wiley

ARTICLE

State Department Issues Final Rule on Dual and Third-Country National Employees

May 20, 2011

As part of the ongoing U.S. export control reform effort, on May 16, 2011, the State Department's Directorate of Defense Trade Controls (DDTC) published a final rule in the *Federal Register* easing restrictions under the International Traffic in Arms Regulations (ITAR) on dual and third-country national employees of approved foreign businesses, government entities and international organizations. [1] Effective August 15, 2011, a new exemption (22 C.F.R. § 126.18) eliminates the separate licensing requirement for dual and third-country nationals employed by licensed foreign end-users and consignees. Although the final rule reduces the burden on foreign end-users and consignees in many respects, it also requires that foreign entities benefiting from the new exemption implement comprehensive screening or approval processes for employees, which may require such entities to review and modify their existing compliance programs.

Background

DDTC administers the ITAR, which control exports and reexports of defense articles, technical data and defense services. For purposes of the ITAR, a dual national is a person who is a national, citizen or permanent resident of the country of his or her employer and another country that is not the United States. A third-country national, on the other hand, is a person who is a national, citizen or permanent resident of a country other than the country of his or her employer or the United States.

In general, exports of defense items must be authorized either by a license or under a Technical Assistance Agreement (TAA), Manufacturing License Agreement (MLA) or Warehouse Distribution

Authors

John R. Shane
Partner
202.719.7222
jshane@wiley.law

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

Practice Areas

Export Controls and Economic Sanctions
International Trade

Agreement (WDA). For approval purposes, both the physical location of the foreign licensee and the citizenship or nationality of its employees are important. In this regard, in some cases, an exemption in 22 C.F.R. § 124.16 grants blanket authorization for transfers of technical data and defense services to dual and third-country national employees of an approved foreign end-user, provided that the employees are nationals exclusively of U.S. allies (*i.e.*, countries that are members of NATO or the European Union, Australia, Japan, New Zealand and Switzerland). [2] When this exemption does not apply, however, DDTC has required U.S. companies applying for authorizations to specifically identify the countries of dual national and third-country national employees who may have access to defense articles (including technical data) exported to approved foreign entities.

Recently, DDTC determined that dual and third-country nationals pose little threat to U.S. national security. At the same time, the requirement to gather and identify country of birth, citizenship and permanent resident status information of employees of foreign licensees (particularly DDTC's emphasis on national origin) has caused human rights and privacy concerns and tension with U.S. allies. [3] These factors prompted changes to DDTC's traditional treatment of dual and third-country nationals.

Summary of Final Rule

The key changes to the ITAR and the potential impact of DDTC's final rule are summarized below.

Elimination of the Separate Licensing Requirement for Dual and Third-Country National Employees of a Licensed Foreign End-User or Consignee

The final rule adds an exemption to the ITAR allowing intra-company, intra-government and intra-organization transfers of unclassified defense articles, including technical data, by foreign licensees to their dual and third-country national employees where the exemption in 22 C.F.R. § 124.16 cannot be implemented because of applicable domestic laws. The exemption applies to foreign business entities, foreign governmental entities and international organizations, but does not extend to academic institutions.

Importantly, the dual and third-country nationals must be bona fide "regular employees" directly employed by the foreign consignee or end-user. A regular employee includes an individual permanently and directly employed by the company. In addition, although DDTC declined to permit the application of the exemption to contract employees, it did narrowly broaden the definition of regular employee to also include an individual in a long-term contractual relationship with a company where the individual works full time and exclusively for the company, at the company's facilities, and under the company's direction and control, and executes a Non-Disclosure certification. Further, the staffing agency that has seconded the individual cannot have any role in the work performed by the individual, or any access to ITAR-controlled technology.

Any transfer of defense articles pursuant to the new exemption must take place within the physical territory of the country where the foreign end-user is located, where the governmental entity or international organization conducts official business or where the foreign consignee operates.

