Complying with Immigration, Export Control, and Industrial Security Requirements When Working Collaboratively with Foreign Nationals: A Case Study[1]

M. Beth Peters, David W. Burgett, and Joy E. Sturm*

With the trend toward globalization of the economy, U.S. companies are increasingly seeking to hire and work with foreign nationals. These individuals may be sought to fill marketing and business positions or to assist in selling products and services abroad. Moreover, the rapid growth in the information technology sector has resulted in an increased need for highly skilled engineers and computer scientists on the part of technology companies in the United States.[2] Whether U.S. companies are tapping into the non-U.S. workforce or simply interacting with teaming partners or potential customers, they face an intricate web of immigration, export control, and national security laws and regulations. The lack of centralization and limited coordination among the agencies that regulate these areas makes compliance particularly challenging.

The first regulatory hurdle raised in connection with hiring or working with foreign nationals is in the area of immigration law. U.S. companies must consider and comply with immigration laws and requirements implemented and administered by the U.S. Immigration and Naturalization Service (INS) and certain other agencies when hiring or simply working with foreign nationals in the United States.

The export control regulations are another set of regulatory constraints that apply when hiring or working with foreign nationals. Administered primarily by the U.S. Departments of Commerce and State, with the participation of the Department of Defense (DOD), these regulations place restrictions on companies employing foreign nationals under what is frequently referred to as the deemed export[3] rule. Under this rule, U.S. companies and federal agencies are required to treat access by a foreign national to controlled technology and

*M. Beth Peters and David W. Burgett are partners and Joy E. Sturm is an associate in the law firm of Hogan & Hartson, L.L.P.

1. This article is an adapted version of an article that previously appeared in the West Group publication *Briefing Papers* and *Immigration Briefings* in 2000. This article is being published with the express permission of West Group.

2. Ruth Ellen Wasem, Congressional Research Service, Immigration and Information Technology Jobs: The Issue of Temporary Foreign Workers 1–7 (May 12, 1998).

3. The term deemed export comes from Commerce Department parlance and is intended to refer to transfers of technology or software data to foreign nationals within the United States. While the specific term, deemed

software as an export to the foreign national's home country. Given the introduction of legislation recently that would provide more severe penalties for violation of these regulations and the increase in high-profile export control enforcement actions, it is perhaps more important than ever to ensure compliance with these detailed regulations. Recent enforcement actions include the assessment of a $10 million fine against the Boeing Company in 1998 for transferring restricted technical data to joint venture partners from countries including Russia and Ukraine in connection with the Sea Launch satellite program.[4] In another recent case involving deemed exports, two high-tech companies in California were indicted in October 2000, for allegedly transferring microwave technical data that has military applications in radar to Chinese nationals in the United States.[5]

A third set of restrictions applies to companies that work under federal contracts or programs that require access to classified materials. In addition to the export controls described above, DOD industrial security regulations restrict the sharing of classified information with foreign nationals as well as the influence or control by foreign nationals with respect to such classified work. These restrictions have received increased attention in the wake of the 1999 indictment of a U.S. physicist at Los Alamos National Laboratory for allegedly mishandling classified information[6] and a 1999 report released by a U.S. House of Representatives Select Committee[7] that was critical of government and private adherence to national security controls.

This paper presents a case study involving a U.S. company's proposed interactions with foreign nationals that raises issues under the various regulatory frameworks. The paper is divided into sections addressing compliance with the following: (1) immigration regulations; (2) export control regulations, including the deemed export rule; and (3) DOD industrial security regulations. Each section provides a description of the legal framework, and then analyzes the regulatory issues raised in the case study.

I. The Case

Gearco, a U.S. company that designs protective gear, seeks to hire certain foreign nationals and to work collaboratively with a non-U.S. company. The company has several divisions that are located in separate buildings in an industrial park. Gearco's Civilian Gear Group focuses solely on the development of basic protective gear that it sells to civilian organizations such as police departments and civilian search and rescue units. Another division within the company, the Military Products Group, develops more sophisticated protective gear in conjunction with military forces of the United States and various other countries. Some of the gear developed by this group is used for protection of individuals

---

export, is not used in the State Department export control scheme, State Department regulations classify such transfers under the definition of export and place similar types of restrictions on them. For ease of reference, the term deemed export is used throughout this paper to refer to this concept in both the State Department and Commerce Department regulatory contexts.

4. Walter Pincus, *Boeing Fined $10 Million for Data Transfer to Ukraine*, N.Y. TIMES, Oct. 3, 1998, at A-6.

5. *Federal Indictment Returned Against California Companies in Case Involving Transfer of Information to Foreign Nationals*, 42 GOVERNMENT CONTRACTOR No. 41, ¶ 431, at 1 (Nov. 1, 2000).

6. Jennifer Weeks & John P. Holdren, *Energy Secrets: Finding the Balance*, 56 BULL. ATOM. SCIENTISTS, Mar. 1, 2000, at 20–21.

7. Report of the Select Committee on U.S. National Security and Military/Commercial with China, H.R. Rep. No. 105–851 (1999). Also, during the past year, a number of DOD Inspector General reports have documented violations of the industrial security regulations by DOD agencies. *See, e.g.*, Office of Inspector General, Department of Defense, Report No. D-2001-007, *Foreign National Security Controls at DOD Research Laboratories* (Oct. 27, 2000).

in the armed forces and other organizations. This gear is designed to reduce detection by radar and other sensor equipment. Other products developed by this division are designed for protection against chemical and biological agents. The company also has another division—the Federal Systems Group—that works on classified DOD contracts involving the development of protective technologies. While the Federal Systems Group was established as a subsidiary of the Gearco parent organization, the other two divisions—the Civilian Gear Group and the Military Products Group—are operations within the parent company. The Federal Systems Group is the only group within the company that may access classified information; it alone holds a facility security clearance.

In recent months, Gearco's Civilian Gear Group has been contemplating entering into an agreement with a French company, GearFrance, pursuant to which GearFrance would assist Gearco's Civilian Gear Group in the production of certain lines of protective gear. Gearco wishes to have five employees of the French company visit Gearco's offices in Morristown, New Jersey for a period of two to four weeks to collaborate on the design and development of the protective gear lines using Gearco's proprietary technology. The group of employees includes two French nationals, two Canadian nationals, and one person who is a citizen of both Pakistan and the United Kingdom.

At the same time, Gearco's Military Products Group has identified two foreign nationals to work in its commercial satellite division. It wishes to hire a person who was born in China and has become a citizen of the United Kingdom. He is currently in the United States, having recently received a Ph.D. in Materials Science from the University of Pennsylvania School of Engineering and Applied Science. The Chinese-British dual national would be hired to work on the development of new materials and technologies for next generation protective gear. In addition, because the vice president of Gearco's Military Products Group has recently resigned, Gearco is seriously considering hiring an Israeli executive who currently works overseas at a company that produces protective technologies similar to those developed by Gearco. The Israeli national is currently working and living in Israel and will need to be flown to Gearco's offices in New Jersey for a final round of interviews. Assuming she accepts the job, she will need to relocate to the United States.

It is evident that Gearco's plans will require analyses under U.S. immigration and export control regulations. Additionally, because one of Gearco's divisions—the Federal Systems Group—works on classified programs, Gearco will have to consider the industrial security requirements before it hires foreign nationals or permits non-U.S. citizens to visit the facility occupied by that group.

II. Immigration Law Considerations

Immigration laws and regulations come into play both where a company intends to host a foreign national as a non-employee (e.g., a consultant or joint venture collaborator) and where a company seeks to employ a foreign national in a temporary or permanent position. The INS, a component of the Department of Justice, and the Departments of State and Labor each play a role in regulating the employment of foreign nationals. The INS and the State Department share the responsibility for determining the immigration status for which a foreign national may qualify. The INS also enforces the immigration laws at U.S. borders. The State Department oversees the U.S. embassies and consulates abroad that issue visas to qualified foreign nationals seeking entrance to the United States for specified periods. In addition, the Department of Labor ensures that companies planning to employ foreign nationals meet certain prescribed labor conditions.

A. Immigration Status Determination

The first step when considering whether to hire a foreign national is to determine the individual's immigration status. If the foreign national is already in the United States, a company must determine whether the individual is in the country on a temporary basis or is a legal permanent resident (LPR) (as evidenced by an alien registration card, or green card, a refugee, or an asylee). A refugee or asylee in the United States generally will have an employment authorization document evidencing that individual's authorization to work in the United States. LPRs, refugees, and asylees are eligible to work in the United States, and a U.S. employer may therefore hire them without sponsoring them for a visa or work authorization. Moreover, as discussed below, export licensing requirements necessitated by certain transfers of U.S. technology or software to a foreign national generally do not apply to individuals in these categories.

If the foreign national is not an LPR, refugee, or asylee and does not otherwise have authorization to work in the United States, the prospective employer must determine whether the person will qualify for a nonimmigrant visa that will permit the person to work for the company in the United States. The appropriate visa category depends on a variety of factors, including, but not limited to, the requirements of the position, the length of employment, where the person will be employed, and the individual's education and work experience. Business visitors and individuals identified for employment by a company are eligible for different visa categories, as described below.

B. Business Visitors

When seeking to have a foreign national come to the United States for a visit—but not for employment—a B-1 visa is appropriate. The B-1 business visitor visa category covers persons who are employed abroad and need to enter the United States for a short period of time to engage in business activities, such as meetings and consultations.[8] A person who performs services as an employee of a U.S. company and receives remuneration for such activities generally is not eligible for B-1 status. The foreign national must apply for the B-1 visa at a U.S. embassy or consulate abroad. For a meeting or plant visit that has been set in advance, a letter from the U.S. company describing the meeting or visit typically is submitted with the B-1 visa application. If the embassy or consulate issues the B-1 visa, the INS will admit the foreign national under a B-1 visa for the period of time required, generally not to exceed six months.[9]

Foreign nationals from certain designated North Atlantic Treaty Organization (NATO) countries and other U.S. allies, such as France, Germany, Japan, Italy, and Spain, have been able to enter the United States for business purposes for up to ninety days without a visa under the Visa Waiver Pilot Program. Severe penalties may be assessed if the individual stays in the United States beyond the ninety-day period or is employed by a U.S. company during that period.[10] Although the Visa Waiver Pilot Program expired on April 30, 2000, legislation permanently extending the program was enacted in October 2000.[11]

8. Immigration Regulations, 8 C.F.R. § 214.2(b) (2000).
9. *Id.*
10. *Id.* § 217.2.
11. Visa Waiver Permanent Program Act, Pub. L. No. 106–396, 114 Stat. 1637 (2000).

C. Temporary Employment of Foreign Nationals

There are a number of visa categories that may apply where a company seeks to employ a foreign national who is not an LPR, refugee, or asylee temporarily in the United States. Nonimmigrant visa categories commonly used to sponsor foreign nationals include, but are not limited to the H-1B, L-1, H-3, and TN visa categories. Additionally, students with F-1 or J-1 status also may be eligible to work for U.S. employers.

