# DEEMED EXPORT AND RE-EXPORT COMPLIANCE: ISSUES RELATED TO ANTI-DISCRIMINATION AND FOREIGN LAWS

M. Beth Peters, Esq.
Aleksandar Dukić, Esq.
Gideon Maltz, Esq.
**Hogan & Hartson LLP**[*]
**Washington, DC**

## I. INTRODUCTION

It is generally understood that shipments or transfers of goods or data from the United States to another country represent an export that is subject to U.S. export regulations and potentially may require a license or other authorization. What is less widely known, however, is that the release of data even within U.S. borders can be deemed by U.S. export control laws to be an export to the recipient's country of nationality or citizenship. Similarly, the delivery of data in a foreign country to a national or citizen from a third country can be deemed a reexport to that third country.

Consequently, if a company is to avoid significant civil liability—as well as substantial damage to the company's reputation and good standing, and, potentially, criminal liability—it must exercise due caution in its management and release of controlled information and technology both inside and outside the territorial United States. Two recent Government Accountability Office reports, suggesting compliance issues in universities and industry, may well place pressure on the relevant government agencies to step up their monitoring and enforcement. 1/

This article lays out the broad sets of regulations that govern deemed exports (and reexports), explores the legal pitfalls with respect to anti-discrimination and privacy laws, both in the U.S. and abroad, that companies have to address, and outlines the suggested practices by which a company can promote regulatory compliance. While this article will focus exclusively on U.S. export regulations, companies with overseas operations should also carefully consider foreign export control regulations, which are becoming increasingly common. 2/

---

[*] M. Beth Peters is a partner and Aleksandar Dukić and Gideon Maltz are associates with the law firm of Hogan & Hartson LLP.

1/ Government Accountability Office, Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Companies, GAO-07-69 (Dec. 2006); Government Accountability Office, Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Universities, GAO-07-70 (Dec. 2006).

2/ For example, the 40 countries party to the Wassenaar Agreement recently agreed to stiffen restrictions on technology transfers to non-member countries. Gary Yerkey, "Export Controls Multilateral Regime Agrees to Tighten Controls on 'Intangible' Technology Exports," Export Controls (Dec., 2006).

## II. THE DEEMED EXPORT REGULATORY REGIMES

The U.S. government has established two primary regulatory regimes that govern exports and deemed exports. The Export Administration Regulations (EAR), which are administered by the Commerce Department's Bureau of Industry and Security (BIS), deal with "dual-use" items, software and technologies (i.e., those suitable for both military and nonmilitary uses). 3/ The International Traffic in Arms Regulations (ITAR), which are administered by the State Department's Directorate of Defense Trade Controls (DDTC), focus on "defense articles" and "defense services." 4/

Under both regulatory regimes, technology does not have to cross national borders to be subject to U.S. export controls. The provision of technical data to a foreign national temporarily working in the United States is effectively treated as an export to that foreign national's home country and triggers licensing issues under the EAR or ITAR. 5/ The reasoning behind the deemed export rule is that foreign persons 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 or obtained while in the United States.

### What Constitutes a Deemed Export?

Under the EAR, a deemed export is any release of technology or source code subject to the EAR to a foreign national in the United States (such release is deemed to be an export to the national's home country/countries). 6/ Under the ITAR, a deemed export includes disclosure (oral or visual) or transfer of technical data to a foreign person whether in the United States or abroad (although the ITAR does not formally refer to this activity as a deemed export, it is covered under the ITAR's definition of an "export"). 7/ Both regulations would regard the release of controlled information to the staff of a foreign embassy as a deemed export.

The EAR and ITAR rules cover virtually any means of communication to the foreign national, including telephone conversations, email and fax communications, sharing of computer data, briefings, training sessions, and visual inspection of equipment. 8/ A deemed export may occur when a company hires a foreign national, works collaboratively with foreign nationals employed by other companies, or merely hosts foreign nationals on a company visit or training.

