IMMIGRATION BRIEFINGS®

From the Publisher of *INTERPRETER RELEASES*

Practical Analysis of Immigration and Nationality Issues

FOREIGN NATIONALS IN U.S. TECHNOLOGY PROGRAMS: COMPLYING WITH IMMIGRATION, EXPORT CONTROL, INDUSTRIAL SECURITY AND OTHER REQUIREMENTS

by

M. BETH PETERS, DAVID W. BURGETT AND JOY E. STURM

In recent years, with the globalization of the economy and the demise of communism, the interaction between U.S. corporations and foreign nationals has increased steadily. This has led to a growing number of sales of U.S. military and commercial items abroad. As a consequence, more and more U.S. companies are seeking to hire foreign persons to fill marketing and business positions to assist in selling products or services. At the same time, the rapid growth in the information technology sector has resulted in an increased need for highly skilled engineers and computer professionals on the part of high-tech companies in Silicon Valley and other regions throughout the country.[1] As these companies find that there are not enough U.S. workers to fill these positions, they are frequently turning to foreign nationals to meet their needs.[2]

Whether U.S. companies are tapping into the non-U.S. workforce or simply interacting with foreign teaming partners or potential customers, they face a complex and daunting web of immigration, export control, and national security laws and regulations. The lack of centralization and limited coordination among the various agencies that regulate in these areas makes compliance particularly challenging.

The most obvious regulatory hurdle attendant to hiring and working with foreign nationals arises in the area of immigration law. U.S. companies must comply with the immigration laws and the requirements set forth by the U.S. Immigration and Naturalization Service and certain other agencies when hiring and working with foreign nationals.

Another layer of regulatory constraints that applies when hiring or working with foreign nationals—one with which legal practitioners often are not as familiar—is the export control regulations. These regulations, administered primarily by the U.S. Departments of Commerce and State, with the participation of the Department of Defense, place restrictions on companies employing foreign nationals under the "deemed export" rule. This rule requires U.S. companies and federal agencies to treat access by a foreign national to controlled technology and software as an export to the foreign national's home country. Given the recent increase in high-profile export control

The Issue In Brief

IMMIGRATION LAW CONSIDERATIONS

"DEEMED EXPORT" RULE

EAR LICENSING ANALYSIS

ITAR LICENSING ANALYSIS

PENALTIES FOR "DEEMED EXPORT" VIOLATIONS

DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY REGULATIONS

DISCRIMINATION CONCERNS

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. *The authors gratefully acknowledge the assistance of Scott M. Deutchman, a former associate of the firm, in drafting this* BRIEFING. *This* BRIEFING *includes material originally published in Edition II,* BRIEFING PAPERS *NO. 00-3 (West Group 2000).*

enforcement actions and the increase in "deemed export" compliance investigations,[3] it is perhaps more important than ever to ensure compliance with these detailed regulations. For example, in 1998, the Boeing Company was fined $10 million for transferring restricted technical data to joint venture partners from countries including Russia and Ukraine in connection with the "Sea Launch" satellite program.[4] (Many of the violations allegedly occurred at a U.S. facility when the company permitted foreign nationals access to controlled data without first obtaining an export license.) In another recent case, a major aerospace company was indicted for making allegedly fraudulent and misleading statements in connection with licensing of exports to China—serious charges that, if proven, could result in corporate fines of up to $10 million.[5]

Yet a third set of restrictions comes into play where foreign nationals are involved in the performance of a federal contract that requires access to classified materials. In addition to the export controls described above, DOD regulations pertaining to industrial security place restrictions on the sharing of classified information with foreign nationals. These regulations apply to federal contractors as well as to Government agencies working within classified programs. In the wake of the 1999 indictment of a Los Alamos laboratory physicist for allegedly mishandling classified information[6] and a 1999 report released by a U.S. House of Representatives Select Committee that was critical of Government and private adherence to national security controls,[7] these restrictions are receiving increased attention.

This BRIEFING examines the various laws and rules of which you should be aware and the analyses that you should perform when your client plans to hire or to work collaboratively with foreign nationals on programs that may involve controlled technology or classified information. The BRIEFING reviews the various immigration law considerations involved, and discusses (1) the "deemed export" rule, (2) the analysis required to determine whether a license is required for a deemed export, (3) the penalties for violating the deemed export rule, (4) the DOD industrial security regulations, and (5) citizenship- or national origin-based discrimination concerns that may arise when deciding whether to employ foreign nationals.

IMMIGRATION LAW CONSIDERATIONS

If your client is interested in working with foreign nationals, it must find its way through the maze of immigration law-related requirements that Congress, through the administering agencies, places on employers. Immigration laws and regulations come into play both where a company intends to host a foreign national as a nonemployee (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 all play a role in regulating the employment of foreign nationals. The INS shares with the State Department the responsibility for determining the immigration status for which a foreign national may qualify. The INS also enforces the immigration laws at the U.S. borders when foreign nationals arrive in the country. 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

Immigration Briefings is published by West Group (ISSN 0897-6708). Address correspondence to: Editor, 50 Broad St. East, Rochester, NY 14694

For subscription information: call (800) 221-9428, or write West Group, Credit Order Processing, 620 Opperman Drive, PO Box 64833, St. Paul, MN 55164-9753. Immigration Briefings is publsihed 12 times per year. The subscription is $415.

Periodical Postage Paid at St. Paul, MN. POASTMASTER: Send address changes to Immigration Briefings, 620 Opperman Drive, St. Paul, MN 55164-9753.

periods. In addition, the Department of Labor ensures that companies planning to employ foreign nationals meet certain prescribed labor conditions.

◆ Immigration Status Determination

The first step when considering hiring a foreign national is to determine the individual's immigration status. If the foreign national is already in the United States, you 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 ("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 visas or work authorizations. 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, you must determine whether the person will qualify for a 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.

If your client plans to hire foreign nationals for temporary or permanent employment, it should consider the processing time required for any necessary visa or work authorizations. 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.[8]

◆ Business Visitor

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.[9] A person who performs services as an employee for a U.S. company and receives remuneration for such activities is *not* eligible for B-1 status. The foreign national applies 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.[10]

Foreign nationals from certain designated countries, including North Atlantic Treaty Organization 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 90 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 90-day period or is employed by a U.S. company during that period.[11] The Visa Waiver Pilot Program expired on April 30, 2000. However, legislation permanently extending the program has passed the House. The Senate is expected to take up the matter after it returns in September. In the meantime, the INS and the State Department have agreed to issue parole for 90 days to visa waiver country nationals. Initially the INS and State Department announced that they would continue this practice until May 30, 2000, but subsequently announced that they would continue it through September 30, 2000.

◆ Temporary Employees

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. In addition, students in F-1 or J-1 status also may be eligible to work for U.S. employers.

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 a cap on the number of new H-1B petitions that can be approved each fiscal year. For FY 2000, the INS was permitted to approve only 115,000 new H-1B petitions,[15] and reached this cap on July 20, 2000 after having stopped accepting H-1B petitions for fiscal year 2000 on March 21, 2000 when it had received sufficient petitions to reach the cap. In August, the INS began processing petitions for H-1B workers whose employment will start in fiscal year 2001, which begins October 1, 2000. Under current law the cap for fiscal year 2001 is set at 107,500.[16] It is hoped, however, that Congress will soon act on legislation now before it to increase this number.[17]

Foreign nationals in the United States in 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.[18] They may not begin working for the new employer until the H-1B petition is approved.