1. *H-1B Visa*

A foreign national may be eligible for an H-1B visa if the person will provide services in "a *specialty occupation* which requires theoretical and practical application of a body of highly specialized knowledge."[12] The position must require at least a bachelor's degree or equivalent and the person must meet the minimum requirements for the position.[13] A company may sponsor an individual for H-1B status for a three-year period, which can be extended to a maximum stay of six years.[14] Congress has established caps on the number of new H-1B petitions that can be approved for various fiscal years. For FY 2000, the INS was permitted to approve only 115,000 new H-1B petitions.[15] In October 2000, legislation was enacted to increase the H-1B cap to 195,000 for the next three fiscal years.[16] Foreign nationals in the United States with H-1B status who merely change employers and extend their status may be sponsored by a new employer for H-1B status without being subject to this cap.[17]

2. *L-1 Visa*

If a company wants to temporarily transfer a person it employs from abroad to the United States, the individual may be eligible for L-1 status as an intracompany transferee. A foreign national who has been employed abroad for one continuous year within the preceding three years by a qualifying organization can be admitted temporarily to the United States to work for a "parent, branch, affiliate, or subsidiary of that employer in a managerial capacity or executive capacity, or in a position requiring specialized knowledge."[18] Generally, a qualifying organization is a U.S. or foreign entity that is doing business as an employer in the United States and in at least one other country directly or through an affiliate.[19] In the case of a manager or executive, an individual is eligible to be transferred to a U.S. employer for an initial period of no more than three years, which can be extended for a total of seven years in L-1 status in the United States.[20] A person with specialized knowledge can enter the country in L-1 status for an initial period of no more than three years, which can be extended for a total of five years.[21]

---

12. 8 C.F.R. § 214.2(h)(4)(i)(A)(1) (emphasis added).
13. *Id.*
14. *Id.* §§ 214.2(h)(9)(iii)(A)(1), 214(h)(15)(ii)(B)(1).
15. *Id.* § 1184(g)(1)(A)(iii).
16. American Competitiveness in the Twenty-First Century Act, Pub. L. No. 106–313, 114 Stat. 1251 (2000).
17. 8 C.F.R. § 214.2(h)(8)(ii)(A).
18. *Id.* § 214.2(l)(1)(i).
19. *Id.* § 214.2(l)(1)(ii)(G).
20. *Id.* §§ 214(l)(11), (l)(15)(ii).
21. *Id.*

3. *H-3 Visa*

An H-3 visa is appropriate in cases where a company seeks to have a foreign national come to the United States to engage in structured training with the intention that the individual will leave the United States to apply that training abroad.[22] To sponsor a foreign national for H-3 status, a company must establish that: (1) there is a structured training program in place in which the foreign national will participate (typically requiring a classroom or similar component and that the position does not consist primarily of on-the-job training); (2) the training is not available to the foreign national outside the United States; and (3) the training is necessary for the foreign national to be able to do his job overseas.[23] Training may be approved for a period of up to two years.[24]

4. *TN Visa*

Under the North American Free Trade Agreement (NAFTA), Mexican and Canadian nationals are eligible under the TN category to enter the United States to work in certain professional capacities.[25] Canadian nationals are permitted to apply to the INS for TN status at the border immediately before entry and are not required to have a visa.[26] For Mexican nationals, a TN petition must be submitted to the INS, which, if approved, will enable the individual to apply for a TN visa at a U.S. embassy or consulate abroad.[27] TN status is valid for no more than one year but is renewable on an as-needed basis.[28]

5. *F-1 Visa/J-1 Visa*

Typically, foreign national students graduating from U.S. universities will be in the United States on F-1 or J-1 visas. Graduates who are in F-1 or J-1 status may be eligible to work for U.S. employers if they receive practical training authorization.[29] For example, after graduation, F-1 and J-1 students generally are eligible for a period of practical training for up to one year[30] and eighteen months,[31] respectively. Such practical training does not require the U.S. employer to file a sponsoring petition with the INS. After the period of practical training is concluded, the employer must decide whether to sponsor the student for a work visa, if eligible. In certain cases, the U.S. employer may petition the INS to change the foreign student's status from F-1 to H-1B, for example, without requiring the student to leave the country.[32]

D. Permanent Employment of Foreign Nationals

If a company seeks to employ a foreign national on an indefinite basis, it can sponsor the individual for permanent residence (i.e., a green card). Ordinarily, the first step toward

22. *Id.* § 214.2(h)(7).
23. *Id.* § 214.2(h)(7)(ii).
24. *Id.* § 214.2(h)(9)(iii)(C)(1).
25. *Id.* § 214.6.
26. *Id.* § 214.6(e).
27. *Id.* § 214.6(d).
28. *Id.* §§ 214.6(d)(3)(iii), (f)(1), (h).
29. *Id.* §§ 214.2(f), (j).
30. *Id.* § 214.2(f)(10), (11).
31. *Id.*
32. *Id.* § 248.1.

sponsorship is to obtain a labor certification from the Department of Labor stating that there are no qualified and available U.S. workers to fill the position in the area of intended employment.[33] Certain foreign nationals are exempt from labor certification, including multinational executives and managers, persons with extraordinary ability, and persons with advanced degrees or exceptional ability whose employment is in the national interest.[34] Once a labor certification is issued, the sponsoring employer must file a preference petition with the INS seeking approval to employ the individual in the certified position. If the petition is approved, the individual is eligible to apply for permanent resident status either at a U.S. embassy or consulate abroad, or at the INS if the person is already in the United States legally.[35] The difficulty often faced by employers is that increasing backlogs in applications have resulted in substantial delays (for two to four years) before an individual is able to obtain permanent resident status.[36] A foreign national often will work for a U.S. employer in a nonimmigrant category until the green card process is completed.

Whether a company plans to hire foreign nationals for temporary or permanent employment, it should consider the processing time required for any necessary visa or work authorization in order to ensure compliance with the immigration requirements. Failure to comply with the U.S. immigration laws can subject a company to civil and criminal penalties, particularly if a company knowingly employs foreign nationals without proper work authorization.

E. Gearco Analysis

Gearco has to consider the immigration law requirements in three contexts: (1) for the visiting individuals from GearFrance; (2) for the Chinese-British dual national who Gearco wishes to hire to work as an engineer in Gearco's Military Gear Group; and (3) for the Israeli national who is being considered for the vice president position in that same division. With respect to the GearFrance employees whom Gearco seeks to have visit Gearco's offices, it is fairly clear that they may enter the United States temporarily on B-1 visas to discuss design and development issues with Gearco's Civilian division. The B-1 visas are appropriate because the GearFrance employees will enter the United States as business visitors for the purpose of attending extended business meetings and consultations with Gearco and because they will remain employees of GearFrance and will not be under the employ of Gearco. It should also be possible for the GearFrance employees with French, Canadian, or U.K. passports to travel to the United States without a visa under the Visa Waiver Program.

In contrast to the individuals from GearFrance, who will enter the United States as business visitors, the individuals who were identified for employment in Gearco's Military Products Group will require, at a minimum, temporary work visas. With respect to the Chinese-British dual national who just received a Ph.D. in Materials Science from a U.S. university, it is likely that this individual currently holds an F-1 visa, which was obtained in

33. *See id.* § 1182(a)(5)(A); *see also* 20 C.F.R. pt. 656 (2000).

34. 8 U.S.C. §§ 1182(a)(5)(D), 1153(b).

35. *Id.* §§ 1255(a), 1202(a); 8 C.F.R. § 245.1; 22 C.F.R. § 42.41.

36. The American Competitiveness in the Twenty-First Century Act of 2000, enacted in October 2000, is intended to enhance the ability of H-1B workers to move among companies during the green card process. Pub. L. No. 106–313, 114 Stat. 1251 (2000).

order for him to be able to study in the United States. Individuals with F-1 visas generally are eligible to work in the U.S. for a period of practical training for up to one year. To the extent that this Chinese-U.K. dual national will be staying with the company beyond the one-year period, it will be necessary for Gearco to sponsor the individual for a work visa. As the Chinese-U.K. dual national will be working in a position requiring a bachelor's degree in engineering or materials science, it will be appropriate for Gearco to file an H-1B petition on his behalf. Gearco could sponsor the individual for H-1B status for an initial period of three years that can be extended up to six years. If he intends to stay with the company for longer than six years or for an indefinite period of time, it will be necessary to sponsor him for permanent residence.

As for the Israeli national traveling to the United States for a final round of interviews for the vice president slot at Gearco's Military Products Group, she will be eligible to apply for and obtain a B-1 visa for the visit. Assuming she is offered and accepts the position, she will need to relocate to the United States. Because she will be employed in a specialty occupation as well, Gearco will need to file an H-1B petition with the INS in order to authorize her to work in the United States on a temporary basis. As with the Chinese-British dual national engineer who is currently in the United States, if it is determined that she will be with the company and working in the United States for more than six years, it will be necessary to sponsor her for permanent residence.

III. Export Control Requirements: The Deemed Export Rule

The federal government imposes significant restrictions on the export of goods, services, and technology that are grounded in U.S. foreign policy and national security considerations. It is well known that shipment of goods from the United States to another country is an export that potentially may be subject to export licensing or other restrictions. But, it is less widely known that delivery of data to a foreign national—even within U.S. borders—can be deemed to be an export of the data to the foreigner's country of nationality. This deemed export rule often requires companies to obtain licenses or take other steps before releasing controlled information to foreign nationals. Because the processing of export licenses and required authorizations can take a significant period of time, ninety days or longer, companies often must delay employment of foreign nationals or restrict the type of work they do and segregate them from access to certain technical data until an export license is secured. This rule often affects U.S. high-tech and electronics firms that routinely hire foreign nationals, as well as defense contractors that hire or collaborate with foreign persons on government contracts for the development of defense items and technology.

A. Export Law Jurisdictional Framework

Most export control regulations come within the jurisdiction of one of two federal agencies: (1) the State Department's Office of Defense Trade Controls (ODTC) or (2) the Commerce Department's Bureau of Export Administration (BXA). The ODTC administers and enforces the International Traffic in Arms Regulations (ITAR),[37] promulgated under the Arms Export Control Act.[38] Under the ITAR, the ODTC regulates the export of de-

37. 22 C.F.R. pts. 120–30.
38. 22 U.S.C. § 2778.

fense articles and services and implements various UN embargoes. The BXA administers and enforces the Export Administration Regulations (EAR),[39] promulgated under the Export Administration Act (EAA),[40] which regulates the export of dual-use (i.e., suitable for both military and nonmilitary use) items and services.[41] The EAR implements a number of multilateral export control agreements, including agreements of the Nuclear Suppliers Group, the Missile Technology Control Regime, the Australia Group, and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.[42]

In addition to the BXA and the ODTC, the Treasury Department's Office of Foreign Assets Control (OFAC) implements various comprehensive sanctions programs by controlling exports to certain terrorist-supporting and embargoed destinations (including, but not limited to, Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Yugoslavia), organizations, and individuals.[43] OFAC's authority derives from a number of statutes, including IEEPA and the Trading with the Enemy Act.[44] OFAC has concurrent licensing authority with the BXA (and, to a limited extent, the ODTC) for exports to certain countries and organizations subject to OFAC sanctions programs.[45] Where concurrent jurisdiction exists, licensing is often centralized in one of the agencies (e.g., OFAC handles licensing for most countries subject to OFAC sanctions programs, but the BXA exercises jurisdiction for exports of certain items to Cuba).[46] Whenever an export to one of these countries is contemplated, OFAC regulations should be consulted.[47] Depending on the country at issue, deemed exports may be controlled under various OFAC programs.

Moreover, several other agencies, including the Department of Energy and the Nuclear Regulatory Commission, exercise limited export jurisdiction over items and data that they are charged with regulating.[48] If an export will involve information within any such agency's jurisdiction, that agency's regulations must be consulted, as well.

B. What Is a Deemed Export?

Under the two main export control regimes—the EAR and the ITAR—an export does not have to cross national borders to be subject to export controls. Rather, when a company

39. 15 C.F.R. pts. 730–74 (2000).