Although the deemed export rule does not apply to controlled equipment as such, access to a controlled item may constitute a release of technical data: if mere viewing of an item would

---

3/ 15 CFR Parts 730—779.

4/ 22 CFR Parts 120—130.

5/ 15 CFR § 734.2(b)(2); 22 CFR § 120.17.

6/ 15 CFR § 734.2(b)(2)(ii).

7/ 22 CFR § 120.17.

8/ 15 CFR § 734.2(b)(3); 22 CFR §§ 120.17, 125.2(c).

reveal information, such exposure may constitute a deemed export (this will likely depend on the technical expertise of the individual with such access). 9/

**Who is a U.S. Person and Who is a Foreign Person?**

For the purposes of the deemed export regulations, U.S. persons are those who qualify as "protected individuals" under the Immigration Reform and Control Act (IRCA) of 1986. 10/ These individuals are U.S. citizens, U.S. legal permanent residents ("green card" holders), refugees, asylees, and temporary residents under specific IRCA amnesty provisions. 11/ Protected individuals may be exposed to EAR and/or ITAR-controlled information without triggering deemed export regulations. 12/ Anyone who is not a "protected individual" is a "foreign national" (under the EAR) or a "foreign person" (under the ITAR), which are legally equivalent terms. 13/

The EAR and ITAR do differ in their determination of foreign status in one crucial respect: the identification of the relevant nationality or citizenship of the foreign person. The BIS guidance on this matter states that the agency looks only at a person's latest citizenship or legal permanent residence in determining restrictions. 14/ The DDTC, under the ITAR, however, takes into account all of a person's nationalities and citizenships and imposes the controls that correspond to the most restrictive nationality or citizenship. So, for example, a Chinese national who subsequently became a Canadian citizen generally will be treated as Canadian by the EAR and as Chinese by the ITAR. We understand that the DDTC continues to review this issue internally.

**What is Technical Data or Technology That May be Controlled?**

The EAR controls the release of technology that could be applied to both civilian and military purposes. Technology broadly means the "information necessary for the 'development,' 'production,' or 'use' of a product." 15/ Significantly, the BIS recently clarified that "use" technology refers to the specific information necessary for the "operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing" of a product

---

9/ M. Beth Peters, David W. Burgett & Joy E. Sturm, "Foreign Nationals in U.S. Technology Programs: Complying with Immigration, Export Control, Industrial Security and Other Requirements," Immigration Briefings, (Oct. 2000) 7. See also M. Beth Peters, David W. Burgett & Joy E. Sturm, "Complying with Immigration, Export Control, and Industrial Security Requirements When Working Collaboratively with Foreign Nationals: A Case Study," The International Lawyer 35.1 (May 21, 2001).

10/ 15 CFR § 734.2(b)(ii); 22 CFR § 120.16.

11/ 8 USC § 1324b(a)(3).

12/ The regulations dealing with classified information treat only U.S. citizens as U.S. persons. National Industrial Security Program Operating Manual § 2-210.

13/ Supra note 10.

14/ Department of Commerce, "Revisions and Clarification of Deemed Export Related Regulatory Requirements," 71 Federal Register 30840, 30841 (May 31, 2006).

15/ 15 CFR Part 772.

(emphasis added), 16/ and the information must include all six of these categories to trigger an applicable "use" control. 17/ The definition of technology also includes "technical data" and "technical assistance," the latter of which may include instruction or consultation, as well as the transfer of "technical data" including blueprints, plans, diagrams, models, manuals, and instructions. 18/ The EAR deemed export rule applies to software only if its source code (the programming instructions that are intelligible to human readers) is released to a foreign person in the United States (in general, the EAR does apply to exports of software from the United States). 19/

The ITAR restricts the disclosure of technical data related to military articles and services. Technical data includes information "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." 20/ The ITAR further includes in the definition of technical data such classified information that relates to defense articles and services and information covered by an invention secrecy order. 21/ Technical data also includes software, both the source code and the object code (the binary translation of source code that is ready by a computer system). 22/

The EAR contains the Commerce Control List (CCL), which specifies the items, software and technology controlled, including the level of applicable controls. 23/ Items, software and technology controlled under the ITAR are included on the U.S. Munitions List (USML). 24/

Neither the EAR nor the ITAR control publicly available information. 25/ While the precise definitions differ under the two sets of regulations, publicly available information in both encompasses information already released through print publications, presentations at public conferences, fundamental research and documents posted on websites.