L-1 Visa. If your client 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 be employed by a "parent, branch, affiliate, or subsidiary of that employer in a managerial capacity or executive capacity, or in a position requiring specialized knowledge."[19] 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.[20] 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.[21] 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.[22]

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.[23] To sponsor a foreign national for H-3 status, your client must establish that (1) there is a structured training program in place (typically requiring a classroom or similar component and that the position does not consist primarily of on-the-job training) in which the foreign national will participate, (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 the job overseas.[24] Training may be approved for a period of up to two years.[25]

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.[26] Canadian nationals are permitted to apply to the INS for TN status at the border immediately before entry and do not require a visa.[27] For Mexican nationals, a TN petition must be submitted to the INS; if approved, the petition will enable the individual to apply for a TN visa at a U.S. embassy or consulate abroad.[28] TN status is valid for no more than one year but is renewable on an "as needed" basis.[29]

F-1 Visa/J-1 Visa. Students in F-1 or J-1 status may be eligible to work for U.S. employers if they receive practical training authorization.[30] For example, after graduation, F-1 students generally are eligible for a period of practical training for up to one year.[31] Such practical training does not require the U.S. employer to file a sponsoring petition with the INS. After the period of practical training has concluded, the employer would have to 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]

◆ Permanent Employees

There are a number of ways that a foreign national may apply, or be sponsored, for permanent resident status based on employment or investment in the United States. The Immigration and Nationality Act (INA) sets forth five employment-based preference categories.

The INA requires that some aliens seeking to immigrate on the basis of U.S. employment first receive a labor certification from the U.S. Department of Labor.[33] Aliens seeking to immigrate in the second or

third employment-based preference are inadmissible unless the Secretary of Labor has first issued a labor certification.[34] The second employment-based preference (EB-2) covers aliens with exceptional ability in the sciences, arts, or business and aliens with advanced degrees in professional fields.[35] Under limited circumstances, a small group of these aliens may, in the national interest, be exempted from the labor certification requirement. The third employment-based preference (EB-3) covers aliens with bachelor's degrees in their fields, skilled workers, and unskilled workers.[36]

Aliens seeking to immigrate in the first, fourth, and fifth employment preferences do not need to obtain labor certifications. The first employment-based preference (EB-1) covers "priority workers," that is, aliens with extraordinary ability in the sciences, arts, education, business, and athletics; outstanding professors and researchers; and executives and managers with multinational corporations who meet specific requirements.[37] The fourth employment-based preference (EB-4) covers aliens who are classified as "special immigrants," which includes ministers and other religious workers, aliens who have worked abroad for the U.S. government, and other narrowly-defined groups.[38] The fifth employment-based preference (EB-5) covers alien investors in new commercial enterprises.[39] Because avoiding labor certification makes a permanent residence case both simpler and faster to process, practitioners want to investigate thoroughly whether the alien fits within any of these groups.

Where labor certification is required, the Secretary of Labor must certify to the State Department and the Attorney General that (1) there are not sufficient workers who are able, willing, qualified and available at the time of application for a visa and admission to the United States and at the place where the alien is to perform such skilled or unskilled labor, and (2) the employment of such alien will not adversely affect the wages and working conditions of workers in the United States similarly employed.[40] Once a labor certification is issued, the employer must file a petition with the INS seeking approval to employ the individual in the certified position.[41] If the petition is approved, and provided that an immigrant visa is available, 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 already is in the United States legally.[42]

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. A foreign national often will work for a U.S. employer in a nonimmigrant category until the green card process is completed.

"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 a delivery of goods or data from the United States to another country is an export that potentially may be subject to export licensing or other restrictions. What is less widely known, however, is 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 can take considerable time (90 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. An example may help illustrate how the rule comes into play. Assume a U.S. company that makes satellites and related technology ("Satco") hires a Canadian company ("Canasat") to assist in the production of satellite telecommunications equipment. Satco plans to have Canasat employees visit Satco offices in Austin, Texas for two to four weeks to collaborate on the design and development of the telecommunications equipment that Canasat will manufacture using Satco's proprietary technology. These employees include both Canadian and Israeli nationals. Since the Canasat workers will be in the United States for business meetings and consultations only and will remain employees of Canasat, they will enter the United States as B-1 business visitors.

At the same time, Satco's electronics division has identified a Chinese national who has just received a Ph.D. in electrical engineering from the Massachusetts

Institute of Technology to work on the development of electronic launch technologies. The Chinese national is in the United States on an F-1 visa, and Satco has already filed an H-1B petition with the INS, which is pending. In both scenarios, Satco's plans will involve foreign nationals' access to controlled technology. If Satco does not take the appropriate steps to comply with the applicable export regulations of the Department of State and the Department of Commerce before undertaking the visit and hiring the new employee, it may be liable for civil and criminal penalties.

◆ 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) and (2) the Commerce Department's Bureau of Export Administration (BXA). The ODTC administers and enforces the International Traffic in Arms Regulations (ITAR),[43] promulgated under the Arms Export Control Act.[44] Under the ITAR, the ODTC regulates the export of defense articles and services and implements various United Nations embargoes. The BXA administers and enforces the Export Administration Regulations (EAR),[45] promulgated under the Export Administration Act (EAA), which governs the export of "dual-use" (i.e., suitable for both military and nonmilitary use) items and services.[46] Although the EAA expired in 1994, it has been extended by Executive Order since then under the authority of the International Emergency Economic Powers Act (IEEPA).[47] (Although Congress has considered legislation to implement a new EAA, a new law has yet to be enacted.) 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.[48] Both the ODTC and BXA regulate deemed exports to foreign nationals.

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.[49] OFAC's authority derives from a number of statutes, including IEEPA and the Trading With the Enemy Act.[50] 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.[51] Where concurrent jurisdiction exists, licensing is often centralized in one of the agencies. (For example, OFAC handles licensing for most countries subject to OFAC sanctions programs, but the BXA exercises jurisdiction for exports of certain items to Cuba and North Korea.)[52] Whenever an export to one of these countries is contemplated, you should consult OFAC regulations.[53] 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.[54] If an export will involve information within any such agency's jurisdiction, the cognizant agency's regulations must be consulted.

◆ 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 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.[55] Thus, under the hypothetical scenario involving Satco described above, Satco'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 deemed 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.[56] The rule also covers deemed "re-exports," which occur when technology or software has 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.[57]

Under the EAR, the deemed export rule covers the release of "technology" or software "source code"[58] (but not object code) to a foreign national.[59] ("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 can be read only by a computer system.[60]) "Technology" is defined broadly to include "information necessary for the 'development,' 'production,' or 'use' of a product" and includes "technical data" or "technical assistance."[61] "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."[62] Importantly, under the EAR, the deemed export rule applies to software only if source code is released.[63]

The ITAR's deemed export rule, similar to that of the EAR, applies to the disclosure of "technical data" to "a foreign person, whether in the United States or abroad."[64] The ITAR specifies that the term "foreign person" includes foreign individuals, foreign corporations, and foreign governments.[65] "Technical data" includes information[66] "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."[67] Unlike under the EAR, however, technical data subject to the ITAR's deemed export rule generally includes software (both source code and object code).[68] The ITAR further includes within the definition of "technical data" classified information relating to defense articles and services and information covered by an invention secrecy order.[69] 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.[70] (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.[71] 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.[72] 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."[73] 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 they have accessed. 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.[74] Whether technical data would be revealed would likely depend on the level of technical expertise of the individual having access to the item. For example, a deemed export might occur if an engineer were permitted to view a tank brake assembly (an ITAR-controlled defense item) while on a site visit. 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 a deemed export likely would not occur.[75]

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 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, North Korea, Sudan, or Yugoslavia. Other countries that also may present licensing obstacles include India, China, and the 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. You can avoid problems by taking the time to thoroughly understand the deemed export rule and by implementing internal compliance procedures to help company personnel recognize deemed exports and effectively navigate the maze of export licensing requirements.