40. Although the EAA technically expired in 1994, BXA's authority to administer and enforce the export control regulations has been extended several times by Executive Order under the authority of the International Emergency Economic Powers Act (IEEPA). 50 U.S.C. §§ 1701–06 (2000). In November 2000, however, legislation was enacted that reinstated the EAA through August 2001. Since 1994, Congress has repeatedly considered legislation that would effect a new and revised EAA, with stronger enforcement mechanisms. However, a new law has yet to be enacted. It is anticipated that legislation will be considered in 2001 that would serve to modernize the EAA. *See Export Controls: Senate Votes to Reinstate Export Control Law, Stiffer Penalties for Export Violations*, Fed. Cont. Rep (BNA) (Oct. 17, 2000).

41. 50 U.S.C. app. §§ 2401–20 (2000).

42. Anne Q. Connaughton, *Exporting to Special Destinations or Entities: Terrorist-Supporting and Embargoed Countries, Sanctioned Countries or Entities*, *in* Coping with U.S. Export Controls 369, 385 (Evan Berlack & Cecil Hunt eds., 1999).

43. *See* 31 C.F.R. ch. 5. (2000).

44. *See* 50 U.S.C. app. §§ 1–44 (2000).

45. *See* 15 C.F.R. § 734.3; *see also* R. Richard Newcomb, *Office of Foreign Assets Control*, Coping with U.S. Export Controls, *supra* note 42, at 109, 117.

46. *See, e.g.*, 15 C.F.R. § 746.7(a)(3) (OFAC authorization of export to Iran does not require separate authorization from BXA).

47. 31 C.F.R. ch. 5 (2000).

48. *See* 15 C.F.R. pt. 730 (Supp. III 2000).

permits a foreign national access (within the United States *or* abroad) to controlled information, an export is deemed to have occurred to that person's country of nationality.[49] Thus, under the scenario involving Gearco, Gearco's provision of technical data to an Israeli national temporarily working in the United States is effectively treated as an export to the country of Israel. Such exports, in many cases, require licensing or approval from the U.S. government.

There are many circumstances in which a deemed export can occur. For example, a deemed export may occur when a company hires a foreign national, when it works collaboratively with foreign nationals employed by other companies, or when foreign nationals merely visit a company or attend training sessions. The deemed export rule covers virtually any means of communication to the foreign national—including telephone conversations, e-mail and fax communications, sharing of computer data, briefings, training sessions, and visual inspection during plant tours and visits.[50] The rule also covers deemed re-exports that occur when technology or software has already been legally exported to an end-user in one country (e.g., a foreign company) and foreign nationals from another country are permitted to come into contact with that licensed technology.[51]

Under the EAR, the deemed export rule covers the release of technology or software source code[52] (but not object code) to a foreign national.[53] Technology is defined broadly to include "information necessary for the 'development,' 'production,' or 'use' of a product" and includes "technical data" or "technical assistance."[54] Technical assistance may include instruction or consultation as well as the transfer of "technical data," including blueprints, plans, diagrams, models, manuals, and instructions written or recorded on "media or devices such as disk, tape, [and] read-only memories."[55] Importantly, under the EAR, the deemed export rule applies to software only if source code is released.[56]

Similar to the EAR, the ITAR restricts the disclosure of technical data to "a foreign person, whether in the United States or abroad."[57] The ITAR specifies that the term foreign person includes foreign individuals, foreign corporations, and foreign governments.[58] Technical data includes information[59] "required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles . . . [including] information in the form of blueprints, drawings, photographs, plans, instructions and documentation."[60] Unlike under the EAR, however, restricted technical data generally includes software (both source code and object code).[61] The ITAR further

49. *Id.* § 734.2(b)(2); 22 C.F.R. § 120.17.
50. 15 C.F.R. § 734.2(b)(3); 22 C.F.R. §§ 120.17, 125.2(c).
51. 15 C.F.R. §§ 734.2(b)(4), (5); 22 C.F.R. § 125.1.
52. Source code describes the creative instructions authored in a programming language that are intelligible to human readers; object code, on the other hand, is source code instructions translated into binary format, which are intelligible only by a computer system. *See* http://foldoc.doc.ic.ac.uk/foldoc (detailing definitions of source code and object code).
53. 15 C.F.R. at § 734.2(b)(2)(ii).
54. 15 C.F.R. § 772.1.
55. *Id.*
56. *Id.* § 734.2(b)(2)(ii).
57. 22 C.F.R. §§ 120.17(a)(4), 120.9(a)(2).
58. *Id.* § 120.16.
59. *Id.* § 121.8(f).
60. *Id.* § 120.10.
61. *Id.* § 120.10(a)(4).

includes within the definition of technical data classified information relating to defense articles and services and information covered by an invention secrecy order.[62] Under the ITAR, technical data may be considered a defense article or furnished as a defense service pursuant to a collaborative agreement between a U.S. entity and a foreign person.[63] For ease of reference, the term technology will be used to refer to both technical data and technical assistance.

The EAR and the ITAR do not control publicly available information.[64] Under the EAR, publicly available information is defined as information that is or will be published for general circulation, results from fundamental research, is educational, or is included in certain patent applications.[65] Under the ITAR, this category includes information concerning "general scientific, mathematical or engineering principles," "information in the public domain," and "basic marketing information on function or purpose or general system descriptions of defense articles."[66] Examples of publicly available information under both regimes include, among many other things, documents posted on an Internet website, books, and papers presented at public conferences.

The reasoning behind the deemed export rule is that foreign nationals who do not immigrate to the United States are likely to return to their home countries eventually, and when they do, they will bring with them knowledge of the controlled technology to which they have had access. Both the EAR and ITAR versions of the rule are limited only to certain technology and software—and not to finished products—because the "know how" required to make products is considered far more valuable than the products themselves. When another country receives such know-how, there is no limit on how many products can be made. Another serious concern is that such know-how can be enhanced or improved to create more sophisticated technology and products.

Although the deemed export rule does not apply to controlled equipment or items as such, there may be situations in which access by a foreign national to a particular controlled item may actually constitute a release of technical data and, therefore, a deemed export. Although the regulations do not specifically address this situation, if mere viewing of an item can reveal technical data, such exposure by a foreign national might well be considered a deemed export.[67] Whether technical data would be revealed likely would depend on the level of technical expertise of the individual having access to the item. For example, an export might occur if an engineer were permitted to view a tank brake assembly (an ITAR-controlled defense item) while on a site visit.[68] However, if a marketing executive with a liberal arts background were permitted the same access, the executive probably could not deduce any technical data from the brake assembly, and an export likely would not occur.

The likelihood of obtaining an export license depends in large part on the nature of the technology or software and on the home country of the foreign national. Not surprisingly, obtaining a license for an individual from a NATO or other allied country will be far easier

62. *Id.* §§ 120.10(a)(2)-(3).
63. *Id.* §§ 120.21, .22.
64. 15 C.F.R. § 734.3(b)(3); 22 C.F.R. §§ 120.10(a)(5), .11.
65. 15 C.F.R. § 734.3(b)(3).
66. 22 C.F.R. §§ 120.10(a)(5), .11.
67. *See* Maarten Sengers & John Black, *Showing Defense Articles to Foreign Nationals in the U.S.: No License Required?*, EXPORT PRAC., Oct. 1999, at 12.
68. *See id.* at 12–13.

than for a foreign national from one of the more sensitive destinations. It may be difficult or impossible to obtain a license if the foreign national is from a country subject to U.S. sanctions administered by OFAC, such as Cuba, Iran, Iraq, Libya, Sudan, or Yugoslavia. Other countries that also may present licensing obstacles include India, China, and certain former Soviet republics. Because foreign policy and national security concerns play a significant role in determining the export treatment the United States accords a given country, companies must assess the current political and regulatory environment when contemplating a deemed export.

It is important to have sufficient lead time to deal effectively with licensing requirements when considering hiring or planning for collaborative work with foreign nationals—especially those from sensitive destinations. Problems may be avoided by taking the time to thoroughly understand the deemed export rule and by implementing internal compliance procedures to help personnel detect deemed exports and to provide guidance on how to proceed under the licensing requirements.

C. Immigration Status Considerations

A threshold inquiry in dealing with the foreign nationals rule is whether the individual who requires access to technology or software is considered a foreign national (under the EAR) or a foreign person (under the ITAR) of one or more countries.[69] Under both regulatory frameworks, the release of controlled technology or software to certain protected individuals under the Immigration Reform and Control Act (IRCA) of 1986 is not restricted.[70] Included within this protected class are legal permanent residents (green card holders), refugees, asylees, and temporary residents under certain IRCA amnesty provisions. Permanent residents who do not take steps toward naturalization and citizenship in a timely manner are not included within this class.[71] Individuals within this protected class may be employed or otherwise exposed to controlled technology and technical data without triggering any export licensing or approval requirements.

If a license for a deemed export will be difficult or impossible to obtain for a prospective employee in light of the nature of the technology or software and the employee's country of nationality, a company may consider seeking to sponsor the individual for permanent residence. As noted above, this process may take anywhere from two to four years, and therefore may not be a viable option. Moreover, while waiting for such approval, the company must ensure that the foreign national is not permitted access to any covered technology or software.

In addition, where an individual is a citizen or permanent resident of more than one country, nationality/immigration status under the EAR and ITAR also must be considered. Under the ITAR, the ODTC treats a dual national as a national of both countries. Thus, if an export would be prohibited to either country of nationality, the ODTC would deny an export license.

Until recently, the approach taken by the BXA had been consistent with that of the ODTC. However, in summer 2000, the BXA adopted a different standard in applying the EAR that provides, generally, that the "last permanent resident status or citizenship ob-

69. 15 C.F.R. § 734.2(b)(ii); 22 C.F.R. §§ 120.16, .17.
70. *See* 8 U.S.C. § 1324b(a)(3) (cited in 15 C.F.R. § 734.2(b)(ii); 22 C.F.R. §120.16)).
71. *Id.*

tained governs."[72] It provided: "for individuals who are citizens of more than one foreign country, or have citizenship in one foreign country and permanent residence in another, as a general policy, the last permanent resident status or citizenship obtained governs [for purposes of the deemed export rule]."[73]

D. Identification and Classification of the Technology

If a foreign national subject to the deemed export rule will require access to controlled technology or software, the information must be identified and analyzed to determine whether the EAR or the ITAR applies. If a company engages in export transactions, it necessarily will have classified the commodities and/or technology it exports abroad to comply with the basic EAR and ITAR requirements. Moreover, if a company manufactures defense articles or provides defense services subject to the ITAR, it is required to register with the ODTC even if it does not engage in export transactions.[74] Nonetheless, when considering whether to hire or to work collaboratively with a foreign national, it is necessary to classify all internal technology and software that the foreign national may access—and this may include information other than that which the company may generally export abroad.

In undertaking this analysis, a company must first determine the relevant "exposure parameters." For example, if an engineer is needed, the company must determine whether the person requires access to product design, product development, or production data. If the foreign national is hired to work in sales or management, it must determine the level of technical understanding of relevant product lines that will be necessary.[75] In addition, the company must consider whether the person will attend meetings or may otherwise be exposed to technical data relating to projects other than the person's own.[76]

Not only must a company consider the physical layout and security aspects of the facility where the individual will work, but it is also important to consider the level of access the individual will have to online information. For example, it should consider whether the person will work on a stand-alone computer or will be linked with others on a network and whether the network has password protection that will prevent the foreign national from accessing information that is controlled under the EAR or ITAR. If a company maintains a corporate intranet that contains any controlled technical data, it also must consider whether and to what extent the person's access can be limited.

E. Does the EAR or ITAR Apply?

Once the exposure parameters are determined, a company must ascertain which, if any, regulatory jurisdiction governs the export of the technology or software. In other words, a company must classify the technology or software as either subject to the BXA's jurisdiction under the EAR or the ODTC's jurisdiction under the ITAR. It is also necessary to deter-

72. *See Control Freaks: Deemed Recovery*, Export Prac., Aug. 2000, at 9; *see also* http://www.bxa.doc.gov/DeemedExports/DeemedExportsFAQs.