**Do Economic Sanctions Regulations Also Restrict Deemed Exports?**

The Treasury Department's Office of Foreign Assets Control (OFAC) administers the U.S. economic sanctions and trade embargoes against targeted countries, entities, and individuals

---

16/ Id.

17/ Supra note 14.

18/ Supra note 15.

19/ 15 CFR 734.2(b)(2)(ii).

20/ 22 CFR § 120.10.

21/ Id. at § 120.10(a)(2),(3).

22/ Id. at § 120.10(a)(4).

23/ 15 CFR Part 774, supp. 1.

24/ 22 CFR § 121.1.

25/ 15 CFR § 734.3(b)(3); 22 CFR §§ 120.10(a)(5), 120.11.

in furtherance of U.S. foreign policy and national security interests. 26/ Depending on the sanctioned country at issue, OFAC may share jurisdiction with BIS or may have exclusive jurisdiction to regulate exports to, and other activities with or involving, a sanctioned country or a targeted entity or individual. In general, OFAC restrictions with respect to a country that is subject to a comprehensive embargo (e.g., Cuba, Sudan or Iran) extend beyond a prohibition on exports and restrict imports, financial and other transactions, as well as facilitation of transactions and, in some instances, the ability to travel. 27/ OFAC regulations do not recognize the concept of deemed exports. However, they do restrict the ability of U.S. persons to receive or provide services to and otherwise deal with targeted individuals and entities, both within and outside the United States. 28/

Specifically, OFAC maintains a list of Specially Designated Nationals and Blocked Persons (SDNs), which includes persons and entities with whom U.S. persons cannot deal in any way (and whose property or interests in property within the possession or control of a U.S. person must be blocked/frozen). 29/ The SDN list contains more than 6,000 entries for persons and entities associated with terrorism, narcotics trafficking, the proliferation of weapons of mass destruction, and sanctioned country governments or other targeted entities. The SDN list is not an exhaustive list of persons with whom activities are prohibited. For example, all Cuban nationals are SDNs (unless they are legally resident in the United States or are otherwise unblocked) but they are not named on the SDN list.

A U.S. person is prohibited from engaging in virtually any transaction with an SDN. As such, no U.S. company could release any technical data to an SDN, either in the United States or abroad. Consequently, U.S. companies should ensure that its employees, customers, vendors, and subcontractors are not SDNs.

**What Are a Company's Risks under Deemed Export Regulations?**

In order to assess its risks with respect to deemed export compliance, a company should evaluate a number of factors. This risk assessment should form the basis of a company's decisions regarding the necessary breadth and depth of its deemed export compliance program. Companies should consider the nature of the technology or the technical data with which they work (is there information subject to the EAR, the ITAR, or both?); the location of facilities (what foreign countries are they in?); the nationality and citizenship of employees and subcontractors' employees, including those located abroad; and accessibility of controlled information (are documents stored in physically secure areas? Is electronic information segregated on a password-protected database?).

---

26/ More information about OFAC and U.S. sanctions programs is available at http://www.treas.gov/offices/enforcement/ofac/index.shtml.

27/ 31 CFR Parts 500—598.

28/ Federal regulations do allow the employment of Iranian and Sudanese nationals in the United States, if they have proper visas. 31 CFR §§ 560.505, 538.312(c).

29/ The SDN list is available at http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf.