◆ Immigration Status Considerations

A threshold inquiry in dealing with the deemed export 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.[76] Under both regulatory frameworks, the deemed export rule does not apply to the release of controlled technology or software to certain "protected individuals" under the Immigration Reform and Control Act (IRCA) of 1986.[77] 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.)[78] 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, your client may consider seeking to have the individual classified as an employment-based immigrant. As noted above, this process may take as long as two to four years, and therefore may not be a viable short-term option. While waiting for such approval, your client must ensure that the foreign national is not permitted access to any covered technology or software.

The Commerce Department recently has attempted to clarify the licensing requirements in cases where a foreign national is a citizen or permanent resident of more than one foreign country. The Commerce Department is now applying a new interpretation which states that the "last permanent resident status or citizenship obtained governs." The Commerce Department's revised interpretation is:

> If the individual is a naturalized citizen or permanent resident of the United States, the 'deemed export' rule does not apply. In other words, he or she is not subject to the provisions of the 'deemed export' regulation. 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. [79]

Therefore, if a Chinese national identified by Satco in the hypothetical described above also was a citizen of the United Kingdom, and the individual's most recent citizenship were with the United Kingdom, then releases of technology would be viewed as releases to the United Kingdom.

◆ Identification & 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 classified to determine whether the EAR or the ITAR applies. If your client engages in export transactions, it should have classified the commodities and technology it exports abroad to comply with the basic EAR and ITAR requirements. Moreover, if your client manufactures defense articles or provides defense services subject to the ITAR, it must register with the ODTC even if it does not engage in export transactions.[80] 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, your client must first determine the relevant "exposure parameters." For example, if the foreign national is an engineer, you must determine whether the person requires access to product design, development, or production data. If the foreign national is hired to work in sales or management, you must determine the level of technical understanding of relevant product lines that will be necessary.[81] In addition, you 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.[82]

Not only must you consider the physical layout and security aspects of the facility where the individual will work, you also must consider the level of access the individual will have to online information. For example, you 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 you maintain a corporate intranet that contains any controlled technical data, you also must consider whether and to what extent the person's access can be limited.

◆ Does The EAR Or ITAR Apply?

Once you have determined the exposure parameters for the foreign national's access, you must ascertain which, if any, regulatory jurisdiction governs the export of the technology or software. In other words, your client 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 determine whether the data may be subject to control by any other agency, which could include 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.[83]

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 10 "categories": nuclear materials, chemicals and toxins, materials processing, electronics, computers, telecommunications (including satellite communications technology) and 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.[84]

In contrast to the BXA's jurisdiction, the ODTC mainly regulates "defense articles," "defense services," and related technical data and software.[85] ITAR-covered articles, services, and related technical data are on the U.S. Munitions List (USML), which includes 21 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.[86] The ITAR also covers certain nonmilitary items and technologies, including commercial satellites and related technical data.[87]

Under the Satco hypothetical described earlier in this BRIEFING, the visit to Satco by Canasat employees would involve access to satellite communications technology covered by the EAR, subjecting Satco to the EAR deemed export rule and BXA jurisdiction. By contrast, the planned hire of a Chinese national for work on technical data related to launch electronics parameters would implicate the ITAR and ODTC jurisdiction. Separate analyses therefore are required for these two transactions.

If it is unclear whether particular technology or software is subject to BXA or ODTC jurisdiction, you 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.[88]

Once you have determined which regulatory regime applies, you 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.

EAR LICENSING ANALYSIS

◆ Basic Considerations

The BXA's policy is to approve deemed export license applications where (a) the EAR policy applicable to the technology allows approval of the application to the home country of the foreign national, (b) there is not an unacceptable risk that the items in question will be diverted to unauthorized end-uses or end-users, and (c) the applicant agrees to comply with the conditions related to the licenses.[89] 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.[90] 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.[91]

As noted above, the Commerce Control List, the list of controlled items under the EAR, is divided into 10 categories. Each category lists covered goods, software, and technology under various export control classification numbers (ECCNs). (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.[92] 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.[93]

The first step in the licensing analysis is 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 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.[94] 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.[95] (These prohibitions are discussed more fully below.) Deemed exports of technology or software in the EAR 99 category also do not require licenses except where general prohibitions apply.

Under the Satco hypothetical, Canasat employees, including Canadian nationals and Israeli nationals, will visit Satco offices to work on EAR-controlled telecommunications technology included in ECCN 5E001. Under this ECCN, the reasons for control are national security (NS) and antiterrorism (AT). A review of the Commerce Country Chart demonstrates that the reasons for control for exports to Canada include neither NS nor AT—i.e., the appropriate cells in the chart do not include an "X." Therefore, access by the Canadian nationals to the controlled telecommunications technology falls within the NLR category and, assuming no other general exception applies, deemed exports to the Canadian national visitors will not require a license. However, the Commerce Country Chart entry for Israel *does* include NS as one of the applicable reasons for control. Thus, the licensing requirement applies to the Israeli visitors.

◆ License Exceptions

Even if a particular ECCN 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.[96] 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."[97]

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.[98] 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.[99] 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.[100] Where the TSR license exception is available, your client 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.[101]

With respect to the Satco hypothetical, a review of ECCN 5E001 and the chart setting forth the countries in Country Group B reveals that the TSR exception applies to deemed exports to the Israeli national visitors from Canasat. This is because the only ECCN reason for control that applies to Israel is NS and because Israel is included in Country Group B. Thus, assuming that no other general prohibitions apply, Satco may host the Israeli national visitors without obtaining licenses from BXA. However, Satco must obtain appropriate written assurances against further transfer to ineligible countries from these Israeli nationals before permitting them access to EAR-controlled telecommunications technology.

The TSR written assurance is not required to be made in any particular format and may be made by letter.[102] The assurance must provide that the individual will not re-export 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 controlled under the national security controls as identified on the CCL.[103] 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.[104]

If, upon review of the ECCN, the nationality of the end-user, and the Commerce Country Chart, it appears that a license exception applies, your client 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).[105] If, after considering all EAR general prohibitions, you determine that no license exceptions apply, the next step is to obtain a license from the BXA.

◆ Licensing Process

If a license is required for the release of technology or software to a foreign national, you must submit a formal license application to the BXA. The license application for exports, including deemed exports, is Form BXA-748P.[106] 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.[107] 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 90 days to rule on the application; however, the 90-day clock can be stopped if any reviewing agency submits questions to the company.[108] 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.[109]

If the BXA intends to deny your license application, it will notify you within five days of its decision. Applicants have 20 days from the notification date to respond to the notice of intent to deny.[110] If the denial becomes final, it may be appealed to the Under Secretary of Export Administration.[111]

◆ License Conditions

When the BXA approves a license, it may impose various, and sometimes stringent, conditions on the foreign national's access to technology.[112] One standard license condition 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.

