The Deemed Export Rule:  
What Companies Should Know Before Transferring
Commerce-Controlled Technology to Foreign Nationals

Kathleen M. Paralusz

I. INTRODUCTION

In a post-September 11th America, perhaps one of the most critical objectives in promoting our national security is preventing would-be terrorists and the countries that harbor them from gaining access to sensitive U.S. technology. One of the best ways in which the U.S. Government and U.S. companies can achieve this goal is to vigorously monitor the transfer of controlled dual-use technology, software and technical data to foreign nationals. Accordingly, all companies with foreign national employees should be familiar with the legal implications associated with the “Deemed Export Rule.”

Under the Deemed Export Rule, the U.S. Department of Commerce (“Commerce”) treats the release of U.S.-origin technology, software and technical data to foreign nationals in the U.S. as an export to the individual’s home country. Consequently, the Deemed Export Rule can have a considerable legal impact on companies employing foreign nationals. By employing foreign nationals in positions in which they have access to controlled technology, a company is, for legal purposes, exporting that technology to another country, even if the transfer occurs within U.S. borders and the information never leaves the country. Further, depending on the nature of the technology involved and the country at issue, the Deemed Export Rule can trigger U.S. export licensing requirements and expose a company to significant legal liability for failure to comply with those requirements.

II. THE DEEMED EXPORT RULE

The Deemed Export Rule is codified under the Export Administration Regulations (“EAR”) at 15 C.F.R. 734.2(b)(2)(ii) and administered by Commerce's Bureau of Industry and Security (“BIS”). Under the Rule, an export of U.S.-origin technology, software, or technical data is deemed to take place, for legal purposes, when it is released to a foreign national. “Release” is broadly defined and can occur via any of the following methods: (1) visual inspection (including reading technical specifications, plans, blueprints, etc. or viewing U.S.-origin equipment or facilities); (2) oral exchange of information in the United States or abroad; or (3) application abroad of personal knowledge or technical experience acquired in the United States.

For BIS’ purposes, covered technology includes data required for the design, development or production of controlled items. Therefore, it is imperative that companies correctly classify their commodities on Commerce’s Commodity Control List (“CCL”) and establish the appropriate export licensing requirements. The primary concern, of course, is that companies run the risk of violating U.S. export controls simply by employing foreign nationals in positions in which they have access to controlled software, technology or technical
information without obtaining appropriate export licenses. As a general rule, if a company’s commodity requires a license to export to a particular country, then it is highly likely that an export license will be required to transfer technology to a foreign national from that same country when the technology involves the design, development or production of that commodity. Note that the Rule does not apply to publicly available technology, nor does it apply to U.S. citizens, permanent resident visa holders, refugees or asylees.

III. LICENSING AND ENFORCEMENT

A. Export Licensing

Deemed export licenses generally are valid for 2 years and comprise nearly 10 percent of all export licenses approved by BIS. In 2001, for example, BIS approved 822 deemed export license applications and rejected 3. Most of the approved licenses authorized foreign nationals to work with advanced computer, electronic, or telecommunication and information security technologies in the United States. These approvals included foreign nationals from countries of concern, such as China, Russia, Iran, India, Syria, Iraq and Pakistan.

BIS reviews deemed export licenses in accordance with the same procedures that apply to export license applications for tangible commodities, software or technical data. Therefore, a company should identify all potential exposure or access a foreign national employee might have to controlled technology, software and technical data. Next, the company should determine the proper CCL category, reasons for control, and whether any license exception applies. For example, if the Technology and Software Restricted (“TSR”) exception applies under Part 740.6 of the EAR, then the company need only obtain from the employee a signed non-disclosure assurance statement that he or she will not disclose, transfer or re-export the information in violation of U.S. export controls.