73. *Id.*

74. 22 C.F.R. § 122.1.

75. Lisa Caplinger, *Putting Together a License Package for Hiring a Foreign Person*, Soc'y for Int'l Affairs News Notes, Mar. 1997, at 4–6, *available at* http://www.sined.org/nnmar97.htm/#putting.

76. *Id.*

mine whether the data may be subject to control by any other agency, including the Department of the Treasury, the Department of Energy, or other agencies, depending on the nature of the information and the nationality of any foreign nationals who may require access.[77]

Exports of most commercial nonmilitary items, including commodities, technology, and software, come within the jurisdiction of the BXA and are regulated under the EAR. The EAR applies to dual-use items (items that could be suitable for both military and nonmilitary use) as well as to various items that have no military use but are considered to require protection for national security or other reasons. The EAR's Commerce Control List (CCL) sets forth a series of entries describing the items subject to licensing requirements and the bases for control. The CCL contains ten categories: nuclear materials; chemicals and toxins; materials processing; electronics; computers; telecommunications (including satellite communications technology) information security (including encryption items); lasers and sensors; navigation and avionics; propulsion systems; and certain space vehicles. Each category is further subdivided into various groups, including separate groups for technology and software—the two groups that come into play under the deemed export rule.

In contrast to the BXA's jurisdiction, the ODTC mainly regulates defense articles, defense services, and related technical data and software.[78] Articles, services, and related technical data covered by the ITAR are on the U.S. Munitions List (USML), which includes twenty-one categories of both classified and unclassified items. The USML includes the following items as well as related services and technical data: military equipment, military electronics, military cryptographic items and equipment, ammunition, spacecraft systems and associated equipment, and nuclear weapons design and test equipment.[79] The ITAR also covers certain nonmilitary items and technologies, including commercial satellites and related technical data.[80]

If it is unclear whether particular technology or software is subject to BXA or ODTC jurisdiction, a company can request that the ODTC determine the proper classification under its commodity jurisdiction procedure. This may involve consultations among the Departments of State, Commerce, and Defense.[81] Once a company has determined which regulatory regime applies, it must analyze whether licensing for a deemed export is required based on the nature of the relevant technology or software and the country of nationality of the foreign national who requires access.

F. Gearco Analysis

Based on the facts of the study set forth at the outset of this paper, the visit to Gearco by GearFrance employees would involve access to technical data relating to civilian protective gear. This would appear to be covered under the EAR's CCL under ECCN 1E001 (covering technology relating to ECCN 1A005), which applies to body armor that is not manufactured to military specifications or any equivalent standard. This would subject Gearco to the EAR deemed export rule and BXA jurisdiction.

77. 15 C.F.R. § 734.3.
78. 22 C.F.R. § 120.2.
79. *Id.* § 121.1.
80. *Id.*
81. *Id.* § 120.4.

In contrast, the planned hire of a Chinese-British dual national for the company's Military Products Group, to work on the development of technologies for the development of protective gear for armed forces or for protection against chemical and biological agents, would implicate the ITAR and ODTC jurisdiction, under Category X of the USML entitled "Protective Gear Equipment." In addition, if the Israeli executive being interviewed by Gearco were to become the vice president of the Military Products Division, she likely would also need to access technical data relating to the development of the technologies underlying the division's products, which would be covered by the ITAR. Thus, separate analyses are required for the GearFrance visit to the Gearco Civilian Gear Group and the two contemplated hires by Gearco's Military Products Group.

IV. EAR Licensing Analysis

A. Basic Considerations

The BXA's general policy is to approve deemed export license applications where (1) the EAR policy applicable to the technology allows approval of the application to the home country of the foreign national; (2) there is not an unacceptable risk that the items in question will be diverted to unauthorized end-uses or end-users; and (3) the applicant agrees to comply with the applicable conditions related to the licenses.[82] The BXA generally consults with other agencies—including the Departments of State, Defense, and Energy—in making licensing decisions in connection with items controlled for national security, missile technology, nuclear nonproliferation, and chemical and biological weapons proliferation reasons.[83] If an export is contrary to the policy of any one of these agencies, the BXA is likely to deny a license application. BXA regulations impose a presumption of license denial where the individual's country of nationality is one of the countries subject to OFAC sanctions.[84]

As noted above, the Commerce Control List is divided into ten categories. Each category lists covered goods, software, and technology under various export control classification numbers (ECCN). Items subject to the EAR, but not enumerated within a particular ECCN, fall within a category of residual items known as EAR 99. The various ECCNs set forth reasons for control, such as national security and antiterrorism. The EAR includes a Commerce Country Chart that is subdivided into columns reflecting the various reasons for control, with each country having various cells under each reason for control column.[85] The chart indicates the reasons for control that apply to each country. ECCN-specific reasons for control do not apply where an "X" is not included in the applicable cell on the Commerce Country Chart.[86]

The first step in the licensing analysis requires determining whether a license is required for a particular export or, alternatively, whether the export falls within the category of No License Required (NLR). Exports of technology or software classified within the various

82. Office of Chem. & Biological Controls & Treaty Compliance, Dep't of Commerce, Guidelines for Preparing Export License Applications Involving Foreign Nationals, Attach. 1—Standard License Conditions for Applications Involving Foreign Nationals.

83. 15 C.F.R. § 750.3.

84. *Id.* pt. 746.

85. *Id.* pt. 738, supp. 1, § 738.3.

86. 15 C.F.R. § 738.4(a)(2)(ii).

ECCNs are considered to be within the NLR category where the country of export—here the country of nationality of the foreign national who will have access—does not have an "X" in the applicable ECCN "reason for control" categories on the Commerce Country Chart.[87] The NLR category does not apply, however, where a general prohibition, including the prohibition applicable to nationals of embargoed or terrorist-supporting countries, precludes an export. These prohibitions are discussed more fully below.[88] Deemed exports of technology or software in the EAR 99 category also do not require licenses except where general prohibitions apply.

B. License Exceptions

Even if analysis of a particular ECCN and the Commerce Country Chart indicates that a license generally is required, licensing exceptions may negate the licensing requirement. For the most part, however, these exceptions do not apply to the countries, destinations, and individuals subject to OFAC sanctions programs.[89] Other sensitive destinations that often are not eligible for the licensing exceptions are Russia and China.

License exceptions that may apply to deemed exports include the Technology and Software Unrestricted (TSU) and the Technology and Software Restricted (TSR) exceptions. The TSU license exception applies to certain mass-market software; operations technology and software (but only the minimum necessary for the installation, operation, maintenance, and repair of lawfully exported products); sales technology; and software bug fixes, which the EAR refers to as software updates.[90]

The TSR license exception, on the other hand, may apply to a significant number of deemed exports, depending on the classification of the technology and software and the country at issue.[91] TSR permits the export of more sensitive technology and software than is covered by TSU. TSR applies where the foreign national receiving the deemed export is from a country included in the EAR's designated Country Group B and transfer of the technology to the destination is restricted for national security reasons only.[92] Certain embargoed and terrorist destinations, a number of former Soviet republics, China, and Vietnam are excluded from Country Group B and therefore are not eligible for this exception.[93] Where the TSR license exception is available, a company must obtain a written statement from the foreign national pledging not to transfer the data to countries that are not eligible for the TSR exception.[94]

The TSR written assurance may be made by letter, and companies are not required to use any particular format.[95] The assurance must provide that the individual will not reexport or release the covered technology or software source code to a national of a country for which the TSR exception is not available. It also must provide that the direct product of the technology will not be exported to those countries if the product is otherwise con-

87. *Id.* § 738.4(a)(2)(ii)(A).
88. *Id.* § 738.4(a)(2)(ii)(B).
89. *Id.* pt. 746.
90. *Id.* § 740.13.
91. *Id.* § 740.6.
92. *Id.* § 740.6(a).
93. *Id.* pt. 740, supp. 1.
94. *Id.* § 740.6(a).
95. *Id.* § 740.6(a)(3).

trolled under the national security controls as identified on the CCL.[96] These assurances, required as a condition for utilization of the TSR exception, may be included in a company's standard nondisclosure or confidentiality agreement. Deemed exports made to foreign nationals under the TSR exception are not subject to BXA reporting requirements otherwise applicable to exports made under this licensing exception.[97]

If, upon review of the ECCN, the nationality of the end-user, and Commerce Country Chart, it appears that a license exception applies, a company must then determine whether any of the EAR general prohibitions would negate the exception. In addition to the general prohibition that applies where the individual or entity receiving the export is a national of an embargoed destination, prohibitions apply where (1) the foreign national is on the EAR's denied persons or entities list, (2) the export is to a prohibited end-user or for a prohibited end-use, and (3) a company knows that an export will result in a violation of the EAR (e.g., because the putative end-user will engage in a prohibited re-export).[98] If, after considering all of the EAR general prohibitions, it is determined that no license exceptions are applicable, the next step is to obtain a license from the BXA.

C. Licensing Process and License Conditions

If a license is required for the release of technology or software to a foreign national, a company must submit a formal license application to the BXA. The license application for exports, including deemed exports, is Form BXA-748P.[99] This form requires the applicant to provide details relating to the company, the technology that the foreign national must access, and the foreign national's immigration status.[100] The application must state with specificity the actual technology and scope of exposure required. The application also should describe any measures the applicant company intends to undertake to prevent unauthorized access to controlled technology or software that will not be covered by a license. In addition, the BXA asks that the applicant submit a résumé that includes the foreign national's employment history and any special information the applicant believes the BXA should consider in reviewing the application.

The BXA has ninety days to rule on the application; however, the ninety-day clock can be stopped if any reviewing agency submits questions to the company.[101] Licenses granted by the BXA for deemed exports are typically valid for two years, but the BXA may grant a license for a longer period if necessary.[102]

If the BXA intends to deny a license application, it will notify the applicant within five days of its decision. Applicants have twenty days from the notification date to respond to the notice of intent to deny.[103] If the denial becomes final, it may be appealed to the Under Secretary of Export Administration.[104]

When the BXA approves a license it may impose various, and sometimes stringent, conditions on the foreign national's access to technology.[105] One standard license condition

96. *Id.* §§ 740.6(a)(1), (2).
97. *Id.* § 743.1(b).
98. *Id.* § 736.2.
99. Guidelines for Preparing Export License Applications, *supra* note 82, at 7–10.
100. *See id.*
101. 15 C.F.R. §§ 750.4(a), (b).
102. *Id.* § 750.7(g)(1).
103. *Id.* § 750.6.
104. *Id.* pt. 756.
105. *See* Guidelines for Preparing Export License Applications, *supra* note 82, at 7–10.

provides that the company applying for the license must inform the foreign national in writing of all license conditions and the foreign national's responsibility not to disclose, transfer, or re-export any controlled technology without prior U.S. government approval. Another standard condition requires the applicant to establish satisfactory procedures to ensure compliance with license conditions and provide a copy of these procedures to the BXA. These procedures often include the establishment of firewalls or other safeguards to prevent the foreign national from exceeding the scope of access provided for in the license. The BXA also reserves the right to monitor the company to ensure compliance.

D. The Gearco Analysis

Under the Gearco case study, GearFrance employees, including French nationals, Canadian nationals, and one dual national of China and the United Kingdom, are scheduled to visit Gearco offices to discuss EAR-controlled technology under ECCN 1E001 relating to the design and development of protective gear classified under ECCN 1A005. Under ECCN 1E001, the reasons for control are national security (NS1) and antiterrorism (AT). A review of the Commerce Country Chart demonstrates that the reasons for control for exports to France exclude AT, but include NS1—that is, the appropriate cell in the chart includes an "X." Therefore, access by the French nationals to the controlled technology appears to require a license. However, a review of ECCN 1E001 reveals that license exception TSR applies to the category. As Country Group B, which includes France, is eligible for license exception TSR, deemed exports to the French national visitors will not require a license provided that the French nationals sign appropriate written assurances against further transfer to ineligible countries.

