military in nature. The ITAR includes the concept of defense services, which includes the furnishing of training and or technical data that relates to ITAR-controlled items to foreign persons either in the United States or abroad. The EAR provisions tend to be clearer and more specific in its coverage than the ITAR.[77] In addition to the public domain, fundamental research, and teaching exemptions, an additional exemption is also relevant to universities.[78]

VI. CONCLUSION

Compliance with this complicated maze of export regulations can be daunting for corporations, particularly small companies as well as universities and colleges.[79] Costs include the expenses involved in maintaining an inventory of the equipment and technology that are subject to ITAR and EAR, as well as applying for export licenses and deemed export licenses for foreign national employees and affiliates.[80]

---

[76] Scope of Export Administration Regulations, Questions and Answers—Technology and Software Subject to the EAR, Supplement No. 1 to Part 734, http://www.gpo.gov/bis/ear/pdf/734.pdf (last visited April 6, 2008; author retains copy).

[77] *Export Controls and Universities: Information and Case Studies*, Council on Governmental Relations (2004). http://www.cogr.edu/docs/export%20controls.pdf (last visited April 6, 2008).

[78] *Id*. This additional exemption is available for disclosures of unclassified technical data in the United States by U.S. institutions of higher education to foreign persons who are their bona fide and full-time regular employees. This exemption is available if: "(i) the employee's permanent abode throughout the period of employment is in the United States; (ii) the employee is not a national of a country to which exports are prohibited pursuant to Section 126.1 (of the ITAR): and (iii) the institution informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of the Directorate of Defense Trade Controls." 22 C.F.R. § 125.4(10).

[79] Export controls can complicate corporate transactions in several ways, for example: 1) by necessitating export licenses and other export approvals as well as the need for amended or new ITAR registrations which require government approval; 2) by requiring notifications regarding certain types of corporate transactions involving ITAR-registered companies, and often State Department reviews of transactions to verify whether a party is a reliable exporter; 3) by triggering more intensive scrutiny of compliance records in assessing whether the proposed transaction would threaten the national security, particularly with companies that generate sensitive export-controlled technology; and 4) by recognizing successor liability for export control violations committed by the acquired entity before the acquisition. *See* Clark & Jayaram, *supra* note 2. DDTC admittedly applies the doctrine of successor liability to deter fraudulent restructuring designed to escape liability; for example, in 2003 Boeing Company paid $32 million to settle charges resulting from the provision to several Chinese nationals by Hughes Space and Communications ("HSC," a subsidiary of Hughes Electronics) of controlled data on the failed launches of two commercial communications satellites mounted on Chinese-origin rockets, even though Hughes Electronics reserved liability for any pre-acquisition export violations in the sale of HSC to Boeing See also A.X. Fellmeth, *Cure Without a Disease: The Emerging Doctrine of Successor Liability in International Trade Regulation*, 31 YALE J. INT'L L., 127-188 (2006).

[80] B.C. Findley, Revisions to the United States Deemed-Export Regulations: Implications for Universities, University Research, and Foreign Faculty, Staff and Students, 4 Wisconsin L. Rev. 1223-1274 (2006).

Badway argues that current export control regulations put American businesses, especially small companies, at a competitive disadvantage with European competitors. He states that most small companies cannot afford the added expense of a staffed compliance program. He further notes that European competitors often face less stringent controls, making it easier for them to export dual purpose goods more promptly.[81] This result is particularly disconcerting since the technologies the controls are attempting to protect to the detriment of American business, are often readily available elsewhere. More often, the controls do little more than delay the inevitable exportation, while demanding excruciating attention to detail with respect to the license application.[82] This supports the argument being made by some that recommend terminating the transaction based approval program that is currently in place and replacing it with regional or partner based trade agreements.[83] On the other hand, Sievert[84] counters that simply because enemies of the United States can acquire articles from non-United States suppliers does not mean that United States companies should not be vigilant and exercise corporate responsibility in the exportation of goods and services in the interest of national security. However, he admits that the current export control system could be relaxed somewhat, especially on those shipments to firms, organizations, and countries that have demonstrated a history of using such items for peaceful purposes and do not further transfer or re-export the items.[85]

