STATE DEPARTMENT PROPOSES TO REFORM ITAR RULES ON THIRD-COUNTRY NATIONALS

For years, State Department approval has been required for a foreign firm to allow access to defense articles controlled under the International Traffic in Arms Regulations ("ITAR") by employees who are dual-nationals or third-country-nationals, even when the firm holds the articles under an approved license or agreement. Further, the privilege has extended only to nationals of the European Union, NATO countries, Australia, New Zealand, Japan, and Switzerland. Understandably, the requirement (found in ITAR section 124.16) has caused difficulties for companies with multinational workforces. Recently, the President's Task Force on Export Control Reform concluded that the regulation "poses a tremendous administrative burden" on end users, has human rights implications, and has unnecessarily strained international relations—all without a corresponding benefit to national security. The finding was underscored by law enforcement and intelligence data showing that most unauthorized disclosures do not occur within the scope of approved licenses to foreign end users.

In light of these findings, the Department of State is now proposing to amend the ITAR to eliminate the requirement for additional approvals for transfers by end users to dual and third-country national employees. The amended rule would place the affirmative responsibility for ITAR compliance on the end user—including the duty to prevent improper disclosure or retransfer of ITAR-controlled items—while preserving the exporter's duty of due diligence. The proposed rule may be found in the Federal Register at 75 Fed. Reg. 48,625 (Daily Ed. August 11, 2010), *available at* http://edocket.access.gpo.gov/2010/2010-19833.htm.

The proposed rule would eliminate ITAR section 124.16 and add ITAR section 126.18, which would establish new rules for intracompany transfers of ITAR-controlled items. In particular, the proposed ITAR section 126.18 would make clear that

> . . . no approval is needed from the Directorate of Defense Trade Controls (DDTC) for the transfer of defense articles, including technical data, within a foreign business entity, foreign governmental entity, or international organization that is an approved end-user or consignee for those defense articles (including technical data), including the transfer to dual nationals or third country nationals *who are bona fide, regular employees, directly employed by the foreign business entity, foreign governmental entity, or international organization*.

Id. (emphasis supplied). The proposed rule would require that the transfer occur within the physical territories of the end-user's country, and that it be within the scope of an approved export license, other export authorization, or license exemption.

Under the proposed rule, a foreign person wanting to receive any ITAR-controlled defense article (including technical data) must first implement "effective procedures to prevent diversions" to unauthorized destinations. As with any ITAR violation, unauthorized transfers would subject the end user to potential criminal and civil sanctions, including debarment.

The proposed regulation sets out two means by which a foreign end-user may satisfy its obligations (although the proposed regulation states that the foreign end user "can" satisfy the rule's requirements by selecting one of the two means, presumably other means might also satisfy the requirements). Specifically, the foreign end-user could 1) require a security clearance approved by the host-nation government for its employees, or 2) institute a screening process for employees and require execution of a non-disclosure agreement to bar further dissemination of ITAR-controlled items. In addition to selecting either of these two options, however, the foreign end user *must also screen its employees for substantive contacts with prohibited countries* (such as recent or regular travel, recent or continuing contact, continued allegiance and "acts otherwise indicating a risk of diversion"), and it must maintain a technology security/clearance plan. Compliance manuals and screening records must be made available to the U.S. State Department on request.

Key to the State Department proposal is the following provision, which departs from past guidance and makes clear that actions, *not nationality*, will be the determining factor in assessing risk:

> Though nationality does not, in and of itself, prohibit access to defense articles or defense services, an employee that has substantive contacts from persons from countries listed in §126.1(a) [i.e., prohibited countries] shall be presumed to raise a risk of diversion, unless DDTC determines otherwise.

The proposed amendment follows Defense Secretary Gates' announcement that the Obama Administration will take a risk-based approach to export compliance and abandon rules that have little or no demonstrable benefit to the national security. While reducing administrative burdens, however, it would put the onus on end users to establish and maintain aggressive compliance programs. Since most companies working with defense articles already have such programs in place, the tradeoff may well be worth it. The Department of State is accepting comments on the proposed rule until September 10, 2010.

Kaye Scholer's National Security Practice Group advises U.S. and foreign clients on foreign acquisitions in the U.S. defense and national security sector, as well as all matters concerning export compliance. To learn more about this proposed rule or U.S. export-control regulations and processes, please contact any member of the National Security Group.

Farhad Jalinous
+1 202 682 3581
farhad.jalinous@kayescholer.com

Ronald K. Henry
+1 202 682 3590
ronald.henry@kayescholer.com

Karalyn Meany
+1 202 682 3547
karalyn.meany@kayescholer.com

Keith Schomig
+1 202 682 3522
keith.schomig@kayescholer.com

Norman Pashoian
+1 202 682 3562
norman.pashoian@kayescholer.com