With respect to the GearFrance employees from Canada, the Commerce Country Chart entry for Canada includes neither NS nor AT as applicable reasons for control. Thus, the export would be considered NLR and the licensing requirement would not apply for the Canadian visitors. Assuming that no other general prohibitions apply, Gearco may host the Canadian national visitors without obtaining licenses from BXA.

With respect to the dual national from Pakistan and the United Kingdom, as described above in Section III.C, it is BXA's policy to consider this individual to be a citizen of the United Kingdom, so long as the person's most recent country of citizenship is the United Kingdom. Assuming that is the case, the dual national would be treated in a similar manner to the two French nationals. This is because, under the Commerce Country Chart, the United Kingdom is subject to the same reasons for control as France (NS1). As with France, the TSR exception applies because the United Kingdom is listed in Country Group B and the only reason for control is NS1. Thus, assuming no other general licensing exceptions will apply, deemed exports to the dual national from Pakistan and the United Kingdom will not require a license. However, Gearco would have to obtain appropriate written assurances against further transfer to ineligible countries before permitting access to EAR-controlled technology.

Interestingly, if the BXA were to treat the individual as being from Pakistan (because that was the more recent country where he obtained citizenship), the TSR license exception still would apply. This is because the only control on transfer of ECCN 1E001 technology to Pakistan is NS1 and because Pakistan is included in Country Group B. Moreover, none of the exclusions to application of the TSR exception would apply with respect to Pakistan.

As noted above, the individuals identified for hire by the Military Products Group would require access to ITAR-covered technologies. Thus, the required analysis for those individuals will be independent of the instant analysis performed under the EAR.

V. ITAR Licensing Analysis

A. Basic Considerations

The export licensing analysis relating to foreign nationals in the United States under the ITAR differs somewhat from that required under the EAR, but it is based on the same basic policy concerns. As discussed above, a foreign national is permitted to access ITAR-controlled technical data or software in a number of ways. One way a transfer may occur is under an agreement for collaboration between a U.S. company and a foreign company or government, such as a manufacturing license agreement (MLA) or a technical assistance agreement (TAA). MLAs and TAAs are contracts under which a foreign entity may receive USML defense services and technical data from a U.S. entity.[106] In addition, as discussed below, effective September 2000, ODTC established another method by which transfers pursuant to collaborative programs may be effected—pursuant to "special comprehensive export authorizations."[107] However, these authorizations may only be obtained for programs between U.S. companies and companies in NATO member countries, Australia, and Japan. Another context in which an export may occur is in connection with an ordinary employment relationship between a U.S. company and a foreign national. An export may also occur during a plant visit or meeting. Under the ITAR, the type of approval required for the export of controlled technical data depends on the manner in which the transfer occurs. If the transfer is pursuant to a proposed collaborative agreement between a U.S. company and a foreign company or government (i.e., an MLA or a TAA), approval of the proposed agreement, rather than a license, is required. In most other cases, such as in connection with employment of a foreign national, a license is required.

As under the EAR, basic considerations that come into play in the ITAR licensing determination are (1) the destination of the export—that is, the country of nationality of the prospective employee, and (2) the sensitivity of the technical data or software. In many cases, an individual's nationality creates a presumption of denial of export licensing or approval.

The ODTC may deny a license or approval if denial is required by statute or if the ODTC determines that denial is in furtherance of world peace, national security, or U.S. foreign policy.[108] The ITAR lists countries for which there is a presumption of denial of export licenses—including certain proscribed countries and embargoed destinations.[109] The proscribed destinations are countries or areas that are prohibited from receiving U.S. exports for foreign policy and national security reasons. As of this writing, ITAR-proscribed destinations[110] include Afghanistan, Armenia, Azerbaijan, Belarus, Cuba, India, Iran, Iraq, Libya, North Korea, Pakistan, Syria, Tajikistan, and Vietnam. Countries subject to ITAR

106. 22 C.F.R. §§ 120.21, .22.
107. *Id.* § 126.14.
108. *Id.* § 126.7.
109. *Id.* § 126.1(a).
110. *Id.* § 126.1(a).

restrictions as a result of U.S. embargoes include Myanmar, China, the Federal Republic of Yugoslavia (Serbia and Montenegro), Haiti, Liberia, Rwanda, Somalia, Sudan, and Zaire. These lists are continually revised based on foreign policy considerations. Therefore, before filing an export application, it is advisable to obtain current information from the ODTC.

B. License Exemptions

There are a number of fairly narrow exemptions from the ITAR licensing requirements that must be considered in the export analysis before proceeding with the licensing or approval process. These exemptions, however, do not apply to exports to certain countries, including all proscribed and embargoed destinations.[111] As the exemptions are quite narrow and are subject to numerous qualifications, it is necessary to analyze each export to a foreign national on a case-by-case basis.

1. *Country-Specific Exemptions*

An established country-specific exemption under the ITAR is the Canadian exemption, which applies to certain unclassified technical data for end-use in Canadian citizens.[112] For technical data within its scope, this exemption effectively expands U.S. borders to encompass Canada and gives Canadians the same status as U.S. citizens. This established exemption had been narrowed in April 1999.[113] After protracted discussions between the United States and Canada relating to its scope, the exemption was reissued in February 2001. While the exemption still does not cover classified technical data and defense services, it has been expanded to include certain defense articles (e.g., commercial satellites) and defense services under limited circumstances that had not been covered by the previous version of the exemption.[114]

In addition, certain of the seventeen licensing reforms announced in May 2000 that apply to nationals of NATO countries, Australia, and Japan, would provide general exemptions from ITAR licensing requirements. One exemption, effective September 2000, permits the transfer of unclassified technical data that is in support of a DOD bid proposal without obtaining an ODTC license.[115] Importantly, such transfers must be pursuant to an official written request from an authorized DOD official, and the data are limited to (1) build-to-print data, (2) build/design specifications, and (3) basic research.[116] Another, more sweeping license exception that was included as part of the platform of seventeen reforms includes an extension to qualified countries of the broad license-free export treatment regarding unclassified exports that to date has only been provided to Canada.[117] This exemption would be offered on a country-specific basis and is intended to be made available only to countries

111. *Id.* § 123.16.

112. 22 C.F.R. § 126.5(b).

113. Amendments to the International Traffic in Arms Regulations, 64 Fed. Reg. 17,531 (Apr. 12, 1999) (to be codified at 22 C.F.R. pts. 121, 123–4, 126).

114. Colin Clark & David Pugliese, *Effort to Renew U.S. –Canada Export Status Drags*, Defense News, Mar. 20, 2000, at 3; *U.S., Canada Agree to Harmonize Controls on Defense, Aerospace Technology*, 72 Fed. Cont. Rep. (BNA) 457 (Oct. 18, 1999).

115. 22 C.F.R. § 125.4(c).

116. *Id.*

117. Martha A. Matthews, *Albright Announces 17 Reforms to Enhance U.S. Defense Industry Cooperation with Allies*, 73 Fed. Cont. Rep. (BNA) 606–07 (May 30, 2000); Defense Trade Security Initiative.

that share with the United States "congruent and reciprocal" policies in export controls, industrial security, intelligence, law enforcement, and that provide reciprocity in market access. As of this writing, ODTC has not yet extended this exemption to any of the eligible countries.

2. *Technical Data Relating to Classified Information*

Several ITAR exemptions relate to the export of technical data including classified information. Exemptions applicable to classified information, which are qualified in many ways, relate to (1) plant visits in cases where the ODTC has authorized the visit and the U.S. firm has complied with DOD industrial security regulations (discussed below); (2) disclosures in response to a DOD request or directive; (3) exports in furtherance of a federal contract; and (4) exports of data in the form of operations, maintenance, and training information relating to a defense article previously authorized for export to the same recipient.[118] One important exemption permits companies, subject to certain conditions, to export pursuant to the U.S. Foreign Military Sales Program without obtaining an ODTC license or approval.[119]

3. *Exemptions Relating to Unclassified Technical Data*

Also exempted from ITAR licensing requirements is unclassified technical data related to classified information previously authorized for export to the same recipient, provided that the data does not reveal details of design, development, production, or manufacture of any defense article.[120] In addition, disclosure of technical data within the United States by U.S. educational institutions to bona fide full-time foreign employees is exempt from ITAR licensing requirements. However, this exemption applies only if the employee maintains a permanent abode in the United States throughout the employment period, the employee is not a national from a proscribed or embargoed destination, and the employer informs the foreign employee in writing that the data may not be transferred to other foreign persons without prior written approval.[121]

Another licensing exemption applies when the DOD has approved for public release without a license technical data generated under a federal contract or agreement.[122] Either the cognizant agency or the DOD Directorate for Freedom of Information and Security Review will review controlled technical data and make a determination whether the material can be released.[123] If the material is approved, the ODTC considers it to be in the public domain and exempt from licensing requirements.[124] If an exemption applies, a company must submit a certification that the proposed export is exempted from the licensing and approval requirements.[125] The certification must be retained on file for five years.[126]

118. 22 C.F.R. § 125.4.

119. *Id.* § 126.6(c); *see generally* David J. Kulkelman et al., *Foreign Military Sales*, Briefing Papers No. 99–5 (1999).

120. 22 C.F.R. § 125.4(b)(8).

121. *Id.* § 125.4(b)(10).

122. *Id.* § 125.4(b)(13).

123. *See id.*; NISPOM § 10–200 (DOD 5220.22-M).

124. 22 C.F.R. § 125.4(b)(13).

125. *Id.* § 125.6.

126. *Id.*

C. Defense Services Agreements and Special Comprehensive Authorizations

A defense services agreement—a TAA or an MLA—are required when technical data are provided in connection with defense services. Such an agreement is required (instead of a license, as described below) for employment or a long-term visit arranged between a U.S. company and a foreign company or government.[127] Before executing a TAA or MLA, ODTC approval must be obtained. Also, the company must furnish a list of all foreign nationals who would need to be covered by the agreement. A standard form cover letter and required clauses are included in ODTC's Suggested Format documents.[128] If the MLA or TAA relates to significant military equipment or classified technical data, the applicant must submit a Non-transfer and Use Certificate (Standard Form DSP-83) signed by the foreign party to the agreement, assuring that the party will not re-export or otherwise share the data with any person who is not authorized to access it.[129] If classified technical data are to be furnished, the exporting company also must comply with DOD industrial security regulations (discussed below).[130] Typically, once the ODTC has approved the agreement, no further ODTC licensing is required as long as all exports to foreign nationals come within the scope of the agreement.[131] The exporting company must file one copy of the agreement with the ODTC within thirty days from the date on which the agreement becomes effective.[132] Moreover, the parties must notify the ODTC if they decide not to execute an approved agreement.[133]

In addition, proposals or presentations related to a potential MLA or TAA for the manufacture abroad of significant military equipment also require prior approval where the agreement would involve "the furnishing abroad of any defense service including technical data" that is ultimately intended for use by the armed forces of any foreign country.[134] Approval may take the form of a written approval from the ODTC or a license for the export of technical data.[135]

Special comprehensive authorizations, an alternative to the TAA and MLA under certain circumstances for NATO countries, Japan, and Australia, include the following four types of authorizations: (1) Major Program Authorizations; (2) Major Project Authorizations; (3) Global Project Authorizations; and (4) Technical Data Exports for Acquisitions, Teaming Arrangements, Mergers, Joint Ventures, and Similar Arrangements "Teaming Authorizations."[136] Importantly, ODTC has provided that these authorizations may cover a period of up to ten years.[137]

---

127. *See* ODTC, Licensing Employment or Long-Term Visit of Foreign Person by a U.S. Company (Nov. 1996).