Note that the new exemption does not explicitly apply to defense services, creating some ambiguity for U.S. exporters and foreign licensees. Declining to include defense services within the scope of the exemption, DDTC instead stated in the final rule that "defense services are rendered to the named company rather than the individual employees." DDTC went on to note that "if the contemplated defense service involves defense articles already licensed to the company, the proposed exemption would generally cover dual and third-country national employees receiving the defense service." [4] The impact of this exclusion in practice remains to be seen.

New Requirements for Effective Procedures

As a condition for using the new exemption, foreign end-users and consignees must have effective procedures to prevent diversion of defense articles to destinations, entities or for purposes that could threaten U.S. national security interests. The final rule identifies two types of measures that "may satisfy" the requirement for effective procedures: (1) a security clearance approved by the host nation government for its employees; or (2) a comprehensive screening mechanism.

With regard to the latter option, DDTC detailed several steps that must be taken by the foreign licensee, which may require modification to the foreign company's current compliance procedures. These measures include:

- **Non-Disclosure Agreement:** The foreign licensee would execute a Non-Disclosure Agreement providing assurances that its employees will not transfer any defense articles unless specifically authorized by the licensee.
- **Screening for "Substantive Contacts":** The foreign licensee also would be required to screen its employees for "substantive contacts" with restricted or prohibited countries listed in section 126.1 of the ITAR (*e.g.*, Iran, Sudan, China, etc.). DDTC has indicated that substantive contacts can include regular travel to such countries; recent or continuing contact with agents, brokers and nationals of such countries; continued demonstration of allegiance to such countries; maintenance of business relationships with persons from such countries; maintenance of a residence in such countries; and the receipt of a salary or other continuing monetary compensation from such countries. An employee who has substantial contacts with persons from prohibited countries is presumed to raise a risk of diversion.

While DDTC has not provided much in the way of guidance regarding substantive contacts, it did indicate in the final rule that it is not its intent to deny access to defense articles solely due to an employee's relationships or contacts with family members in a context posing no risk of diversion. Contacts with government officials and agents of governments of prohibited countries, on the other hand, would require heightened scrutiny, even if the officials or agents are family members of the employee. Similarly, DDTC indicated that the new rule is not intended to automatically disqualify employees who travel to prohibited destinations where such travel does not involve contacts with foreign agents or proxies likely to lead to diversion of ITAR-controlled items.

- **Technology/Security Clearance Plan:** Foreign licensees would be required to maintain a technology/security clearance plan that includes procedures for screening dual and third-country national employees.

- **Recordkeeping Requirements:** Finally, the foreign licensee must maintain records related to its plan and screening activities for five years that will be available to DDTC upon its request.

Thus, although the new rule alleviates some administrative burdens for foreign licensees, in the absence of a security clearance, it also requires foreign entities to create and implement compliance procedures and engage in detailed investigations of employees' contacts with prohibited countries. Such foreign licensees will be required to make determinations as to the risk of diversion and the ultimate applicability of the new exemption based on DDTC's less-than-clear "substantial contacts" test.

---

[1] *International Traffic in Arms Regulations: Dual Nationals and Third-Country Nationals Employed by End-Users*, 76 Fed. Reg. 28,174 (Dep't State May 16, 2011) (final rule).

[2] 22 C.F.R. § 124.16. The final rule retained this exemption, adding a new definition of "regular employee" to the current language of the exemption.

[3] *Amendment to the International Traffic in Arms Regulations: Dual Nationals and Third-Country Nationals Employed by End-Users*, 75 Fed. Reg. 48,625 (Dep't State Aug. 11, 2010) (proposed rule).

[4] While DDTC indicated in the final rule that defense services are not "transferred" within a company in the same manner in which defense articles can be transferred, the exemption in 22 C.F.R. § 124.16 for dual and third-country nationals of countries of close U.S. allies specifically applies to access to defense articles and retransfers of technical data and defense services. *See* 22 C.F.R. § 124.16.