Government Contracts & International Trade Blog
The Latest Updates on Developments Affecting Government Contracts
Presented By SheppardMullin

Government Contracts, Investigations & International Trade Blog

June 16, 2011 by Sheppard Mullin

New ITAR Rule on Transfer of Defense Articles to Dual and Third-Country Nationals Creates Substantial New Compliance Obligations

By John M. Hynes

On May 16, 2011, the Department of State ("Department") published its final rule in the Federal Register amending provisions of the International Traffic in Arms Regulations ("ITAR") regarding the transfer of ITAR controlled defense articles (including technical data) to dual and third-country nationals employed by approved foreign end-users. *See* 76 Fed. Reg. 28174-78 (amending 22 C.F.R. pts. 120, 124 and 126).

Provided that certain screening and record-keeping requirements are met, the new rule eliminates the need to secure prior approval from the Directorate of Defense Trade Controls ("DDTC") before transferring unclassified defense articles (including technical data) to dual or third-country nationals who are employees of foreign end-users or consignees (including approved sub-licensees) approved for such defense articles. The new rule goes into effect August 15, 2011.

Background and the Current Rule

The new rule affects the transfer of defense articles (including technical data) to certain dual and third-country national employees. A dual national employee is one who is a national of the country of his employer and also of another country outside the United States. A third-country national employee is one who is a national of neither the United States nor the country of his or her employer.

The ITAR's "deemed export" rule treats a transfer of defense articles to a national of a foreign country as an export to that country itself. Thus, under the current rule, U.S. companies seeking to export defense articles (including technical data) pursuant to a DDTC approval (such as a manufacturing license agreement ("MLA") or technical assistance agreement ("TAA")) must obtain additional approval or invoke an exemption to allow dual or third-country national employees of the foreign business partner to access such defense articles. Moreover, the current rule unequivocally bars such transfers to nationals of restricted or prohibited countries

listed in ITAR part 126.1 (*i.e.*, Belarus, Cuba, Eritrea, Iran, North Korea, Syria, Venezuela, Burma, China, Liberia and Sudan).

To comply with the current rule, approved foreign end-users are required to gather nationality and country of birth information for all employees who would have access to defense articles under the agreement, and report that information to the U.S. company. The U.S. company is then required to submit these data to the DDTC for approval and list the nationalities of such employees on the MLA or TAA.

One current exemption to this requirement permits the DDTC to approve access of unclassified defense articles to dual or third-country national employees or approved sub-licensees of the foreign business partner who are exclusively nationals of NATO countries, European Union countries, Australia, Japan, New Zealand or Switzerland.

Criticisms of the Current Rule

The current rule has been widely criticized as imposing too heavy of an administrative burden on companies and creating inconsistent obligations on foreign business partners. The rule has forced U.S. companies and their foreign business partners to perform substantial due diligence regarding the nationalities of employees working on programs involving defense articles. The rule also requires companies to list such nationalities on the MLA or TAA, amend the MLA or TAA if a dual or third-country national employee is added to the program and screen off dual or third-country national employees who have not been approved by the DDTC.

Importantly, the current rule also has forced foreign business partners to risk violations of labor and other human rights laws of foreign countries. The rule's focus on nationality as a determinative factor in whether an employee can access defense articles creates competing obligations for companies in countries whose discrimination and human rights laws prohibit companies from inquiring about their employees' national origin. By way of example, Canada's human rights laws prohibit discrimination on the basis of national origin; thus, Canadian companies run into a direct conflict in trying to comply with both the ITAR rule described above and Canada's human rights laws.

The New Rule

The Department adopted a new rule to address the concerns with the existing rule described above. To that end, the Department has added a new exemption to the general rule prohibiting transfers of defense articles to dual and third-country national employees, and amended an existing exemption to that general rule.

Definition of "Regular Employee"

As a preliminary matter, the new exemption, as well as the amended existing exemption (both explained below), both include the term "regular employees." To add clarification to the new exemption and amended exemption, the new rule adds part 120.39 to the ITAR to define "regular employee" as not only a permanent employee of the company, but also an individual in a long-term contractual relationship with the company who (1) works full time at the company's facilities under the company's direction and control and (2) executes non-disclosure certifications for the company.

New Exemption Regarding Transfers of Defense Articles to Dual and Third-Country National Employees of Approved End-Users

The new rule is intended to create a policy for transfers of defense articles by approved end-users to dual and third-country nationals employed by such end-users, while at the same time ensuring that adequate safeguards are in place to prevent unauthorized transfers. To that end, the new rule seeks to replace the current restrictions based on nationality with restrictions based on concrete risk factors to mitigate the likelihood of unauthorized transfers.