128. *See* ODTC, Guidelines for Preparing Technical Assistance Agreements, Manufacturing License Agreements, and Distribution Agreements 7 (Mar. 1998); 22 C.F.R. §§ 124.7, .8, .9.

129. 22 C.F.R. § 124.10.

130. *Id.* § 124.3(b).

131. *Id.* §§ 124.1(a), .3.

132. *Id.* § 124.4.

133. *Id.* § 124.5.

134. *Id.* § 126.8(a)(3).

135. *Id.* § 126.8(c).

136. *Id.* § 126.14(a). As of the date of this writing, the ODTC has informed the author that it has not yet received any applications from companies for special comprehensive authorizations.

137. *Id.* § 126.14(b)(3).

Under Major Program Authorizations, U.S. prime contractors are able to seek at the beginning of a project a single, comprehensive license (for technical data, defense services, and hardware) to cover a wide range of ventures, including projects for the commercial development of defense articles. Major Project Authorizations permit U.S. contractors to define the parameters of a single comprehensive license to cover some or all of the exports associated with a major commercial sale of defense articles to NATO member countries, Japan, and Australia. Under a Global Project Authorization, a U.S. company may obtain a single, comprehensive license to cover all exports planned under a government-to-government agreement for a cooperative project. Finally, under a Teaming Authorization, a qualified U.S. defense company may obtain a single, comprehensive authorization to exchange a broad set of technical data necessary to permit teaming and collaborative work between the U.S. firm and a qualified foreign firm from NATO member countries, Japan, or Australia. The regulation provides little guidance on how to apply for and administer these authorizations. It simply requires that a company submit a letter describing the transaction that includes a number of standard clauses that are similar to those required in MLAs and TAAs. However, the regulation does not specify that a company is required to have foreign parties sign off on the letter, as is required in order to obtain MLAs and TAAs.

D. Licensing Process

If a company seeks to provide a foreign national access to ITAR-controlled technical data other than in connection with an assistance agreement and no exemption applies, the company generally must obtain a license from the ODTC.[138] In making its licensing determinations, the ODTC often seeks recommendations from other agencies. Because national security concerns come into play in the export licensing analysis, the DOD plays a significant role in the licensing process. In fact, both the ODTC and DOD typically request information in connection with export license applications.

ODTC license application requirements are somewhat more stringent than those of the BXA. Different license applications are required for classified and unclassified data. If the foreign national requires access to unclassified data, the application will consist of a Standard Form DSP-5 along with several attachments. This application requires biographical information on the foreign national, a detailed description of the technical data to be disclosed, and an explanation of the purpose of the disclosure (e.g., to employ the foreign individual as an electrical engineer at a particular facility to work on satellite launch parameters). In addition, the ODTC requires applicant companies to represent that they seek to retain the foreign national "[d]ue to acute shortages of technical personnel in the area of our needed expertise."[139]

Supporting documentation, required to be submitted along with the DSP-5, includes (1) a cover letter providing background information and explaining the requirement for the

138. One exception, where a license is not necessary for every transfer to a foreign national, is where it is necessary to transfer technical data relating to certain satellite parts, components, and accessories to a foreign national from a NATO member country or other major non-NATO U.S. ally. 22 C.F.R. § 123.27. Under this provision, exports of technical data may be made pursuant to bulk licenses that cover all related transactions.

139. *See* Licensing Employment or Long-Term Visit of Foreign Person By a U.S. Company, *supra* note 127.

foreign national; (2) materials or brochures depicting the technology to which the individual will and will not be exposed; (3) the person's résumé; and (4) a description of the position the person will fill.[140] The DOD requires additional biographical information about the foreign national and extensive information about the work that person will perform.[141]

In connection with the DSP-5 license application for unclassified technical data, both the ODTC and DOD require companies to establish Technology Control Plans (TCP).[142] Apart from requiring specifics regarding the scope of technical data that the foreign person may receive, the TCP must specify that the person will be permitted to access information only on a need-to-know basis. It requires a company to educate the foreign national about the restrictions applicable to the foreign national specifically, as well as rules, policies, and procedures relating generally to facility security and the sensitive and proprietary nature of the work. The TCP must set forth employee identification badge requirements and other requirements that maintain a firewall between the foreign national and controlled technical data and software that will not be covered by the requested license.

The TCP also must provide that, on termination of the agreement, the employer will obtain a statement from the foreign national certifying that the individual has not disclosed company proprietary documents or other data to any unauthorized person.[143] A nondisclosure statement signed by the foreign person must be included as an attachment to the TCP. The statement must indicate that the technical data "will not be disclosed further, exported or transferred in any manner to any other foreign person or any foreign country" without prior approval of the ODTC.[144]

For classified technical data, Standard Form DSP-85 is required instead of the DSP-5. A description of the type of technical data to be accessed by the foreign person must be included on this form. A company must also provide a signed Non-transfer and Use Certificate (Standard Form DSP-83), which provides additional assurance from the foreign individual that the individual will not share the data with any person who is not authorized to access the data and will not re-export the information outside the United States.[145] As for unclassified data, a company must establish and implement a TCP. When the ODTC issues a license to export classified technical data, the official license is sent directly to DOD; only an informational copy is forwarded to the applicant company.[146] Moreover, where the export involves classified data, the company must obtain approval from the DOD Defense Security Service (discussed below).

In connection with all licenses and agreement approval requests, the ITAR requires an exporter to submit a detailed certification letter.[147] The letter must certify, among other things, that neither the company (including all directors and officers), nor the foreign national who will receive the export, has been indicted for or convicted of violating designated criminal statutes. The letter also must certify that neither party is ineligible to contract

140. *Id.*

141. NISPOM § 10–509; *see* Soc'y Int'l Affairs NewsNotes, Sept. 1998.

142. Licensing Employment or Long-Term Visit of Foreign Person By a U.S. Company, *supra* note 127, TCP attach.; NISPOM § 10–509.

143. Licensing Employment or Long-Term Visit of Foreign Person By a U.S. Company, *supra* note 127, TCP attach.

144. *Id.* TCP attach. Exh. A, Sample "Non-Disclosure Statement."

145. 22 C.F.R. §§ 123.10, 125.7(b).

146. *Id.* § 125.9.

147. *Id.* § 126.13.

with or receive a license or approval to import or export defense articles or services from any U.S. government agency.[148]

Unlike the BXA, which sets a ninety-day target period for acting on license applications, the ODTC places no time limit on the application review and approval process. If approved, an ITAR license generally applies for a four-year period.[149] If a license is denied, a written request for reconsideration may be filed within thirty days after being informed of the adverse determination. Upon reconsideration, a company will be given an opportunity to present additional information to the ODTC.[150]

E. Gearco Analysis

Under the Gearco case study, it would not be appropriate to apply for a TLA, MLA, or any of the NATO-specific authorizations because the exports at issue would not be pursuant to any particular program between a non-U.S. entity and Gearco. Rather, the exports involve individuals that would be brought in as employees of the company. Thus, Gearco will be required to apply for individual licenses by utilizing the DSP-5 license application.

As discussed in section III.E, the visitors from GearFrance will require access to technologies covered by the EAR, and not the ITAR. Thus, it is unnecessary to consider the application of the ITAR to the exchanges with those individuals. However, the hiring of the engineer who is a dual national of China and the United Kingdom and the potential hire of the Israeli executive would, in fact, implicate the ITAR. Gearco's Military Products Group likely will have great difficulty obtaining a license for the engineer who is a citizen of both China and the United Kingdom to access the ITAR-covered protective gear under Category X, given that China is one of the ITAR proscribed destinations. As described above, it is the ODTC's policy to treat dual-nationals as nationals of both countries; therefore, the country of nationality with the more rigorous restrictions governs the licensing analysis. Thus, the ODTC would treat the engineer as a citizen of China. The ODTC's policy currently is to deny all licenses for exports to China. However, it is possible that the U.S. policy toward China may be changed, in part, in the near future, as demonstrated in a recent statement by the ODTC providing that it would resume exports of commercial space equipment to China in light of the fact that China has recently announced that it will cease cooperation with other countries in developing missiles that can be used to deliver nuclear weapons.[151] However, even if this were not the case, Gearco might attempt to obtain a license under a general ITAR exception that provides that a license may be obtained in a "case of exceptional or undue hardship, or when it is otherwise in the interest of the United States Government."[152] If Gearco could make the required showing, it might be able to obtain a license for the individual to work on the development of ITAR-covered technology under this provision.

Filing a license application also would be necessary with respect to the Israeli national who is being considered for the vice president position at Gearco's Military Products Group

148. *Id.*

149. *Id.* § 123.21.

150. *Id.* § 126.7(c).

151. *See U.S. Resumes Licensing Exports of Space-Related Equipment to China*, 74 Fed. Cont. Rep. (BNA) 510 (2000).

152. 22 C.F.R. § 126.3.

to the extent that she will need to have access to controlled technologies under the ITAR. As Israel is not one of the embargoed or proscribed countries under the ITAR, Gearco should be able to obtain a license for access to controlled technical data relating to the design and development of ITAR-covered protective gear. Assuming the Israeli national is offered and accepts the vice president position, Gearco would need to take steps to file a DSP-5 license application with the ODTC. In addition, if the vice president could not perform her job duties without being able to access technical data, it would be beneficial for Gearco to make the individual's employment contingent on obtaining such a license.

VI. Penalties for Violating the Deemed Export Rule

The severity of the penalties that may be assessed—which include substantial fines, the denial of export privileges, imprisonment of employees responsible for criminal violations, or a combination of these—underscores the importance of compliance with the deemed export rule. Violations include exporting without a required license, failure to comply with license conditions, and misstatement of facts during the licensing process.

Under the current versions of the EAA and the EAR, any person who knowingly violates or conspires to or attempts to violate any export regulation, order, or license may be fined up to $50,000 or five times the value of the exports involved, whichever is greater, or may be imprisoned for not more than five years, or both.[153] In addition, certain willful criminal violations may result in corporate fines of not more than five times the value of the export involved or $1 million, whichever is greater.[154] Individuals may be fined up to $250,000 and may be imprisoned for up to ten years.[155] Civil violations may result in penalties generally not to exceed $12,000 for each violation of the EAA, the EAR, or any license issued thereunder.[156] Among the potential administrative penalties are revocation of outstanding licenses and company-wide denial of export privileges.[157]

Willful violations of the ITAR may result in criminal fines for corporations or individuals of up to $1 million per violation or, in some cases, twice the gross gain resulting from the violation or imprisonment of individuals for up to ten years, or both.[158] Violations can result in civil penalties for corporations or individuals of $500,000 or more per violation.[159] Violations also may result in suspension and debarment from export of defense articles or defense services.[160] A debarment typically lasts three years.[161]

Violations of export regulations can lead to administrative penalties that directly affect a company's ability to obtain federal contracts. For example, violations of the ITAR—particularly those relating to the handling of classified information obtained pursuant to government contracts—may result in suspension and debarment from government contracting.[162]

153. 50 U.S.C. app. § 2410(a) (1979).
154. *Id.* § 2410(b).
155. *Id.*
156. *Id.* § 2410(c); 15 C.F.R. § 6.4(a)(2); 65 Fed. Reg. 65260-01 (Nov. 1, 2000).
157. 15 C.F.R. pts. 764, 766.
158. 22 C.F.R. § 127.3; 22 U.S.C. § 2778(c); 18 U.S.C. § 3571 (1994).
159. *See* 22 C.F.R. § 127.10; 22 U.S.C. § 2410(c); 18 U.S.C. § 2461.
160. *See* 22 C.F.R. § 127.7.
161. *See id.*
162. *See* 48 C.F.R. § 9.104–1 [EAR] (2000).