Nevertheless, compliance programs and risk assessment plans are essential to United States businesses and universities that deal in either dual use or defense related articles, technology, or services. If companies fail to comply with export control laws, they often find themselves involved in protracted defense litigation, which is often time consuming and costly. Companies may experience the loss of exporting privileges and debarment from government contracts. They may also be faced with the prospect of bad publicity that often flows from these events. To ensure compliance in this regulatory framework, companies should conduct self-audits based on the risk of non-compliance and develop internal controls, including an export control compliance manual that identifies red flags to consider for compliance-triggering transactions, such as shipping to new customers, sending data and specifications to suppliers, developing new product lines, hiring new employees, and sharing technology.[86] Dunn developed a comprehensive model compliance program for companies that includes appropriate forms and lists specific red-flag alerts to heed at critical processing points. [87]

The Bureau of Industry and Security, which administers the licensing program for the Commerce Department, provides support for companies to implement compliance systems in order to establish a process for the evaluation of the requirements and the documentation of compliance with those requirements based upon the type of product being exported, the country to which the product is being exported, the entity or person

---

[81] A.A. Badway, *Controlling the Export of Dual-Use Technology in a Post-9/11 World*, 18 TRANSNAT'L LAW., 431-454 (2005)

[82] M.D. Klaus, *Dual-Use Free Trade Agreements: The Contemporary Alternative to High-Tech Export Controls*, DENV. J. INT'L L. & POL'Y, 105-134.

[83] *Id*.

[84] R. J. Sievert, Urgent Message to Congress - Nuclear Triggers to Libya, Missile Guidance to China, Air Defense to Iraq, Arms Supplier to the World: Has the Time Finally Arrived to Overhaul the U.S. Export Control Regime? - The Case for Immediate Reform of Our Outdated, Ineffective, and Self-Defeating Export Control System, 37 TEX. INT'L L. J., 89-109 (2002).

[85] *Id.*

[86] A. Doornaert, *Export Controls of the U.S. Government: Scope and Legal Challenges*, 84 MICH. BAR J., 28-31 (Dec. 2005).

[87] T.L. Dunn, *Surviving United States Export Controls Post 9/11: A Model Compliance Program*, 33 DENV. J. INT'L L. & POL'Y, 435-559 (2005)

to whom the product is being exported, and the applicable requirements in such circumstances.[88] Drawing from these resources, Rege[89] provides suggestions for the implementation of an Internal Control Program (ICP) for universities to ensure compliance. This program would be beneficial to business operations as well. First, companies should develop a policy statement clearly indicating their commitment to complying with export control laws. Second, they should fortify the policy with education programs and training manuals for key personnel. Third, they should identify a department with primary responsibility for ensuring compliance and implementing a comprehensive accounting system, which maintains records of completed transactions for at least five years, as generally required by BIS and DDTC. Fourth, the company should conduct periodic internal reviews to verify compliance, including unannounced visits to relevant areas of the operations. Fifth, the business should implement a well-publicized system of notification procedures to follow for questions that may arise regarding the propriety of specific transactions, which includes corporate counsel in the information loop. Finally, procedures should be in place to continuously monitor OFAC's list of Specially Designated Nationals, as well as BIS's *Denied Person List*, which registers individuals and entities that have been denied export privileges and with whom business may not be transacted. Such measures, if implemented, would serve to create a corporate culture of compliance. As companies are under an obligation to self-regulate, corporate leadership must create such a culture of compliance and ensure that violations do not occur, particularly since enforcement provisions consider compliance as an aggravating or mitigating factor once culpability is determined.[90]

---

[88] M.J. Meagher, *Heads Up: Complying with Export Control Laws*, 46 BOSTON BAR JOURNAL, 14-15 (May/June 2002). The Directorate of Defense Trade Controls in the State Department also provides guidelines for a compliance program (Guidelines for DTC Registered Exporters/Manufacturers Compliance Program, 2006). DDTC suggests that companies develop operational compliance programs, which include manuals that articulate the processes to be followed in implementing the company program. It advises that manuals and programs include 1) a detailed organizational structure which describes the company's trade functions and control structures for tracking compliance, 2) a directive by senior management indicating corporate commit-ment to ensure compliance, 3) methods tailored to the corporate structure, organization and functions which are designed to identify, tag, and account for export controlled items, data, and transactions, 4) procedures for the re-export and re-transfer of items or technical data, 5) procedures for screening customers, carriers and countries for restricted or prohibited exports and transfers, 6) the implementation of a recordkeeping system for U.S. origin products, 7) the establishment of and internal audit system for periodic compliance checks, 8) a company training program on export control regulations, 9) procedures for the notification of potential violations and employee discipline, and 10) the establishment of an Ombudsman office to investigate problems and provide independent evaluations on the effectiveness of the compliance program.

[89] Rege, *supra* note 23.

[90] M.G. Morris, *The Executive Role in Culturing Export Control Compliance*, 104 MICH. L. REV. 1785-1808 (2006).