ITAR LICENSING ANALYSIS

◆ Basic Considerations

The deemed export licensing analysis 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 may gain access to ITAR-controlled technical data or software in a number of ways. One way a deemed export 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.[113] Another context in which a deemed export may occur is in connection with an ordinary employment relationship between a U.S. company and a foreign national. A deemed export may also occur during a plant visit or meeting. Under the ITAR, the type of approval required for the deemed 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 generally required.

As under the EAR, basic considerations that come into play in the ITAR licensing determination are (a) the "destination" of the deemed export—i.e., the country of nationality of the prospective employee, and (b) 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 of a deemed export 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.[114] The ITAR lists countries for which there is a presumption of denial of export licenses—including certain "proscribed destinations" and "embargoed destinations."[115] 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[116] include Afghanistan, Armenia, Azerbaijan, Belarus, Cuba, India, Iran, Iraq, Libya, North Korea, Pakistan, Syria, Tajikistan, and Vietnam. Countries subject to ITAR restrictions as a result of U.S. embargoes include Burma, 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 a deemed export application, it is advisable to obtain current information from the ODTC.

Under the Satco hypothetical set forth earlier, Satco likely will have great difficulty obtaining a license for the Chinese engineer to access the ITAR-covered satellite technology given that China is one of the ITAR-embargoed countries. However, Satco may attempt to obtain a license under a general exception providing 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."[117] If Satco can make the required showing, it may be able to obtain a license for the Chinese national to work on the development of ITAR-covered technology under this provision.

◆ License Exemptions

There are a number of fairly narrow exemptions from the ITAR licensing requirements that must be considered in the deemed export analysis before proceeding with the licensing or approval process. These exemptions, however, do not apply to deemed exports to certain countries, including all proscribed and embargoed destinations.[118] As the exemptions are quite narrow and are subject to numerous qualifications, it is necessary to analyze each deemed export on a case-by-case basis.

Several ITAR exemptions relate to the export of technical data, including classified information. The 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.[119] One important exemption permits companies to export to foreign governments pursuant to the U.S. Foreign Military Sales program without obtaining an ODTC license or approval.[120]

An established country-specific exemption under the ITAR is the "Canada exemption," which applies to certain unclassified technical data for end-use in Canada by Canadian citizens only (and not Canadian nationals with dual citizenships). It does not apply to unclassified technical data directly related to a classified defense article or certain weapons, aircraft, ocean vessels, and nuclear propulsion equipment.[121] 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. The exemption was narrowed in April 1999,[122] and the United States and Canada have been engaged in discussions to determine what the scope of the exemption will be in the future.[123]

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 do not reveal details of design, development, production, or manufacture of any defense article.[124] 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.[125]

Another licensing exemption applies where the DOD has approved certain technical data generated under a federal contract or agreement for public release without a license.[126] 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.[127] If the material is approved, the ODTC will consider the material to be in the public domain and exempt from licensing requirements.[128]

If an exemption applies, your client must submit a certification that the proposed deemed export is exempt from the licensing and approval requirements.[129] The certification must be retained on file for five years.[130]

◆ Defense Services Agreements

A defense services agreement—a TAA or an MLA—is 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.[131] 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 "Suggested Format" documents.[132] If the MLA or TAA relates to significant military equipment or classified technical data, the applicant must submit a "Nontransfer 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.[133] If classified technical data is to be furnished, the exporting company also must comply with DOD industrial security regulations (discussed below).[134]

Typically, once the ODTC has approved the agreement, no further ODTC licensing is required as long as all deemed exports come within the scope of the agreement.[135] The exporting company must file one copy of the agreement with the ODTC within 30 days from the date on which the agreement becomes effective.[136] Moreover, the parties must notify the ODTC if they decide not to execute an approved agreement.[137]

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.[138] Approval may take

the form of a written approval from the ODTC or a license for the export of technical data.[139]

In July 2000, ODTC issued an amended regulation to give U.S. companies more licensing alternatives to the MLA and TAA for NATO countries, Japan and Australia. This regulation becomes effective September 1, 2000 and companies are still considering the implications of these new alternatives. [140]

◆ Licensing Process

If your client seeks to provide a foreign national access to ITAR-controlled technical data other than in connection with an assistance agreement, and no exemption applies, you must obtain a license from the ODTC. 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 deemed export license applications.

ODTC license application requirements are somewhat more stringent than those of 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."[141]

Supporting documentation required to be submitted along with the DSP-5 includes (a) a cover letter providing background information and explaining the requirement for the foreign person, (b) materials or brochures depicting the technology to which the individual will and will not be exposed, (c) the person's résumé, and (d) a description of the position the person will fill.[142] The DOD requires additional biographical information about the foreign national and extensive information about the work that person will perform.[143]

In connection with the DSP-5 license application for unclassified technical data, both the ODTC and DOD require companies to establish Technology Control Plans (TCPs).[144] 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 your client 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.[145] 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.[146]

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. Your client must also provide a signed "Nontransfer and Use Certificate" (Standard Form DSP-83), which provides additional assurance from the foreign individual that that 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.[147] As for unclassified data, your client 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.[148] Moreover, where the deemed 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.[149] The letter must certify, among other things, that neither your client

(including all directors and officers) nor the foreign national who will receive the deemed export has been indicted for or convicted of violating designated criminal statutes. The letter also must certify that neither party is ineligible to contract with or receive a license or approval to import or export defense articles or services from any U.S. Government agency.[150]

Unlike the BXA, which sets a 90-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.[151] If a license is denied, you may file a written request for reconsideration within 30 days after being informed of the adverse determination. Upon reconsideration, your client will be given an opportunity to present additional information to the ODTC.[152]

PENALTIES FOR "DEEMED EXPORT" VIOLATIONS

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 10 years.[155] Civil violations may result in penalties generally not to exceed $10,000 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 10 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 also 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]

Both the EAR and the ITAR have procedures for voluntary disclosure of infractions. Such disclosure is considered a mitigating factor in imposing administrative penalties.[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 10 years in prison per violation. Civil penalties include fines of up to $11,000 per violation.[165]

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

DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY REGULATIONS

Unlike the export control laws, which apply to all private companies whether they are Government contractors or not, the Department of Defense (DOD) industrial security regulations apply only to private companies that have access to classified materials, usually in connection with federal contracts. Thus, in addition to the export control and immigration requirements discussed above, if your client performs contracts involving classified data, it must also take into account DOD regulations that place further

restrictions on contractors' ability to hire and interact with foreign nationals.