## III. COMPLYING WITH DEEMED EXPORT REGULATIONS—WITHOUT VIOLATING OTHER LAWS

In seeking to fully abide by the various regulations governing deemed exports, a company must adopt a number of measures, which, if not handled properly, can expose it to legal liability. The measures include: collecting information on employees' citizenship status and, if necessary, further information on country/ countries of birth, citizenship, and residence; screening employees against OFAC's SDN list; and restricting unauthorized foreign national employees from certain positions and activities. These are all crucial steps in complying with deemed export regulations; but a company should undertake them with a complete understanding of antidiscrimination and privacy concerns under U.S. and foreign laws.

### Anti-Discrimination Laws in US

Any U.S. company must be mindful of domestic antidiscrimination laws, and take care to neither discriminate nor appear to do so. Title VII of the Civil Rights Act prohibits discrimination based on a person's national origin. 30/ Further, under the Immigration Reform and Control Act (IRCA) of 1986, "it is an unfair immigration-related employment practice… to discriminate against any individual (other than an unauthorized alien…) with respect to the hiring…of the individual for employment or the discharging of the individual from employment…because of such individual's national origin." 31/ However, the IRCA further provides an exception for those instances of "discrimination because of citizenship status, which is otherwise required in order to comply with law, regulation, or executive order." 32/

A company should gather, track and update the personal information of employees properly. The collection of I-9 forms at the start of employment is simply not a sufficient vehicle for deemed export compliance for most companies. The purpose of the I-9 form is for the employer to verify a person's identity and employment eligibility. This may be a sufficient means of deemed export compliance if a company only produces EAR99 items and technology; such companies need only address restrictions related to unblocked Cuban nationals, SDNs and other restricted parties, and sanctioned countries. However, for companies with controlled technical data under the EAR or ITAR, I-9 forms are, in themselves, not well suited to ensuring compliance with both the antidiscrimination laws and the deemed export rules. Employers may not dictate the types of documents employees show to verify identity and employment eligibility as it is the right of employees to choose from established lists of "A," "B" and "C" documents on the I-9 form. Some foreign citizens require company immigration sponsorship,, while others do not. In addition, members of the protected class, such as refugees and asylees, are not separately identified on the I-9 form.

Critical personal information may change over time. An employee who starts out as a foreign national may subsequently obtain permanent residence and become a protected person; the

---

30/ 42 USC §§ 2000e-2(a), 1981.

31/ 8 USC § 1324b (a)(1).

32/ 8 USC § 1324b (a)(2)(c).

company's policies with respect to that person need to change accordingly. For example, a company that refuses to hire or promote a person for a position that deals with controlled information acts lawfully if that person is a foreign national, but may commit unlawful discrimination on the grounds of national origin if the person has since become a protected person.

A company may ask prospective employees about their U.S. citizenship and nationality status and may ask questions designed to elicit information as to whether an individual falls within a protected class such that deemed export rules would apply. An employer must tread very carefully in making a hiring decision on the basis of this information. As a rule, an employer is not required to sponsor a foreign person for a work visa or an export license, so it may legitimately reject a foreign national applicant if the nature of the employment would require an export license. However, if a position is unrelated to controlled technology but hiring the foreign national would require a company to take a small effort to prevent her unauthorized access, the company should assess this situation carefully and consult experienced legal counsel.

An employer should also take care not to give any appearance of discrimination. In collecting personal information, it should explain that it needs to do so in order to comply with federal export control regulations. A company should keep all records and documentation. Best practice is to collect all the necessary personal information at the application stage in a uniform manner on a written form, and a company must make sure to solicit such information from everyone, and not just those whom it suspects to be non-U.S. persons.

