PUBLICATION

State Department to Allow Foreign Employees Working with Defense Technologies Easier Access

August 09, 2011

American and foreign defense contractors that have dual national and foreign national employees involved in design and testing of military technologies will need fewer export licenses beginning on August 15, but they will need to update their compliance programs to focus on self-policing. Many companies that employ foreign-born engineers and other technical personnel who have access to software and hardware that is specially designed for military use will have to devise new procedures for screening their own employees, instead of dealing with the government on a case-by-case basis.

Technologies that are specially designed for military and space uses, which are called defense articles and include technical data, software, firmware, parts, and accessories, are subject to the strictest controls on exportation from the United States. These controls are in the International Traffic in Arms Regulations (ITAR), which are administered by the Directorate of Defense Trade Controls (DDTC) of the Department of State. DDTC recently published amendments to ITAR that will go into effect on August 15, 2011, changing the rules that govern access to defense articles, including unclassified technical data. The amendments make new provisions for access by dual nationals and third-country nationals who are regular employees of companies, governments, and organizations that are licensed to use the articles (licensees), under certain conditions, without special permission from DDTC.

What Will Be Required to Comply?

When the ITAR amendments go into effect, licensees will be able to make intracompany, intra-organization, and intragovernment transfers to third-country nationals and dual nationals, as long as they have effective procedures in place to prevent diversion of licensed articles to unauthorized destinations, entities, or purposes. Transfers permitted by the amendments are subject to the limitation that the licensed user must conduct them in the country where it is located or conducts its business. *Effective procedures* consist of requiring that thirdcountry nationals and dual nationals have security clearances issued by the countries where the licensed uses occur or performing internal screening processes and requiring that employees have executed appropriate nondisclosure agreements.

An internal screening process would have to include screening for *substantive* contacts with certain prohibited countries. Substantive contacts include regular travel to such countries, recent or continuing contact with their agents, brokers, or nationals, continued demonstrated allegiance to such countries, maintenance of business relationships with persons from such countries, maintenance of a residence in a prohibited country, receiving a salary or other continuing compensation from such countries, and other acts indicating a risk of diversion.

Licensed companies that comply with certain requirements do not have to go through the usual procedures to retransfer defense articles to dual nationals and third-country nationals, provided that such individuals are nationals only of NATO or EU countries or Australia, New Zealand, Japan, or Switzerland. It is not enough, however, for foreign companies to comply with their own governments' defense export controls regimes; even local regulation compliant foreign companies need to review and revise their procedures to comply with ITAR as amended.

Whom Do the Amendments Help?

These amendments should help companies comply with ITAR and should help defense contractors utilize technical personnel without having to set-up firewalls. The amendments broaden the definition of *regular employee* to enable contractors to benefit from the exemption when they have long-term relationships with the licensees, work on the licensees' premises, and are directly responsible to the licensees. The regulations also help companies that have third-country and dual nationals on their own payrolls working with ITAR-controlled articles.

How Will This Affect the Technology Industry?

Some of the most commonly exported defense articles are software applications and raw algorithms for encryption, control of physical defense articles, and other military uses, as well as designs, components, and accessories for military electronics and computerized hardware. Businesses that deal in these exports will have to adopt effective procedures for screening their dual national and third-state national employees to prevent diversion, as defined by the amendments.

Companies that use defense articles in countries with strict privacy and anti-discrimination laws that protect information about employees' nationalities have had to choose between asking their employees illegal questions or illegally discriminating on the basis of nationality in the assignment of work and violating U.S. export controls. Now, to comply with ITAR companies are less likely to have to violate local law. The amendments help to accommodate the mobility of the global workforce and reduce the likelihood that engineers, programmers, and other technical employees will be denied opportunities because they happen to have been born in different countries from those in which they are working.