◆ DOD Policy

It is the general policy of DOD 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 precontract, performance, and postcontract 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 procedures to ensure that individuals who do not have the proper security clearances are not permitted access to classified materials and that they are monitored closely to ensure FCL compliance.[171]

For individuals requiring access to classified information, the standard procedure is to apply for and obtain 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 all of the following criteria are met: (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)—i.e., 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]

◆ 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 jobs if they obtain "Limited Access Authorizations" (LAAs). The DOD will grant LAAs "in rare circumstances" at its discretion where (a) the foreign national possesses unique or unusual expertise that is urgently needed to support a specific Government contract, and (b) a cleared or clearable U.S. citizen is not readily available.[177] LAAs only permit access to information on a "need-to-know" basis and are granted only 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 is 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 U.S. 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, your client 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 (a) the individual's date and place of birth, job title, and current citizenship, (b) a statement that access will be limited to a specific Government contract (identified by contract number), (c) a description of the unusual or unique skill or expertise possessed by the individual, (d) an explanation of why a qualified U.S. citizen cannot be hired in sufficient time to meet the contract's requirements, (e) a list of the specific material to which access is proposed and the classification level of such material, and (f) the immigration status of the individual.[184]

Once your client has obtained the agency's concurrence, the next step is to submit the individual's application (Standard Form 86, "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 Appeals Board.[186]

◆ Foreign Ownership, Control & Influence

Regardless of whether a prospective employee will require access to classified information and an 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] FOCI would only be found to exist if a foreign national were placed in a company "key management" position that 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.[188] Nevertheless, FOCI may be implicated even if the foreign national is "walled off" from all classified information. Where FOCI exists, the NISPOM requires reporting and steps to mitigate the foreign influence insofar as it could affect classified activities.[189] Thus, it is advisable for companies to consult with the DSS before hiring foreign nationals for key management positions.

◆ Visits & Other Interactions With Foreign Nationals

It is the DSS's general policy that visits—whether by U.S. citizens or foreign nationals—to facilities where classified contracts are being performed are to be kept to a minimum.[190] 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.[191] 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.[192] Moreover, foreign national visits are subject to strict DSS notice and approval requirements.

The NISPOM specifies that all visits to classified facilities that will require access to classified materials are subject to advance notice and approval by the CSA.[193] Approvals are required for one-time visits (generally limited to 30 days) and extended visits (for up to one year) alike.[194] Requests for visits by foreign nationals must be submitted through government-to-government channels if they will involve (a) disclosure of U.S. classified information, (b) disclosure of unclassified information related to a U.S. classified program, or (c) certain plant visits that have previously been approved by the appropriate agency.[195] 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 are not subject to the notice and prior approval requirements (i.e., the contractor is only subject to applicable export control requirements).[196]

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[197] 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.[198] 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.[199]

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.[200] 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,[201] the contractor must obtain the requisite security clearance information in the form of "security assurances" from the visit office.[202]

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—e.g., an individual from France 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 is in place, (2) the foreign national's LAA covers the information sought for access, and (3) the foreign national has a need to know the information.[203]

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.[204] The notification must include a copy of the visit authorization letter and export authorization as well as a TCP[205] 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.[206] If the foreign national will require 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.[207] 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.[208]

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 an ODTC export authorization, the concurrence of the contracting agency, and a facility clearance verification on the foreign company from DISCO.[209] 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.[210]

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.[211]

DISCRIMINATION CONCERNS

Given the numerous and often complex immigration, export control, and industrial security requirements applicable to the hiring of foreign nationals, employers—particularly those working on classified contracts—might be tempted to avoid hiring foreign nationals altogether. However, such an approach might well run afoul of statutory prohibitions against citizenship- and national origin-based discrimination. Before implementing any exclusionary practice or "screening policy," employers would be well-advised to consult the Immigration Reform and Control Act of 1986 (IRCA) and the nondiscrimination provisions in Title VII of the Civil Rights Act.

Under IRCA, a company of four or more employees may not differentiate among applicants for employment who are considered "protected individuals," which is the same class of individuals who are exempt from the licensing requirements under the EAR and ITAR (including permanent residents, refugees, and asylees).[212] IRCA prohibits employers from setting different employment verification standards or requiring different groups of employees to present additional documentation based on citizenship status.[213] The Department of Justice's Office of Special Counsel (OSC) is charged with enforcing IRCA.[214] In addition to being required to pay monetary fines (as much as $10,000 per violation), contractors that violate IRCA may be subject to debarment from Government contracting.[215]

Employers may find relief from IRCA's prohibition under an exception providing that such discrimination is permissible if it is necessary to comply with any law, regulation, or executive order or required by any federal, state, or local government contract—sometimes called the "Government contractor defense."[216] This exception permits a policy of excluding foreign nationals from consideration for positions that require access to *classified* information because the NISPOM generally requires that they be excluded from such access. Note that this exception would not support a policy of excluding foreign nationals from work on classified contracts that does *not* require access to classified information.[217] Although some burdensome regulatory requirements apply, no law requires foreign nationals to be excluded from work that does not entail access to classified information. Moreover, discrimination against "protected individuals" on the basis of the ITAR and EAR requirements would not come within this exception because all "protected individuals" under IRCA generally are exempt from licensing requirements.[218]

While IRCA addresses citizenship-based discrimination, discrimination based on a person's national origin is prohibited under Title VII of the Civil Rights Act.[219] This prohibition applies regardless of whether the prospective employee is a "protected individual" under IRCA.

To avoid inadvertent violation of these provisions, precautions must be taken when interviewing

prospective employees. Inquiring about an individual's citizenship status is not illegal per se. As a general rule, however, the OSC recommends against asking job applicants to specify their citizenship status because such an inquiry could lead a rejected applicant to conclude that your client considered the information in making the hiring decision and discriminated on that basis.

An employer may ask all prospective employees questions designed to elicit information regarding whether an individual is within one of the IRCA classes of protected individuals such that export licensing—i.e., the deemed export rule—and other immigration requirements would not apply. One question that the OSC has "approved" is the following: "Are you currently authorized to work legally for all employers in the United States on a full-time basis, or just your current employer?"[220] However, this question may not ensure compliance with the deemed export rule if the person is eligible to work but does not fall within the IRCA protected class of individuals exempt from export licensing requirements under the EAR and the ITAR. Assuming the prospective employee is not authorized to work for all employers, that individual will not come within the protected classes of IRCA, and the various visa requirements as well as the deemed export rule will come into play. This question does not appear to violate the national origin discrimination provisions of Title VII of the Civil Rights Act.

In addition, your client may, without violating IRCA, elicit additional information as to the individual's country of nationality if such information is required to determine whether the applicant is from one of the sensitive destinations under the EAR, ITAR, and OFAC regulations for which licensing is difficult or impossible to obtain or from which an individual likely would not be afforded access to classified information under the NISPOM. However, your client must use care to ensure that all questions are appropriately drafted to seek the relevant and required information without violating the IRCA or the Title VII discrimination provisions.

GUIDELINES

These *Guidelines* are designed to assist in understanding the immigration law, export control, industrial security, and other requirements that apply when U.S. companies hire or work with foreign nationals. They are not, however, a substitute for professional representation in any specific situation.

