

Legal advisory from Nixon Peabody, employment counsel to Union College

July 9, 2009 , http://www.nixonpeabody.com/publications_detail1.asp?ID=2816

An ounce of prevention: Knowing the deemed export rules

Did you know that simply sharing information with a foreign national in a business or academic setting can expose you and your organization to U.S. export laws? Violating these laws can be serious, resulting in criminal and civil sanctions. What questions can you ask of prospective or current employees? Do you need a license from the federal government in order to share sensitive information? Our White Collar, Immigration, and Labor and Employment attorneys can guide you and your organization through these issues to help protect you from unwanted scrutiny.

7/9/2009

When you think of the word “export,” likely your first thought is of sending something overseas. That “something” is generally tangible. But, for companies and institutions that employ or otherwise engage with foreign nationals, the word export has a far broader definition that includes intangibles such as the sharing of data or information with foreign nationals who are in the United States. Under the deemed export rule, the release of controlled technology to a foreign national working in the United States is akin to a direct export of that technology to the foreign national’s home country, even though it never crosses borders. Like typical exports, these technologies may require licenses from the government before they can be released to foreign nationals. Deemed exports, thus, present issues unique to U.S. companies and entities that interact with foreign nationals and can arise in both business and academic settings.

Why should you care?

The deemed export rules can greatly complicate an entity’s operations. Companies, universities, and other institutions working with controlled technology that employ foreign workers; use foreign consultants; or have branches, campuses, or subsidiaries outside of the United States should be especially wary. Inter-company communication, or even the failure to secure technology internally from your own employees, can cause difficulties. Further, the now-common use of the Internet in business opens up an entirely new avenue of potential exposure. Compliance with these complex rules is a tricky endeavor, but the risk is real, and entities will save much time and many resources by ensuring that they have proper procedures in place before a problem arises and that they properly manage potential violations.

In recent years, government agencies have steadily increased their enforcement of export controls, and the consequences of noncompliance have become progressively more severe. In 2007, the civil and criminal penalties for export control violations increased dramatically. Today, a single civil violation can result in a \$250,000 civil fine or twice the amount of the transaction upon which the penalty is imposed, and a criminal violation can result in a penalty of up to \$1 million per violation and/or imprisonment for 20 years. Moreover, civil penalties can attach retroactively, with the enlarged penalties punishing years-old conduct. Another consideration is the person who is making the transfer. Separate from the aforementioned criminal and civil penalties, if the person making the transfer is not a US citizen, he or she may face removal as a consequence of an illegal transfer to a foreign national.

In addition to increased penalties, in 2007, the U.S. Department of Justice appointed its first national export control coordinator. The coordinator, career prosecutor Steven Pelak, has educated prosecutors on how to bring successful cases in this complicated area, and has been holding prosecutors accountable by requiring regular reports on such investigations. With this type of attention being paid, there is no doubt that export cases will continue to be on the rise in coming years.

Moreover, the federal government is keeping a watchful eye on exports by setting up programs like the Federal Bureau of Investigation (FBI) Counterintelligence Domain Program, which is a national, multi-agency initiative focused on sharing information with private industry and academia to safeguard critical U.S. research and technology. Participants in the program include the FBI, Defense Security Service (DSS), Army Counterintelligence, Naval Criminal Investigative Services (NCIS), Air Force Office of Special Investigations (AFOSI), Counterintelligence Field Activity (CIFA), and the Department of Commerce (Project Guardian). Agents have been known to “drop by” companies and academic institutions to make sure they are taking steps to prevent the unauthorized transfer of technology or sensitive information.

The failure of companies, academic institutions, or individuals to heed the deemed export laws has resulted in actual prosecutions and significant jail time. In May 2008, a California-based manufacturing corporation paid a \$31,500 fine for allowing one of its employees, a citizen of Iran, to access technology relating to the production of aircraft parts. Last September, a retired professor from the University of Tennessee was convicted by a federal jury of export control violations after allowing two foreign national graduate students to access information about a military defense project. On July 1, 2009, he was sentenced to four years in prison.

What is a deemed export?

Deemed exports take their name from the Export Administration Regulations (EAR), the export control regulations set forth by the Department of Commerce. The EAR provide that the release of technology or source code to a foreign national is “deemed” to be an export to that recipient’s home country. The Department of State’s export controls (the International Traffic in Arms Regulations, or ITAR) contain a similar provision in its definition of an export.

The regulations define a “release” of technology broadly. A release includes any transfer of information through visual observation, oral communication, experience, or practice. A company need not transfer information intentionally for the rule to apply; the fact that the foreign national is exposed to the information in the course of his or her job constitutes a release. An e-mail message, a facility tour, or even providing access to a computer that is unsecured can give rise to a deemed export violation.

The deemed export rule also includes “deemed re-exports,” which are transfers of U.S.-origin technology to foreign nationals that occur outside of the United States. Even if the technology was legally exported overseas in the first instance, the exporter must obtain a second license before it can release that information to a foreign national who is not a citizen of the country of import. For this reason, deemed re-exports are of particular concern for any company and institution with a multi-national presence.

Importantly, not all controlled technologies qualify as deemed exports, and not all deemed exports require licenses. The inquiry turns on two threshold determinations: the regulatory classification of the technology, and the citizenship of the foreign national.

Identifying a deemed export—and whether any exceptions apply

The first step for a company or institution dealing with a potential deemed export is to determine the proper classification for the technology. Under the export control regime (setting aside embargoes and similar trade sanctions), the governing export regulations are based on the technology (commercial, military, or dual). The classification lists in the relevant regulations specify the level of control for those technologies.