Assuming that a license is required, however, a company must apply for a deemed export license when both of the following conditions are met: (1) the company intends to transfer controlled technology to the foreign national in the United States; and (2) transfer of the same technology to the foreign national’s home country would require an export license. The company must file Form BXA-748P and submit a letter of explanation providing certain information about the employee and the scope of the proposed transfer. This information includes: (1) basic personal information about the employee, including his country or countries of nationality, place of residence and other biographical details; (2) the location of proposed employment; (3) a detailed job description, including the responsibilities of the position and the scope of the employee’s possible contact with other persons with access to controlled technology or information; (4) a description of the technology, software or technical data involved and the form in which it will be released to the employee; (5) a description of the commodity to be produced with the controlled technology, including a description of the manufacturing process and the company’s output capacity; and (6) an explanation of how the company will benefit from employing the foreign national (i.e., how the employee will affect product improvement, technical processes or other services).
In all circumstances where a company believes that a deemed export license may be required, the company should take special precautions to ensure that the foreign national employee involved does not access controlled technology, software or technical data unless and until BIS issues license approval. As discussed below, failure to obtain BIS’ approval prior to releasing controlled technology, software or technical data to a foreign national can result in serious criminal, civil and administrative penalties, both for the individuals involved and for the company itself.

B. Enforcement

As a result of the national security concerns stemming from countries upgrading their military capabilities with U.S. civilian technology, Commerce has begun to increase its enforcement of the Deemed Export Rule in recent years. Prior to 2000, Commerce treated violations of the Rule as civil enforcement matters. However, in October 2000, a U.S. grand jury in San Jose, California indicted two executives and their companies for illegally transferring sensitive software and technology to China in violation of the Deemed Export Rule. The indictments against Silicon Telecom Industries, Inc., Suntek Microwave, Charlie Kuan and Jason Liao mark the first time that Commerce has prosecuted companies and individuals for violating the Rule. As of December 2002, a trial setting hearing had been scheduled for the two companies and Jason Liao. Charlie Kuan entered guilty pleas on the counts against him and was awaiting sentencing.

The criminal indictments suggest that Commerce is beginning to focus more aggressively on enforcing the Deemed Export Rule. Given the events of September 11, 2001, it is highly likely that this effort will only intensify. Therefore, companies should be aware of the various penalties associated with violating the Rule, including the criminal, civil and administrative penalties that can be assessed against a company and/or individual involved with a violation.

Under the EAR, criminal penalties for “knowing violations” include: (1) fines of five times the value of the exports involved or $50,000, whichever is greater; (2) imprisonment for up to five years, or (3) both. By comparison, the criminal penalties for “willful violations” are even more severe. “Willful violations” are those violations that occur with the knowledge that the exports involved are intended for or will be used to benefit a controlled country or any country to which exports are controlled for foreign policy or military intelligence gathering purposes. The penalties for “willful violations” include fines of up to $1 million per violation for corporations; for individuals, the penalties include fines of up to $250,000 per violation and up to 10 years imprisonment, or both.

The civil and administrative penalties for violating the Deemed Export Rule are equally harsh. Companies and individuals can be assessed civil penalties of up to $10,000 per violation, or up to $100,000 per violation for violations involving national security controls. On the administrative side, violations also may result in the revocation of export licenses, denial of export privileges and/or exclusion from practice before BIS.

As these penalties suggest, violations of the Deemed Export Rule can have severe consequences for the company and individuals involved. Therefore, as a practical matter,
companies should be vigilant in ensuring compliance with the Rule and obtaining appropriate export licenses before transferring any controlled technology, software or technical data to foreign nationals.

IV. CONCLUSION

Following the events of September 11th, the Deemed Export Rule no doubt will continue to have a significant impact on companies engaged in developing and manufacturing high-technology commodities. As discussed above, the Rule imposes stringent regulatory requirements affecting a company’s ability to transfer technology, software and technical data to its foreign national employees. BIS’ increasing focus on enforcement does not suggest that companies will encounter more difficulty in hiring foreign nationals – indeed, BIS denied only three deemed export license applications last year. However, it does indicate that companies that ignore or otherwise fail to comply with the Rule’s requirements can and likely will face serious liabilities, including criminal prosecution. Accordingly, affected companies should carefully evaluate their compliance with current export licensing requirements and take appropriate steps to comply fully with any obligations they have under the EAR.

Kathleen M. Paralusz is an associate in the Export/Import Group at Kirkpatrick & Lockhart, L.L.P., where she counsels clients on compliance with U.S. export controls, including the Export Administration Regulations. The above article is meant to inform companies about the impact of the Deemed Export Rule and does not constitute legal advice. Individuals seeking further information on the Deemed Export Rule or other export matters should consult with their company’s legal counsel and personnel responsible for export compliance prior to addressing any export concerns.