**Anti-Discrimination Laws Overseas**

U.S. companies with overseas operations may confront a difficult tension between the EAR, and in particular the ITAR, and foreign anti-discrimination laws. Deemed reexports occur when technology or software has been legally exported to an end-user in one country and foreign nationals from another country are permitted to come into contact with that licensed technology.33/ The issue arises, for example, where a U.S. company lawfully shares a controlled technology with a Canadian subsidiary that employs Canadian nationals, but then hires a Canadian citizen of Chinese birth. As discussed above, although the EAR treats the new employee as Canadian, the ITAR treats her as Chinese and deems any transfer of information to her as an unauthorized reexport. In addition, because of the U.S. arms embargo against China, DDTC is not likely to issue the necessary ITAR authorization to the Chinese employee.

However, while ITAR regulations may require differentiation among citizens of the same country on the basis of their nationality, such a policy can be viewed, on its face, as discrimination on the grounds of national origin. Such discrimination raises legal issues in many foreign countries. A U.S. company that has any dealings with ITAR-controlled technology in a foreign country, whether through a foreign subsidiary or not, is likely to face this issue.

This conflict between compliance with the ITAR and local antidiscrimination laws has arisen in several countries. General Motors and General Dynamics have faced civil lawsuits, as well as

33/ 15 CFR § 734.2(b)(4); 22 CFR § 125.1.

investigations by the Ontario Human Rights Tribunal, for laying off foreign-born Canadian employees for ITAR compliance reasons. 34/ The Canadian Department of National Defense (DND) itself recently noted in an internal memorandum that denying access to DND employees who were born in or hold citizenship of certain other countries constitutes "discriminatory employment practices… contrary to Canada's Charter of Rights and Freedoms." 35/ Similarly, Australian companies that refuse to use staff "born in countries blacklisted by the US" may be responsible for "a contravention of federal anti-discrimination laws." 36/

Companies that find themselves in this awkward position may in some instances be able to seek exemptions to the local anti-discrimination laws or carve out a position for the employee that restricts access to the controlled technology. In other instances, they will have to make a difficult choice, taking into account the aggressive enforcement of the U.S. export control laws and the associated criminal and civil penalties.

**Privacy Laws in the EU**

The EU-based subsidiaries of U.S. companies must address privacy regulations in their efforts to comply with U.S. regulations. Privacy concerns tend to arise in two scenarios: the first is where an EU-based subsidiary screens employees (or any persons with which it enters into transactions) against the SDN list, or for citizenship or nationality information, and to this end seeks to transfer the relevant personal information back to a site in the U.S. so as to run the screening. The second is where an EU-based subsidiary requests its employees to submit the same information to another U.S. company that insists upon running its own mandatory screening.

The EU passed its Data Protection Directive in 1995, setting the floor for data protection for member countries (national legislation may be more restrictive). 37/ Failure to comply with privacy legislation may bring administrative, civil and even criminal penalties. 38/ The Directive allows the transfer of data to a third country only if "the third country in question ensures an adequate level of protection." 39/ In 1999, the European Commission declared U.S. privacy laws to be inadequate under the Directive, making any transmission of personal data from the EU to the U.S. problematic. 40/ The Directive does allow the transfer of data to a third

---

34/ Ian Austen, "Strict Rules Disqualify Some Canadian Arms Workers," New York Times (Dec. 12, 2006).

35/ "US-Canada Dispute Brewing over American Export Controls on Sensitive Military Technology," UPI (Nov. 3, 2006).

36/ Brendan Nicholson, "US Rejects Workers on Nationality," The Australian (Nov. 9, 2006).

37/ Directive Of The European Parliament On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, 95/46/EC (Oct. 24, 1995).

38/ Francois Gilbert, "How to Legally Transfer Personal Data from the European Union," 865 PLI/Pat 545, 552 (Jun.—Jul. 2006).

39/ Supra note 37 at art. 25.1.