Both the EAR and the ITAR have procedures for voluntary disclosure of infractions. Such disclosure is considered a mitigating factor in administrative proceedings.[163] A compliance program may be viewed as a good faith attempt to ensure future compliance and result in decreased penalties.[164]

Moreover, civil and criminal penalties may be assessed for violations of OFAC export restrictions under the various sanctions programs that the OFAC administers. For example, for willful violations of the U.S. sanctions against Iran, companies may be subject to criminal penalties of up to $500,000 per violation, and individuals may be fined up to $250,000 and sentenced to up to ten years in prison per violation. Civil penalties include fines of up to $11,000 per violation.[165]

Finally, a foreign national who has improperly obtained access to controlled technical data also may be subject to severe penalties under immigration law—including deportation and exclusion.[166]

VII. DOD Industrial Security Regulations

Unlike the export control laws, which apply to all private companies whether they are government contractors or not, the DOD industrial security regulations apply only to private companies that have access to classified materials, and this access is generally obtained in connection with federal contracts. Thus, in addition to the export control and immigration requirements discussed above, if a company performs contracts involving classified data, it also must take into account DOD regulations that place another layer of restrictions on contractors' ability to hire and interact with foreign nationals.

A. DOD Policy

It is DOD's general policy to protect all U.S. classified information in the possession of U.S. industries, educational institutions, and organizations used by federal prime contractors and subcontractors. To implement this policy, DOD's Defense Security Service (DSS) has issued certain publications, including the National Industrial Security Program Operating Manual (NISPOM) and the DOD Personnel Security Program Regulation,[167] which specify procedures for the protection of domestic information from improper access by unauthorized personnel. Classified information includes national security information (including confidential, secret, and top secret information) and restricted data regarding design, manufacture, or use of atomic weapons. It also includes information classified by a foreign government that has entered into a General Security Agreement with the United States.[168]

The NISPOM, which is incorporated by reference in federal contracts that require access to classified information, establishes a series of detailed requirements to ensure the protection of classified information. These requirements govern a contractor's behavior in the

163. *See* 15 C.F.R. § 764.5 (EAR); 22 C.F.R. § 127.12 (ITAR).
164. *See* 15 C.F.R. § 764.5(e)(7); 22 C.F.R. § 127.12(b)(3)(iv).
165. *See* 31 C.F.R. § 560.701; 50 U.S.C. § 1705; 18 U.S.C. § 3571.
166. *See* 8 U.S.C. §§ 1182(a)(3)(A) (exclusion), 1227(a)(4)(A) (deportation).
167. *See* 32 C.F.R. pt. 154 (DOD 5200.2-R).
168. *See* NISPOM, § 10-300.

pre-contract, performance, and post-contract stages of any agreement. Access to classified information may be required under contracts with the DOD, the National Aeronautics and Space Administration, the Department of Energy, and the Department of State, as well as a number of other agencies.[169]

If a contract will require the use of classified information on-site, the contractor must obtain a Facility Security Clearance (FCL), which is an administrative determination that the contractor's facility is eligible for access to classified information.[170] A facility covered by an FCL must operate in a manner consistent with strict safeguarding requirements, under which the contractor must implement various procedures to ensure that individuals who do not have the proper security clearances are not permitted access to classified materials.[171] Moreover, they are monitored closely to ensure FCL compliance.

For individuals requiring access to classified information, the standard procedure involves applying for and obtaining a Personnel Security Clearance (PCL). Contractors that seek to employ foreign nationals in connection with classified contracts face serious constraints, however, because the NISPOM provides that only U.S. citizens are eligible for PCLs.[172] The NISPOM further states that "[e]very effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information."[173]

Notwithstanding this provision, the DSS may issue access authorizations to foreign national employees for certain categories of classified information under limited circumstances. Non-employee foreign nationals visiting contractor facilities (e.g., for symposia or training programs) also may obtain access to classified materials.[174]

Under the U.S. National Disclosure Policy, authorization for disclosure of classified military information to a foreign person may be granted only if: (1) the disclosure supports foreign policy; (2) the release will not negatively affect U.S. military security; (3) the foreign recipient has the capability and intent to protect the classified information; (4) the benefit of the disclosure outweighs any potential risks; and (5) the scope of the disclosure is limited to the information necessary to accomplish U.S. objectives.[175]

Requests for authorization for foreign nationals' access to classified information are treated on a case-by-case basis and must go through the cognizant security agency (CSA)—that is, the agency administering the classified program at issue (often this is the DSS). In addition to receiving CSA authorization, a company must obtain export authorization from the ODTC (discussed above).[176]

B. Limited Access Authorizations

Although a contractor's foreign national employees are not able to obtain PCLs, those employees can access limited classified information as required in connection with their

169. *See id.* §§ 1-100 – 1-104.
170. *See id.* § 2-100.
171. *See id.* ch. 5.
172. *See id.* § 2-210.
173. *Id.*; 32 C.F.R. § 154.16(c) (2000).
174. *See* NISPOM, § 10-201.
175. *Id.* § 2-210.
176. *See id.* §§ 5-508 (general prohibition on disclosure of export-controlled information and technology to foreign nationals unless contractor complies with export laws); 10-308 (exports of foreign government classified information); 10-409 (requirement to substantiate applicable exception to ITAR if applicable); 10-603 (export authorization required for use of classified information abroad).

jobs if they obtain Limited Access Authorizations (LAA). The DOD will grant LAAs "in rare circumstances" at its discretion where (1) the foreign national possesses unique or unusual expertise that is urgently needed to support a specific government contract and (2) a cleared or clearable U.S. citizen is not readily available.[177] An LAA will only permit access to information on a need-to-know basis and will only be granted to foreign nationals working in the United States.[178] Because the LAA application process can be lengthy, it is advisable to initiate the application process as soon as a foreign national's need for access to classified information becomes apparent. The LAA application can be processed concurrently with any required export license or approval.

An individual with an LAA may be permitted to access information up to the level of Secret, but may not access information designated as Top Secret.[179] Persons with LAAs also are not permitted access to a number of specific categories of information, including (1) restricted data regarding nuclear weapons design or production, (2) information that is not releasable to the country of which the individual is a citizen, (3) intelligence information, (4) information for which foreign disclosure has been prohibited in whole or in part, and (5) NATO information (although foreign nationals of NATO countries may access this information with the proper certification in connection with a specific NATO contract).[180] The level, nature, and type of information an individual may access are specified in each LAA.

As required under the U.S. National Disclosure Policy, considerations affecting issuance of an LAA include the foreign national's allegiance to the United States, susceptibility to foreign influence, and moral character.[181] The individual's country of citizenship also bears upon the determination. Yet there is no requirement that the foreign national have obtained any particular immigration status to be eligible for an LAA.[182] For purposes of the LAA analysis, unlike the BXA and ODTC export control regulations, permanent residents and certain other foreign nationals (the protected classes of foreign nationals who are excluded from the deemed export rule, as provided above) are not distinguished from nonimmigrant foreign nationals.

The LAA application process first requires the concurrence of the contracting agency that an individual possesses a unique skill or expertise urgently needed for performance of a contract. If it is likely that the agency will endorse the LAA application, a company must provide information[183] to the contracting officer that resembles the type of disclosure required by the ODTC before the licensing of a foreign person to access technical data subject to the ITAR. Such information includes (1) the individual's date and place of birth, job title, and current citizenship; (2) a statement that access will be limited to a specific government contract (identified by contract number); (3) a description of the unusual or unique skill or expertise possessed by the individual; (4) an explanation of why a qualified U.S. citizen cannot be hired in sufficient time to meet the contract's requirements; (5) a list of

177. *See id.* § 2–210.
178. *See id.* §§ 2–210, 10–601(b).
179. *See* 32 C.F.R. § 154.16(c)(1)(i).
180. *See* NISPOM, § 2–211.
181. *See id.* § 10–103 (describing National Disclosure Policy).
182. *See* 32 C.F.R. § 154.16(c).
183. *See id.* § 154.16(d).

the specific material to which access is proposed and the classification level of such material; and (6) the immigration status of the individual.[184]

Once a company has obtained the agency's concurrence, the next step is to submit the individual's application (Standard Form 86, entitled "Questionnaire for National Security Positions") to the Defense Industrial Security Clearance Office (DISCO), the DOD's central security clearance processing center, along with the contracting agency's written concurrence stating the reasons for the LAA. DSS conducts a background check to assess the applicant's allegiance to the United States, susceptibility to foreign influence, and moral character. DISCO then makes a determination either to issue an LAA or to forward the file to the DOD Office of Hearings and Appeals (DOHA) for an initial adjudication.[185] The DOHA reviews the file and either grants the LAA or issues a specific statement of reasons why granting the LAA would be inconsistent with the national interest. The background check is not subject to any time limit and can take considerable time because data often must be gathered overseas. If an LAA is not granted, the foreign national may respond in person before a DOHA administrative law judge. The judge's determination may be appealed to the DOHA Appeal Board.[186]

C. Foreign Ownership, Control, and Influence

Regardless of whether a prospective employee will require access to classified information and a LAA, an additional consideration when employing foreign nationals is the possibility that such action could be deemed to establish foreign ownership, control, and influence (FOCI) of the company.[187] In cases where DSS determines that a U.S. company is under FOCI, the company will either be ineligible for an FCL or any FCLs that are already in place may be suspended or revoked unless steps are taken "to remove the possibility of unauthorized access or the adverse affect on classified contracts."[188] Where FOCI may be implicated as a result of the hiring of a foreign national, the NISPOM requires that a company take steps to mitigate the foreign influence insofar as it could affect classified activities.[189]

FOCI generally will only be implicated by the hiring of a foreign national if that individual is placed in a company key management position. Typically, a position would be considered to be a key management position if it afforded the foreign national a level of control or influence that could adversely affect the performance of classified contracts or result in unauthorized access to classified information.[190] This might be the case, and FOCI might be implicated, even if the foreign national is walled off completely from all classified information.

A company that performs both classified and non-classified work and seeks to hire foreign managers to handle non-classified matters only could take steps to avert FOCI by setting up the corporate division that performs classified work as a separate subsidiary of the parent. Creation of this separate subsidiary might increase the likelihood that foreign nationals hired by the parent organization would not be considered to give rise to FOCI over per-

184. *Id.*
185. *See* 32 C.F.R. pt. 155, app. A ¶ 1.
186. *See id.* ¶ 28.
187. *See* NISPOM, § 2-300.
188. *Id.* § 2-301 (b).
189. *Id.*
190. *See id.* § 2-300.

formance of the classified work. The CSA has the discretion to exclude the parent from the FCL requirement where it does not have access to classified materials.[191] To obtain approval from the CSA that a subsidiary may receive an FCL to the exclusion of the corporate parent, typically the applicant corporation must demonstrate that the parent not only will be unable to access classified information, but also that it will not be able to exercise control over decisions relating to performance of the classified contract.[192] The firewall against the parent company must be documented through a board of directors resolution, which resembles the resolution necessary for exclusion of key management personnel from the PCL requirement, which is described below.[193]

In addition, the subsidiary generally must show that it will be able to perform the classified contract(s) as a responsible contractor, independent of its corporate parent. DSS may require the subsidiary to demonstrate its "responsibility" to perform the classified contracts as described in the Federal Acquisition Regulation (FAR). To be considered responsible, a prospective contractor must, for example: (1) have adequate financial resources to perform its contract(s), or the ability to obtain them; (2) have a satisfactory performance record; (3) have a satisfactory record of integrity and business ethics; and (4) have the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them.[194] DSS may, however, approve a subsidiary for an FCL, and permit exclusion of the parent, where the parent retains substantial control over administrative operations of the subsidiary such as (1) tax-related services; (2) payroll administration and accounting support, and (3) information systems support. As long as the subsidiary is deemed to be fully in control of its classified contracts, DSS may approve the proposed exclusionary arrangement.