1. When planning to employ or host a foreign national as a visitor, determine the individual's current immigration status and then take action, if necessary, to obtain the status required for the individual to work at or visit your client for the desired length of time.
2. If the foreign national will be employed by your client, determine whether the individual is a legal permanent resident, refugee, or asylee. Foreign nationals with any of these statuses may work in the United States on an indefinite basis. Subject to limited exceptions, the export licensing requirements necessitated by release of technology and software data to foreign nationals generally do not apply to foreign nationals in these categories.
3. If the foreign national is not a legal permanent resident, refugee, or asylee, determine whether the individual qualifies for a nonimmigrant visa that will permit the individual to work in the United States. Nonemployee business visitors may come to the United States on B-1 visas; individuals who will be employed in the United States on a temporary basis frequently are sponsored under H-1B, L-1, TN, or H-3 visas. Keep in mind that all individuals in the United States in these visa categories are subject to the deemed export rule.
4. In addition to the time required to process any necessary immigration requirements (e.g., obtaining an appropriate visa), take into consideration the amount of lead time necessary to deal effectively with deemed export licensing requirements. If the foreign national will require access to classified information, factor in the amount of time that will be required to obtain all DOD and agency approvals.
5. Identify all controlled technology and software to which the foreign national may require access and classify it under the EAR or the ITAR. Be aware of the circumstances in which a release of controlled information can occur—including through telephone conversations, e-mail, computer networks, and fax

communications. Also, determine whether any other agency, such as the Department of Energy or the Nuclear Regulatory Commission, retains jurisdiction over export of the technology that will be accessed. If it does, consult the agency's export regulations in addition to the EAR or ITAR.

6. Determine whether the foreign national is from a "sensitive" country. This includes countries subject to OFAC sanctions and, if the ITAR applies, the proscribed or embargoed destinations set forth in the ITAR. If the individual is from a country subject to OFAC sanctions, consider OFAC licensing requirements in addition to any EAR or ITAR requirements. Obtaining a license for the release of covered technology, software, or technical data to any such foreign nationals may be difficult, or even impossible.

7. If it becomes clear that a license cannot be obtained for a foreign national, one possible solution would be to obtain permanent residence for the foreign individual. While waiting for the application to be processed, however, you must ensure that the foreign national will be "walled off" from all controlled technology and software.

8. If the foreign national is not from one of the sensitive destinations, determine whether any of the EAR or ITAR (to a lesser extent) license exceptions applies. Many license exceptions are contingent on obtaining assurances or certifications from foreign nationals. If so, be sure to obtain such documents and provide them to the appropriate agency, if necessary.

9. Because the processing of export licenses can take considerable time (90 days or longer), companies often must delay their employment of or interaction with foreign nationals. If delaying employment or a prescheduled visit is not possible, you must ensure that the foreign national does not access controlled technology or software until an export license is secured.

10. Once you know that a foreign national (regardless of immigration status) has either been identified for employment or will be visiting your facility and will require access to classified materials, take the steps necessary to obtain the requisite access LAA or visit authorization, as required under the NISPOM. If the foreign national will be employed in a key management position, take any necessary steps to ensure that foreign ownership, control, and influence risks are mitigated.

11. Take care when screening foreign nationals for employment to consult the nondiscrimination provisions of IRCA and Title VII of the Civil Rights Act to make certain that company policies are consistent with all restrictions on employment discrimination based on citizenship or national origin.

12. Develop and implement a compliance program designed to educate your client's human resources department and managerial personnel on the restrictions that come into play when working with foreign nationals. The program must be comprehensive and flexible enough to keep up with regulatory changes.

RESEARCH REFERENCE

IMMIGRATION LAW SERVICE, West Group, Chapters 37 (Employment-Based Immigration); 38 (Business Visitors), 41 (Students), 44 (Temporary Workers), 45 (Exchange Visitors), 47 (Intracompany Transferees)

Masters, Suzette & Ruthizer, Ted, *The H-1B Straitjacket: Why Congress Should Repeal the Cap on Foreign-Born Highly Skilled Workers*, 00-5 IMMIGRATION BRIEFINGS (West Group May 2000)

Tafapolsky, Alan & Vázquez-Azpiri, James, *Global Warming: The L Blanket Program and the Transnational Corporation*, 99-4 IMMIGRATION BRIEFINGS (West Group April 1999)

Fragomen and Bell, H-1B HANDBOOK (West Group 2000)

Fragomen and Bell, LABOR CERTIFICATION HANDBOOK (West Group 2000)

Fragomen and Bell, IMMIGRATION EMPLOYMENT COMPLIANCE HANDBOOK (West Group OUP 2000)

IRIS (Immigration Research Information Service), CD-ROM

IRIS (Immigration Research Information Service and Immigration Professional), CD-ROM

Interpreter Releases

References

1 Information Tech. Ass'n of Am., Bridging the Gap: Information Technology Skills for a New Millennium 4 (Apr. 10, 2000).

2 Ruth Ellen Wasem, Immigration and Information Technology Jobs: The Issue of Temporary Foreign Workers 1–7 (Cong. Res. Serv. Rep., May 12, 1998).

3 See "Deemed Cases in Pipeline," Export Prac., Mar. 2000, at 17; see also DOD Inspector Gen., Rep. No. D-2000-110, Export Licensing at DOD Research Facilities (Mar. 24, 2000).

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

5 See DOJ Press Release, "McDonnell Douglas, China National Aero Technology Import and Export Corporation and Others Indicted on Federal Charges for Making False and Misleading Statements in Connection With Exporting Machinery to the People's Republic of China" (Oct. 19, 1999); 41 GC ¶ 448.

6 Jennifer Weeks & John P. Holdren, "Energy Secrets: Finding the Balance," 56 Bull. Atom. Scientists, Mar. 1, 2000, at 20–21.

7 Select Comm. on U.S. Nat'l Security & Military / Commercial Concerns With the People's Republic of China, H.R. Rep. No. 105-851 (1999).

8 8 CFR § 274a.10.

9 INA § 101(a)(15)(B) [8 USCA § 1101(a)(15)(B)]; 8 CFR § 214.2(b).

10 *Id.*

For a detailed discussion of B-1 visas, *see* IMMIGRATION LAW SERVICE, Chapter 38 (West Group 2000).

11 INA §217 [8 USCA §1187]; 8 CFR § 217.2 et seq.

12 INA § 101(a)(15)(H)(i)(b) [8 USCA § 1101(a)(15)(H)(i)(b)]; 8 CFR § 214.2(h)(4)(i)(A)(1).

For detailed discussion of H-1B visas, see IMMIGRATION LAW SERVICE, Chapter 44 (West Group 2000), and Fragomen and Bell, H-1B HANDBOOK (West Group 2000).

13 *Id.*

14 8 CFR § 214.2(h)(9)(iii)((A)(1), (h)(15)(ii) (B)(1).

15 INA § 214(g)(1)(A)(iii) [8 USCA § 1184(g)(1)(A)(iii)].

16 INA § 214(g)(1)(A)(iv) [8 USCA § 1184(g)(1)(A)(iv)].

17 For a detailed discussion of the problems associated with the numerical cap on H-1B petitions, *see* Masters, Suzette & Ruthizer, Ted, The H-1B Straitjacket: Why Congress Should Repeal the Cap on Foreign-Born Highly Skilled Workers, 00-5 IMMIGRATION BRIEFINGS (May 2000).

18 8 CFR § 214.2(h)(8)(ii)(A).

19 INA § 101(a)(15)(L) [8 USCA § 1101(a)(15)(L)]; 8 CFR § 214.2(l)(1)(i).

For detailed discussion of L-1 visas, *see* Bower, Barbara, "L–1 Intracompany Transferee Visas," 98–4 IMMIGRATION BRIEFINGS (April 1998); Tafapolsky, Alan & Vázquez-Azpiri, James, "Global Warming: The L Blanket Program and the Transnational Corporation, 99-4 IMMIGRATION BRIEFINGS (April 1999); and IMMIGRATION LAW SERVICE, Chapter 47 (West Group 2000).