40/ European Commission (Directorate General XV) - Data Protection Working Party: Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government (Jan 26, 1999).

country that lacks the adequate level of protection under certain enumerated circumstances or pursuant to extraordinary protections for the data. 41/ In practice, the only enumerated condition that a company can usually invoke is that "the data subject has given his consent unambiguously to the proposed transfer." 42/

Consent is the cornerstone of any analysis of how a company in the above two scenarios should proceed. A subsidiary that seeks to transfer personal data of employees back to the U.S. for screening will have a difficult task: a person whose employment depends on cooperation does not provide consent under EU law. 43/ The subsidiary would be well-advised to purchase its own screening software and conduct the process within the EU. (If the screening identifies a match with the SDN list, the subsidiary may at that point transfer the information to the U.S. for further investigation).

A company that seeks to transfer employees' personal data to another company in the U.S. for it to conduct is own screening may be able to lawfully do so. The company will need to take measures to ensure that the process is free of coercion and effectively characterize the submission of personal data as each employee's individual choice, free of adverse professional repercussions. The company will also need to ensure that there is informed consent and that the employee clearly understands the rights she is waiving. 44/ In some countries with more stringent regulations, such as Germany, the company may need to take further steps, such as meeting with the local labor boards to procure permission.

## IV. THE MECHANICS OF COMPLIANCE

With antidiscrimination and privacy concerns in mind, a company seeking to comply with deemed export regulations must undertake a four-step process: identify whether the technology with which it works is controlled by the EAR, ITAR, or both; collect personal information from employees (or other persons that might be exposed to its technology) to address applicable export controls; analyze whether and to what extent particular employees are permitted unlicensed access to the technology; and, in those cases where employees are not permitted unlicensed access, take appropriate measures to prevent unauthorized access. This is a complicated legal process that, as the recent GAO reports suggest, many organizations do not fully understand. 45/

### Identification of Technology

The first step for a company is to survey the various technologies it uses and determine which fall under the EAR or ITAR. The EAR's Commerce Control List contains 10 categories of controlled items: nuclear materials, chemicals and toxins, materials processing, electronics,

---

41/ Supra note 37 at art. 26.

42/ Id.

43/ Supra note 38 at 560.

44/ Id. at 561.

45/ Supra note 1.

computers, telecommunications (including satellite communications technology) and information security (including encryption), lasers and sensors, navigation and avionics, propulsion systems, and certain space vehicles. 46/ Items subject to EAR but not enumerated within a particular category fall within a residual category known as "EAR99." It is important to ascertain not only whether a company's technology is subject to EAR but also which specific EAR categories apply and what is the specific Export Control Classification Number (ECCN) for those items included on the CCL, as the rules for foreign persons' access vary amongst various ECCNs due to the reason for the export control. 47/

The ITAR applies generally to defense articles, services and related technical data and software. The USML establishes 21 categories of controlled items, including military equipment, military electronics, military cryptographic items and equipment, ammunition, spacecraft systems and associated equipment, and nuclear weapons design and test equipment. 48/ A company with no technology that qualifies under the ITAR need not be concerned with its increased restrictions and restrictive interpretation of dual nationality and therefore may implement a more narrowly tailored screening process—collecting less information—based on its risk assessment.

**Collection of Personal Information**

The second step is to identify whether an employee is not a U.S. person and, if so, solicit information which may include country of birth, country (or countries) of citizenship, and country (or countries) of residence—in order to ensure compliance with U.S. export control requirements. Further, to run initial screening against the SDN list, a company will need the employee's name, and if there is a provisional match, such additional information as date and place of birth, address, and passport number. (If a prospective hire appears on the SDN list, then there is no need for further analysis of the type of technology and so on—a company generally must refrain from any transaction with an SDN).

A company should collect all this information prior to the initiation of a person's employment at the company; if a company has not collected this information from current employees, then it should do so immediately. The company should also make sure to update this information over time, so as to identify when a foreign national becomes a U.S. person, or benefits from a change in citizenship status (for example, becoming a Canadian resident) warranting more liberal treatment, or when an employee gets placed on the frequently updated SDN list.

**The Match of Specific Technologies and Foreign National Information**

The third step a company should take is to analytically match the particular sorts of technologies with which the company deals to the personal details of the employee. Under the EAR, the EAR99 classification generally does not require a license (unless a Cuban national is involved);

---

46/ Supra note 23.