As noted above, DSS requires certain contractor key management personnel to obtain PCLs. Even if a separate classified-only subsidiary were created, it is possible that some members of the parent organization would be considered key personnel necessary in the performance of classified contracts. These personnel include a "senior management official" on the classified project and a "facility security officer"[195] (the individual ultimately responsible for maintaining security at the secured facility). Other key management personnel, as determined by the CSA, must either be granted a PCL or be excluded from access to classified information.[196] DSS often requires that certain corporate officers—including the chief executive officer and/or corporate president—obtain PCLs. Thus, if a foreign national is hired into an executive position, it is possible that he will be considered one of the key management personnel and FOCI will be implicated. Moreover, even if the foreign national were hired for a lower level management position, it is nonetheless possible that DSS would regard it as a key management position.

If a foreign national were to be considered one of the key management personnel, it would be necessary not only to wall off the individual from all classified information, but also to officially exclude the person from obtaining such access.[197] DSS requires companies

191. *See id.* § 2–109.

192. *Cf.* NISPOM, § 2–300 (This section requires safeguards where foreign control or influence come into play).

193. *Cf.* NISPOM, § 2–106.

194. Federal Acquisition Regulations System, 48 C.F.R. §§ 9.104–1 (a),(c),(d),(e) (2000).

195. NISPOM § 2–104.

196. *See id.*

197. *See id.* § 2–305(b).

that are under the threat of FOCI to submit a negation plan demonstrating the steps the company will take to exclude the foreign national. As with exclusion of a parent organization described above, exclusion of key management personnel may be effected by a board of directors resolution documenting that the excluded individuals (1) "shall not have, and can be effectively excluded from access to all classified information disclosed to the organization" and (2) cannot "adversely affect the organization's policies or practices in the performance of classified contracts."[198]

In any case, when a foreign national is considered for a management position, it is advisable to inform the DSS beforehand.[199]

D. Visits and Other Interactions with Foreign Nationals

It is the DSS's general policy that visits to facilities where classified contracts are being performed—whether by U.S. citizens or foreign nationals—are to be kept to a minimum.[200] However, the DSS recognizes that such visits are inevitable in connection with government-to-government agreements, direct commercial sales to foreign governments, symposia, conferences, joint ventures and business arrangements in connection with proposals for or work on classified contracts, or foreign participation in contractor training activities.[201] Where visits necessitate that foreign nationals have access to classified information, the DSS will require either that (1) the individual has received appropriate clearance from a country that maintains a General Security Agreement with the United States permitting reciprocal access to and protection of classified materials or (2) the individual has an LAA in place that covers access to the specified classified information. As with U.S. citizens' visits, access is provided only on a need-to-know basis.[202] Moreover, foreign national visits are subject to strict DSS notice and approval requirements.

The NISPOM specifies that all visits to classified facilities that involve access to classified materials be subject to advance notice and approval by the CSA.[203] Approvals are required for one-time visits (generally limited to thirty days) and extended visits (for up to one year) alike.[204] Requests for visits by foreign nationals must be submitted through government-to-government channels if they will involve (1) disclosure of U.S. classified information,[205] (2) disclosure of unclassified information related to a U.S. classified program,[206] or (3) certain plant visits that have previously been approved by the appropriate agency.[207] Only those foreign nationals who have received the requisite security clearances from their countries of citizenship or who have received LAAs from the DSS are eligible to access classified information. Requests for visits by foreign nationals that will not involve access to classified information, on the other hand, are submitted directly to the contractor and in many cases

198. *Id.* § 2-106(a).

199. *See id.* § 1-302(h)(3) (this section requires that companies submit a CSA-designated form to inform of any change to information previously submitted relating to key management personnel).

200. *See id.* § 6-101.

201. *Id.* § 10-200 *et seq.*

202. *See id.* § 6-105.

203. *See id.* § 6-101.

204. *See id.* § 10-502.

205. *See id.* § 10-507.

206. *See id.*

207. *See id.* § 10-507.

are not subject to the notice and prior approval requirements (i.e., the contractor is only subject to applicable export control requirements).[208]

For a foreign national located abroad (whether the individual is employed by a foreign government or company), the foreign government must send a visit request letter to the applicable U.S. government agency visit office. This office is usually within the military department in charge of the classified program. The letter must indicate that the individual has obtained a security clearance from the individual's country of nationality and specify the information the individual seeks to access. If the individual's home country has entered into a General Security Agreement with the United States[209] and access is required by the foreign national, the visit typically will be authorized. Where the country does not maintain a General Security Agreement with the United States, requests for access are handled on a case-by-case basis. When a visit request is approved, the approval notification contains instructions regarding the level and scope of classified information that may be disclosed.[210] After approval, the contractor will be notified and given an opportunity to deny the visit request. U.S. government-sponsored visits are exempt from the export licensing and approval provisions of the ITAR, so no independent export authorization will be required.[211]

If the foreign national visit request is denied, the contractor still may accept the visitors, but it may only disclose information in the public domain.[212] If the agency visit office declines to render a decision because the visit is not in support of a U.S. government program, however, the visit still may take place and the foreign national may be permitted to access classified information as long as certain procedures are followed. Specifically, in addition to obtaining the proper export authorization,[213] the contractor must obtain the requisite security clearance information in the form of security assurances from the visit office.[214]

Another possible scenario in which a foreign national may request access to classified information involves a visit to a U.S. contractor facility by a foreign national with an LAA—for example, an individual from another country who works at a different U.S. company within the United States and holds an LAA. In this situation, the U.S. contractor could permit access if (1) the requisite export authorization were in place, (2) the foreign national's LAA covered the information sought for access, and (3) the foreign national had a need to know the information.[215]

For extended visits and assignments of foreign nationals to cleared facilities, prior notification to the cognizant security agency is always required, whether access to classified information is involved or not.[216] The notification must include a copy of the visit authorization letter and export authorization as well as a TCP[217] setting forth procedures to ensure that the foreign national cannot access any classified information other than that specifically provided for in the export authorization or license.[218] If the foreign national will require

208. *See id.*
209. *See id.* § 10–104.
210. *See id.* § 10–507(d).
211. *See id.* § 10–507(a); 22 C.F.R. § 125.5.
212. *See* NISPOM, § 10–507(b).
213. *See id.* § 10–507(c).
214. *See id.*
215. *See id.* § 2–210.
216. *See id.*
217. *See id.* § 10–508(c).
218. *See id.* § 10–509.

access to export-controlled information related to, or derived from, a U.S. classified contract, the contractor must obtain the written consent of the contracting agency, and that consent must be included in any request for export authorization.[219] Extended visits and assignments of foreign nationals to contractor facilities will be authorized only if it is deemed "essential" that the foreign national be at the facility under the terms of a contract or U.S. agreement.[220]

Interactions between contractors performing classified contracts and foreign nationals other than in connection with a site visit also are subject to similar prior notification and approval requirements. As noted above, for example, before a contractor makes a proposal to a foreign company that ultimately will involve disclosure of U.S. classified information, the DSS requires the contractor to obtain ODTC export authorization, the concurrence of the contracting agency, and facility clearance verification on the foreign company from DISCO.[221] In addition, when a U.S. contractor enters into an agreement that will involve the provision of classified information to foreign nationals, the DSS requires that a number of security requirements clauses be incorporated into the agreement between the United States and the foreign entity.[222]

In sum, contractors involved in classified contracts face significant restrictions when considering hiring, assigning, or even collaborating with foreign nationals. NISPOM violations pertaining to LAAs, visit approvals, FOCI procedures, or other industrial security procedures can result in an administrative inquiry by the DSS and ultimately lead to a suspension, an invalidation, or a revocation of a contractor's FCL and render a contractor ineligible to work on future classified contracts.[223]

E. The Gearco Analysis

The Gearco case involves visits by foreign nationals to collaborate with individuals in Gearco's Civilian Gear Group on the design and development of civilian protective gear as well as the potential hiring of a Chinese-British dual national and an Israeli national for the company's Military Products Group. Neither the visit to the Civilian Products Group nor the new hires would appear to require access to classified data or to involve interaction with Gearco's Federal Systems Group, which is a Gearco subsidiary that works on classified contracts. Nonetheless, because the Federal Systems Group is affiliated with the company divisions with which the individuals will be interacting, it will be necessary to examine the NISPOM requirements relating to these interactions.

With respect to the foreign nationals who will be visiting with Gearco's Civilian Gear Group, because these individuals will be working exclusively with that group and do not appear to require access to any classified information, they will not require visit approvals under the industrial security regulations. Employment of the individuals by the Military Products Group, however, may well implicate the industrial security regulations. Because these individuals are not intended to require access to classified information, they will not require LAAs. However, if DSS were to consider the positions that these foreign nationals

219. *See id.* § 10–508(b).
220. *See id.* § 10–508(a).
221. *See id.* § 10–202.
222. *See id.* § 10–204.
223. *See id.* § 10–510.

will work in to be key management positions, FOCI would be implicated. This might be the case even if the foreign nationals would not be hired by or working on classified contracts held by the Federal Systems division. As discussed above, any hire of a foreign national by a company that holds classified contracts may result in the implication of FOCI. Thus, it will be advisable for Gearco to notify DSS regarding its intention to hire these foreign nationals before it enters into either employment relationship.

Gearco's hiring of the Chinese-British dual national likely will not implicate FOCI because the individual is intended to work on the technical design and development of non-classified technologies. It does not appear that the individual will have management or oversight responsibilities that relate to the classified work being performed by Gearco's Federal Systems Group. Thus, it is unlikely that DSS would determine that the Chinese-British dual national would be in a key management position; as such, there should be no FOCI created by the potential employment relationship.

On the other hand, Gearco's hiring of the Israeli executive to be Gearco's vice president could result in the implication of FOCI if DSS were to consider the vice president position to be a key management position relative to Gearco's subsidiary's classified contracts. The fact that Gearco has set up the division that handles classified work as a separate subsidiary (Gearco's Federal Systems Group) could minimize the likelihood that the position of vice president within the parent organization would be considered a key management position vis-à-vis the classified work. However, to the extent that the Israeli national were considered to be in the category of key management personnel, the NISPOM would require Gearco to take certain steps, including a board of directors resolution that would officially exclude the individual from access to classified information. This should mitigate any foreign influence insofar as it could affect classified activities.[224] In any case, it will be necessary to consult with DSS throughout the process to ensure that DSS is satisfied that any potential FOCI has been mitigated.

VIII. Conclusion

Numerous concerns come into play when companies interact with or hire foreign nationals. The Gearco case study touches upon a number of the issues that arise under these circumstances. However, it does not cover all of the complex considerations under the immigration, export control, and industrial security laws and regulations. When confronting a situation involving the hiring of foreign nationals or a collaborative project with foreign nationals involving the transfer of technical data, it is best to consult the regulations in the various areas independently to determine which regulatory frameworks potentially may be implicated. Moreover, it is imperative for companies to develop and implement compliance programs designed to educate company human resources department and managerial personnel on the restrictions that come into play when working with foreign nationals. These programs must be comprehensive, yet flexible enough to keep up with regulatory changes.

224. *See id.* § 10-202.