Some technologies are exempt from licensing under the export regulations. For example, certain technology subject to the EAR does not require a license under most circumstances. Additionally, there are discrete license exceptions enumerated in the provisions of EAR and ITAR. Companies and institutions should consult these provisions to determine whether any of them apply to the technology at issue.

Once classification has been resolved, the second step is to determine the citizenship of the foreign national who will encounter the technology. If direct export of the same technology to the foreign national’s home country is prohibited without a license, transfer of that technology to the foreign national within the United States likewise is prohibited without a license. Foreign nationals who are naturalized U.S. citizens, or who have obtained permanent U.S. resident status (green card holders), are exempt from the deemed export rule. There is also a narrow exception for “protected individuals,” which includes political refugees and asylees. If the foreign national does not fall into one of these categories, however, the deemed export rule applies.

If both of these determinations trigger the deemed export rule, companies and institutions should next consider whether the technology qualifies for an exemption from the rule. The exemptions are limited, but, if they are met, the company does not have to obtain a license even though the technology otherwise qualifies as a deemed export. These exemptions include:

- *Technology that is “publicly available” or “in the public domain.”* If technology is ordinarily published and generally accessible to the public, it does not require a license. Information is considered publicly accessible if it is available for free, or for a nominal fee that covers cost plus a reasonable profit. For example, technology discussed at an open conference—meaning a conference that is open to all members of the public, and at which the attendees can take notes—would be considered publicly available.
- *Technology arising from “fundamental research.”* This exception is particularly notable for universities and other educational institutions that have foreign national students or professionals among their ranks. “Fundamental research” is defined as scientific and/or engineering research that is conducted at a higher education institution, the results of which are ordinarily published (or intended to be published) and shared broadly within the scientific community. Research is

not fundamental if the institution accepts any restrictions on control or access, or on dissemination or publication of the results. Such restrictions are characteristic of proprietary research, which requires a license.

- *Technology arising in the context of general education.* Under most circumstances, information released during the teaching of general education courses (sometimes limited to math, science, and engineering) is exempt from licensing, even if it contains controlled technology. Notably, however, release of the same technology *outside* of the classroom or teaching laboratory may require a license.

Increasing the chances of license approval

Absent an applicable exemption, a company or institution must file an application for an export license before releasing export-controlled technology to a foreign national. This application must contain information including, but not limited to, biographical and vocational details of the foreign national; copies of the foreign national's passport, visa, and current resume; a description of the technology the foreign national will encounter and the capacity in which it will be used; and the form in which the technology will be released. Because the license approval process can take months—and because there is no provision allowing a foreign national to access the technology while the license is pending, those seeking export licenses are advised to file their applications immediately upon determining that a license is needed.

The U.S. Department of Commerce's Bureau of Industry and Security (BIS), which processes most deemed export applications, has indicated that including certain supplemental information in a license application can accelerate the approval process. For example, if the foreign national possesses special expertise that is of particular value to the company or institution, the application should so state. Also helpful is evidence that the foreign national has strong ties to the United States, such as family in the country. Similarly, a showing that the foreign national lacks ties to the home country can also be useful to BIS's evaluation of the application.

Changes to the export regime may be on the way

A chief criticism of the deemed export rule is that it stifles the advancement of technology in the name of protecting national security. While a restrictive approach to the dissemination of technology may serve important national security interests, the constantly evolving nature of the global marketplace may decrease U.S. competitiveness. Some fear that over-regulating the transfer of technology may result in foreign students and professionals taking their technological talents elsewhere, thus weakening U.S. companies and universities. Acknowledging this tension between protecting security and furthering research, the U.S. Department of Commerce recently formed an advisory committee to assist it in identifying emerging technologies and recalibrating export controls. This newly formed group, called the Emerging Technologies and Research Technical Advisory Committee, has yet to make any public recommendations, but, for those who interact with foreign nationals, the committee's determinations could have a significant impact on the scope and enforcement of export controls.

Compliance is your best protection

Given the stakes of non-compliance, companies and educational institutions should evaluate their technologies and their relationships with foreign nationals, and should ensure that their policies and procedures comply with the deemed export rule (and with all U.S. export controls). Effective, thoughtful compliance and training programs, coupled with regular reviews or audits, are essential to companies and institutions that engage foreign nationals in their operations. Compliance can be tricky because compliance with export controls must not lead to non-compliance with applicable employment discrimination laws. It is important that employers advise prospective employees that eligibility to receive deemed exports of controlled technology is a condition of employment for key technical and IT positions. And, of course, any information collected or received regarding an employee's or applicant's nationality or citizenship must only be used for export control compliance or other lawful purposes, and must not be used to unfairly discriminate in the hiring process or employment relationship. Prudent employers should consult with counsel as to when and how to collect such information, how to use it lawfully, and when and how to retain it.

With increased globalization, vigilance in the area of deemed exports is critical. Failure to abide by the rules that govern such exports can lead to severe consequences. As is often said, an ounce of prevention—or compliance—is worth a pound of cure.

The foregoing has been prepared for the general information of clients and friends of the firm. It is not meant to provide legal advice with respect to any specific matter and should not be acted upon without professional counsel. If you have any questions or require any further information regarding these or other related matters, please contact your regular Nixon Peabody LLP representative. This material may be considered advertising under certain rules of professional conduct.