20 8 CFR § 214(l)(1)(ii)(G).

21 8 CFR § 214(l)(11), (l)(15)(ii).

22 *Id.*

23 INA § 101(a)(15)(H)(iii) [8 USCA § 1101(a)(15)(H)(iii)]; 8 CFR § 214.2(h)(7).

For a detailed discussion of H-3 visas, *see* IMMIGRATION LAW SERVICE, Chapter 44 (West Group 2000).

24 8 CFR § 214.2(h)(7)(ii).

25 8 CFR § 214.2(h)(9)(iii)(C)(1).

26 INA § 214(e) [8 USCA § 184(e)]; 8 CFR § 214.6.

For detailed discussion of hiring aliens under NAFTA *see* Etherington, David B. and Hawley, Donna Lea, "Hiring Professionals Under NAFTA," 97–2 IMMIGRATION BRIEFINGS (February 1997), and *see* IMMIGRATION LAW SERVICE, Chapter 38 (West Group 2000).

27 8 CFR § 214.6(e).

28 8 CFR § 214.6(d).

29 8 CFR § 214.6(d)(3)(iii), (f)(1), (h).

30 8 CFR § 214.2(f), (j).

See IMMIGRATION LAW SERVICE, Chapter 41 (West Group 2000).

31 8 CFR § 214.2(f)(10), (11).

32 8 CFR § 248.1.

33 INA § 212(a)(5)(A) [8 USCA § 1182(a)(5)(A)].

34 *Id.*

35 INA § 203(b)(2) [8 USCA § 1153(b)(2)].

36 INA § 203(b)(3) [8 USCA § 1153(b)(3)].

37 INA § 203(b)(1) [8 USCA § 1153(b)(1)].

38 INA § 203(b)(4) [8 USCA § 1153(b)(4)].

39 INA § 203(b)(5) [8 USCA § 1153(b)(5)].

40 INA § 212(a)(5)(A)(i) [8 USCA § 1182(a)(5)(A)(i)].

41 INA § 204(a)(1)(D) [8 USCA § 1154(a)(1)(D)].

42 INA §§ 245(a), 222(a) [8 USCA §§ 1255(a), 1202(a)]; 8 CFR § 245.1; 22 CFR § 42.41.

For detailed discussion of labor certification and employment-based preference petitions *see* IMMIGRATION LAW SERVICE, Chapter 37 (West Group 2000), and Fragomen and Bell, LABOR CERTIFICATION HANDBOOK (West Group 2000).

43 22 CFR Parts 120–130.

44 22 USCA § 2778.

45 15 CFR Parts 730–774.

46 50 USCA App. §§ 2401–2420.

47 50 USCA §§ 1701–1706.

48 Anne Q. Connaughton, "Exporting to Special Destinations or Entities: Terrorist-Supporting and Embargoed Countries, Sanctioned Countries or Entities" 13, reprinted in Coping With U.S. Export Controls 385 (Evan Berlack & Cecil Hunt eds., PLI 1999).

49 *See* 31 CFR Ch. 5.

50 50 USCA App. §§ 1–44.

51 15 CFR § 734.3; *see* R. Richard Newcomb, Office of Foreign Assets Control 5 (Sept. 30, 1999), reprinted in Coping With U.S. Export Controls, supra note 39, at 117.

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

53 31 CFR Ch. 5.

54 *See* 15 CFR Part 730, supp. 3.

55 15 CFR § 734.2(b)(2); 22 CFR § 120.17.

56 15 CFR § 734.2(b)(3); 22 CFR §§ 120.17, 125.2(c).

57 15 CFR § 734.2(b)(4), (5); 22 CFR §125.1.

58 But see *Junger v. Daley*, 2000 WL 343566 (6th Cir. 1999) (finding source code to be "speech" protected under the First Amendment in suit challenging constitutionality of export control regulations); *Bernstein v. Department of Justice*, 176 F.3d 1132 (9th Cir. 1999), reh'g granted and op. withdrawn, 192 F.3d 1308 (9th Cir. 1999).
59 15 CFR § 734.2(b)(2)(ii).
60 *See* < http://foldoc.doc.ic.ac.uk/foldoc> (for detailed definitions of "source code" and "object code"); 15 CFR Part 772.
61 15 CFR Part 772.
62 *Id.*
63 15 CFR § 734.2(b)(2)(ii).
64 22 CFR §§ 120.17(a)(4), 120.9(a)(2).
65 22 CFR § 120.16.
66 22 CFR § 121.8(f).
67 22 CFR § 120.10.
68 22 CFR § 120.10(a)(4). 69 22 CFR § 120.10(a)(2), (3).
70 22 CFR §§ 120.21, 120.22.
71 15 CFR § 734.3(b)(3); 22 CFR §§ 120.10(a)(5), 120.11.
72 15 CFR § 734.3(b)(3).
73 22 CFR §§ 120.10(a)(5), 120.11.
74 *See* Maarten Sengers & John Black, "Showing Defense Articles to Foreign Nationals in the U.S.: No License Required?," Export Prac., Oct. 1999, at 12.
75 *See id.* at 12–13.
76 15 CFR § 734.2(b)(ii); 22 CFR §§ 120.16, 120.17.
77 *See* INA § 274B(a)(3) [8 USCA § 1324b(a)(3)] (cited in 15 CFR § 734.2(b)(ii); 22 CFR § 120.16)).
78 *Id.*
79 *See* "Control Freaks: Deemed Recovery," Export Practitioner, Aug. 2000, at 9; *see also* www.bxa.doc.gov/DeemedExports/DeemedExportsFAQs.
80 22 CFR § 122.1.
81 Lisa Caplinger, "Putting Together a License Package for Hiring a Foreign Person," Soc'y for Int'l Affairs NewsNotes, Mar. 1997, at 4–6.
82 *Id.*
83 15 CFR § 734.3.
84 15 CFR Part 774, supp. 1.
85 22 CFR § 120.2.
86 22 CFR § 121.1.
87 *Id.*
88 22 CFR § 120.4.
89 Office of Chem. & Biological Controls & Treaty Compliance, Dep't of Commerce, Guidelines for Preparing Export License Applications Involving Foreign Nationals, Attachs. 1 & 2, "Standard License Conditions for Applications Involving Foreign Nationals."
90 15 CFR § 750.3.
91 15 CFR Part 746.
92 15 CFR Part 738, supp. 1; *see* 15 CFR § 738.3.
93 15 CFR § 738.4(a)(2)(ii).
94 15 CFR § 738.4(a)(2)(ii)(A).
95 15 CFR § 738.4(a)(2)(ii)(B).
96 15 CFR Part 746.
97 15 CFR § 740.13.
98 15 CFR § 740.6.
99 15 CFR § 740.6(a).
100 15 CFR Part 740, supp. 1.
101 15 CFR § 740.6(a).
102 15 CFR § 740.6(a)(3).
103 15 CFR § 740.6(a)(1), (2).
104 15 CFR § 743.1(b).
105 15 CFR § 736.2.
106 Office of Chem. & Biological Controls & Treaty Compliance, supra note 79, at 7–10.
107 *See id.*
108 15 CFR § 750.4(a), (b).
109 15 CFR § 750.7(g)(1).
110 15 CFR § 750.6.
111 15 CFR Part 756.
112 *See* Office of Chem. & Biological Controls & Treaty Compliance, supra note 79, at 7–10.
113 22 CFR §§ 120.21, 120.22.
114 22 CFR § 126.7.
115 22 CFR § 126.1(a).
116 22 CFR § 126.1(a).
117 22 CFR § 126.3.
118 22 CFR § 123.16.
119 22 CFR § 125.4.
120 22 CFR § 126.6(c). See generally David J. Kukelman, Joseph J. Dyer, Greg J. Correnti, "Foreign Military Sales/Edition II," BRIEFING PAPERS No. 99-5 (Apr. 1999).
121 22 CFR § 126.5.
122 64 Fed. Reg. 17531 (Apr. 12, 1999).
123 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).
124 22 CFR § 125.4(b)(8).
125 22 CFR § 125.4(b)(10).
126 22 CFR § 125.4(b)(13).
127 *See id.;* NISPOM § 10-200 (DOD 5220.22-M).
128 22 CFR § 125.4(b)(13).
129 22 CFR § 125.6.
130 *Id.*
131 *See* ODTC, Licensing Employment or Long-Term Visit of Foreign Person by a U.S. Company (Nov. 1996).
132 *See* ODTC, Guidelines for Preparing Technical Assistance Agreements, Manufacturing License Agreements, and Distribution Agreements 7 (Mar. 1998); 22 CFR §§ 124.7, 124.8, 124.9.
133 22 CFR § 124.10.
134 22 CFR § 124.3(b).
135 22 CFR §§ 124.1(a), 124.3.
136 22 CFR § 124.4.
137 22 CFR § 124.5.
138 22 CFR § 126.8(a)(3).
139 22 CFR § 126.8(c).
140 65 Fed. Reg. 45282 (Jul. 21, 2000).; Maarten Sengers, "State Department Liberalizes Licensing Requirements to NATO, Japan & Australia," Export Practitioner, Aug. 2000, at 15-16.
141 *See* Licensing Employment or Long-Term Visit of Foreign Person by a U.S. Company, supra note 121.
142 *Id.*
143 NISPOM § 10-509; *see* Soc'y Int'l Affairs NewsNotes, Sept. 1998.