47/ Some of the reasons for controls are the following: chemical and biological weapons, nuclear nonproliferation, national security, crime control and anti-terrorism. 15 CFR Part 738, supp. 1.

48/ Supra note 24.

certain other categories of technology generally do not require a license when exposed to foreign persons of certain countries; and even amongst those areas where a license is nominally required, regulatory exceptions generally negate the licensing requirement for certain types of technology exposed to foreign persons of certain countries, usually pursuant to a written agreement that the foreign person will not reexport the technology. 49/ All of these provisions are subordinate to the EAR's general prohibitions on exposing the technology, which include any situation where a company knows that the export will indirectly result in a violation of EAR (e.g., because the putative end-user will engage in an illegal reexport). 50/

The ITAR is more restrictive and requires a license for all technology that falls under its purview. The ITAR does provide for certain exemptions to the licensing requirement under very specific conditions. 51/ The only country-specific exemption concerns the release of certain kinds of unclassified technical data to Canadians, under specific circumstances. 52/

This series of analyses is very complex and highly fact-specific. The results depend on the precise nature of the technology involved and the citizenship or nationality of the employee. Unsurprisingly, foreign national employees from friendly countries are far more likely to have lawful unlicensed access to technology than those who are not.

**Seeking a License**

Having determined the precise contours of each foreign national employee's lawful unlicensed access to technology, the company must decide how to address the legal restrictions on certain employees: in each instance, it can either seek a license from the U.S. government so as to provide an employee with lawful access, or, if not, comprehensively restrict the access of the employee to the relevant technology.

If a company chooses to seek a license for its employee, then under the EAR, it must provide specific information concerning the company, the relevant technology, measures to prevent unauthorized access to controlled technology, and the foreign person. If the BIS grants a license, it will typically have a duration of two years and may carry various conditions, including that the applicant company "establish satisfactory procedures to ensure compliance" with license conditions and share these procedures with the BIS. The BIS reports that in FY 2006, it approved 85 percent of the 830 deemed export license applications it received. 53/

---

49/ See generally 15 CFR Parts 738, 740, 746.

50/ Id. at § 736.2.

51/ 22 CFR §§ 125.4, 126.6.

52/ This exemption applies to "Canadian-registered persons," which may include persons with other nationalities or citizenships, so long as those countries are not specifically barred under the regulation; the exemption does not apply to the categories of design methodology, engineering analysis, or manufacturing know-how. Id. at § 126.5.

53/ "Deemed Export in Universities, Government Laboratories and Industry" Panel, Society for International Affairs Conference, Washington DC (Nov. 6—7, 2006).

Under the ITAR, a company must submit a more burdensome license application. At the very least, the applicant company must provide specific information on the company, the technology, the justification for disclosure, and the employee; the company must also declare that it seeks to retain the foreign national due to "acute shortages of technical personnel in the area of our needed expertise." 54/ The DDTC places no time limit on the licensing process and will usually pass the application along to the Department of Defense, and other agencies as appropriate, for review. If DDTC approves a license, it will generally have a four-year duration. The ITAR license approval process is more rigorous and a number of countries, such as China and Venezuela, are "proscribed destinations" and are subject to a policy of denial. 55/

**Preventing Unauthorized Access**

The licensing procedures aside, a company will in many instances need to restrict an employee's access to controlled information. To do so successfully will require a comprehensive corporate strategy. A company must establish safeguards in the information technology infrastructure so that an unauthorized foreign national employee cannot simply access controlled information from her computer. This might mean creating a dedicated, password-protected server for controlled information and removing any sensitive materials from the company intranet.

A company must also take measures to prevent accidental transfer of controlled information. At a minimum this will require a company policy of clearly marking as such all documents that contain controlled information and training employees to be take due care. More sophisticated solutions might include email software that prevents designated emails from being printed or forwarded, that automatically deletes the email after a designated period of time, or that identifies in the directory those employees that are subject to restrictions.