144 Licensing Employment or Long-Term Visit of Foreign Person by a U.S. Company, *supra note 121*, TCP attach.; NISPOM § 10-509.

145 Licensing Employment or Long-Term Visit of Foreign Person by a U.S. Company, *supra note 121*, TCP attach.

146 Licensing Employment or Long-Term Visit of Foreign Person by a U.S. Company, *supra note 121*, TCP Attach., Exh. A, Sample "Non-Disclosure Statement."

147 22 CFR §§ 123.10, 125.7(b).

148 22 CFR § 125.9.

149 22 CFR § 126.13.

150 *Id.*

151 22 CFR 123.21.

152 22 CFR § 126.7(c).

153 50 USCA App. § 2410(a).

154 50 USCA App. § 2410(b).

155 *Id.*

156 50 USCA App. § 2410(c).

157 15 CFR Parts 764, 766.

158 22 CFR § 127.3; 22 USCA § 2778(c); 18 USCA § 3571.

159 22 CFR § 127.10; 22 USCA § 2410(c); 18 USCA § 2461.

160 22 CFR § 127.7.

161 *Id.*

162 FAR 9.406-2.

163 15 CFR § 764.5 (EAR); 22 CFR § 127.12 (ITAR).

164 15 CFR § 764.5(e)(7); 22 CFR § 127.12(b)(3)(iv).

165 31 CFR § 560.701; *see* 50 USCA § 1705; 18 USCA § 3571.

166 INA §§ 212(a)(3)(A), 237(a)(4)(A) [8 USCA §§ 1182(a)(3)(A), § 1227(a)(4)(A)].

167 32 CFR Part 154 (DOD 5200.2-R).

168 NISPOM § 10-300.

169 NISPOM §§ 1-100–1-104.

170 NISPOM § 2-100.

171 NISPOM Ch. 5.

172 NISPOM § 2-210.

173 *Id.*; 32 CFR § 154.16(c).

174 *See* NISPOM §10-201.

175 NISPOM § 2-210.

176 NISPOM §§ 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).

177 NISPOM § 2-210.

178 NISPOM §§ 2-210, 10-601(b).

179 32 CFR § 154.16(c)(1)(i).

180 NISPOM § 2-211.

181 NISPOM § 10-103 (describing National Disclosure Policy).

182 32 CFR § 154.16(c).

183 32 CFR § 154.16(d).

184 *Id.* 185 32 CFR Part 155, App. A ¶ 1.

186 32 CFR Part 155, App. A ¶ 28.

187 *See* NISPOM § 2-300.

188 *Id.*

189 *Id.*

190 NISPOM § 6-101.

191 NISPOM § 10-200 et seq.

192 *See* NISPOM § 6-105.

193 NISPOM § 6-101.

194 NISPOM § 10-502.

195 NISPOM § 10-507.

196 *Id.*

197 NISPOM § 10-104.

198 NISPOM § 10-507(d).

199 NISPOM § 10-507(a); 22 CFR § 125.5.

200 NISPOM § 10-507(b).

201 NISPOM § 10-507(c).

202 *Id.*

203 NISPOM § 2-210.

204 *Id.*

205 NISPOM § 10-508(c).

206 NISPOM § 10-509.

207 NISPOM § 10-508(b).

208 NISPOM § 10-508(a).

209 NISPOM § 10-202.

210 NISPOM § 10-204.

211 NISPOM § 10-510.

212 INA § 274B(a) [8 USCA § 1324b(a)]. *See generally* Lawrence J. Siskind, "Complying with IRCA," BRIEFING PAPERS No. 90-5 (Apr. 1990), IMMIGRATION LAW SERVICE, §§ 24:138 et seq., and Fragomen and Bell, IMMIGRATION EMPLOYMENT COMPLIANCE HANDBOOK (West Group OUP 2000).

213 INA § 274B(a) [8 USCA § 1324b(a)].

214 INA § 274B(c) [8 USCA § 1324b(c)].

215 INA § 274B(g) [8 USCA § 1324b(g)]; FAR 9.406-2(b)(2); Exec. Order No. 12989, 61 Fed. Reg. 6091 (1996).

216 INA § 274B(a)(2)(C) [8 USCA § 1324b(a)(2)(C)].

217 69 INTERPRETER RELEASES 326 (Mar. 16, 1992) (refusal to hire former Soviet citizen on ground that obtaining PCL would be unlikely); 67 INTERPRETER RELEASES 614 (May 12, 1990) (citizenship requirement may be imposed for positions requiring PCLs, but "across-the-board" requirement impermissible); 2 Immigr. Poly. & L. (BNA) No. 8 (June 2, 1988).

218 2 Immigr. Poly. & L. (BNA) No. 21 (Dec. 15, 1988).

219 42 USCA §§ 2000e-2(a), 1981.

220 *See* Letter from William Ho-Gonzalez of the OSC to Alice M. Yardum-Hunter (June 24, 1993).

Readers who are interested in contributing an article or ideas for a future Briefing,

please contact: Beverly Jacklin, 50 East Broad Street
Rochester, NY 14694
Telephone (716) 546-5530, ext. 3349