A company must also configure the physical workspace appropriately. If certain technology is of the sort that mere visual inspection would reveal controlled information, then a separate facility and restricted key card access might be appropriate. Employees should also take due care to store controlled information in locked desks or cabinets.

Central to any compliance strategy is the effective training of personnel. A company should highlight the key points of deemed export control regulations to all its employees; and also explain that they are mark all sensitive documents appropriately, store them securely, and take precaution not to communicate in emails, telephone calls or casual conversation any controlled information to unauthorized employees. A company should also train the unauthorized foreign national employees themselves to make sure that any document they receive does not contain controlled information. More senior managers who have responsibility for supervising the work of unauthorized employees should receive more advanced training to allow managers to carve out projects for such employees in an appropriate fashion.

---

54/ Office of Defense Trade Controls, Licensing Employment or Long-Term Visit of Foreign Person by a U.S. Company (Nov. 1996)

55/ 22 CFR § 126.1(a).

**Working with Subcontractors**

Finally, a company should focus not only on its own employees, but also on its subcontractors. If a company works with a foreign subcontractor, it will obviously need to follow the government licensing procedures laid out above. But even if a company works with a domestic subcontractor, it has strong legal and business interests in ensuring that the subcontractor complies fully with U.S. government regulations. The company's legal interest is in avoiding any liability if it transfers controlled technology to its subcontractor—so it must establish safeguards for the subcontractor to handle it properly. The business interest is in ensuring that the subcontractor is able to effectively deliver on the contract and not find itself at the center of government investigation. A company should therefore insert into the relevant agreements provisions on the subcontractor's compliance with the EAR, ITAR and various sanctions programs.

**GUIDELINES**

These guidelines are designed to aid in understanding the regulatory framework that applies when U.S. companies, or their subsidiaries, hire foreign persons.

1. Identify all controlled technology and software in the company and classify it under the EAR or the ITAR. 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.

2. When hiring an employee, determine whether the individual is a U.S. citizen, or, if not, whether the individual is a legal permanent resident, refugee or asylee. Foreign persons with any of these statuses may work in the U.S. on an indefinite basis and do not trigger export licensing requirements. Also, screen any potential hire against the SDN list.

3. If an employee is not a U.S. legal permanent resident, refugee or asylee, then collect, in a uniform manner and in writing, further information on country of birth, country (or countries) of citizenship, and country (or countries) of residence. Be sure to track any changes in the personal information of an employee.

4. 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 based on citizenship and national origin. If you have overseas operations, consult the law concerning nondiscrimination; if provisions of the ITAR and foreign law conflict, seek a waiver from the foreign law, if possible, or take appropriate steps to minimize legal exposure.

5. If you have EU subsidiaries, consult the EU and national regulations on privacy protections. Ensure that any transfer of personal information to another country deemed not to have adequate protections, such as the U.S., is only done pursuant to genuine and informed consent on the part of the employee.

6. Determine whether the foreign person who is a potential hire or current employee is from a "sensitive" country. This includes, but is not limited to, countries subject to OFAC sanctions and,

if the ITAR applies, the proscribed or embargoed destinations set forth in the ITAR. Obtaining a license for the release of covered technology, software, or technical data to any such foreign persons may be difficult, or even impossible.

7. If it becomes clear that a license cannot be obtained for a foreign person, 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 person will be "walled off" from all controlled technology and software. The permanent resident process can take years to complete.

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 persons. If so, be sure to obtain such documents and provide them to the appropriate agency as necessary.

9. Because the processing of export licenses can take considerable time (90 days or longer), companies must often delay their employment or ensure that the foreign person does not access controlled technology until an export license is issued.

10. Take appropriate measures to prevent the exposure of controlled technology to unauthorized foreign persons. Be aware of the circumstances in which a release of controlled information can occur—including through telephone conversations, e-mails, computer networks, and fax communications.

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