The new rule adds part 126.18 to the ITAR to create a new exemption regarding "intra-company, intra-organization, and intra-governmental transfers to employees who are dual nationals or third-country nationals." This new exemption does not apply to transfers of defense articles by academic institutions to their dual and third-country national employees. Under this new exemption, transfer of "unclassified defense articles" (including technical data) to "bona fide regular employees, directly employed by the foreign consignee or end-user" does not require additional DDTC approval provided that two requirements are met: (1) the transfer takes place completely within the physical territory of the country where the end-user is located and (2) the end-user has effective procedures in place to prevent diversions to unauthorized destinations.

While the first requirement is relatively straightforward, complying with the second requirement is not as simple as it may appear. Under the new rule, compliance with the second requirement can be achieved by (1) requiring the employees to have a security clearance approved by the host nation government or (2) requiring the end-user to have in place a process to screen its employees and to have executed a non-disclosure agreement providing assurances that the employee will not transfer any defense articles to unauthorized persons. This screening procedure must check the employees for "substantive contacts" with restricted or prohibited countries listed in ITAR part 126.1 (*i.e.*, Belarus, Cuba, Eritrea, Iran, North Korea, Syria, Venezuela, Burma, China, Liberia and Sudan). Such "substantive contacts" include:

1. Regular travel to such countries
2. Recent or continuing contacts with agents, brokers and nationals of such countries.
3. Continued demonstrated allegiance to such countries.
4. Maintenance of business relationships with persons from such countries.
5. Maintenance of a residence in such countries.
6. Receiving salary or other continuing monetary compensation from such countries.
7. Acts otherwise indicating a risk of diversion.

This new exemption also includes a record-keeping requirement. Foreign end-users must maintain a security technology plan that includes procedures for screening employees for substantive contacts, and maintain records of such screening for five years. The plan and screening records must be made available to the DDTC upon request.

The Federal Register report makes clear that this new exemption does not apply to "defense services." Many commenting parties recommended that the exemption extend to defense services, but the Department declined to adopt that recommendation because a defense service cannot be "transferred" within a company in the manner that defense articles can. The Department noted that defense services are rendered to the named company rather than the individual employees and that, in any event, if a defense service involves defense articles already licensed to the foreign end-user, the exemption would cover dual and third-country national employees receiving the defense service. Thus, the Department found it unnecessary to expressly include "defense services" in the exemption.

Amendment to Existing Exemption Regarding Transfers of Defense Articles to Dual and Third-Country National Employees of Approved End-Users

As noted above, the current rule contains an exemption providing that the transfer of unclassified defense articles to dual or third-country national employees or approved sub-licensees of an approved foreign end-user does not require additional DDTC approval provided that the employee or sub-licensee is exclusively a national of a NATO country, an EU country, Australia, Japan, New Zealand or Switzerland. The new rule retains this exemption, but extends it to also include dual or third-country nationals who are "bona fide regular employees" of the approved foreign end-user as the term is defined in the new definition of "regular employee" explained above. As such, under the new rule, this exemption will apply not only to permanent employees of an approved end-user, but also to individuals in a long-term contractual relationship with the end-user who work full time and have executed non-disclosure certifications.

Conclusion and Impact of the New Rule

The new rule is a welcomed shift away from what many perceive as arbitrary restrictions based on national origin, and towards restrictions based on concrete risk factors to mitigate the likelihood of unauthorized transfers. As such, it should be more effective in combating unauthorized transfers of defense articles.

However, while the new rule addresses issues related to conflicts with foreign laws and administrative burden that have plagued the current rule, it may in fact lead to those very same problems. By eliminating nationality as the determinative factor in whether a defense article may be transferred to a dual or third-country national employee, the new exemption addresses the concerns of many foreign governments that the current rule conflicts with labor and human rights laws of some countries. The extensive employee screening procedures mandated by the new exemption may create similar conflicts with data privacy, labor and other human rights laws around the world.

The new rule also addresses complaints regarding administrative burden by eliminating the restrictions based on nationality. Foreign business partners will no longer be required to collect detailed nationality and country of birth information for their employees. Moreover, U.S. companies will no longer have to include such information in their applications to the Department or update that information as dual or third-country national employees are added to programs.

At the same time, however, the rule creates new administrative burdens on approved foreign end-users and U.S. companies. Unless the end-user's employees have security clearance approved by the host nation's government, the end-user will be permitted to transfer a defense

article to a dual or third-country national employee only if it first conducts extensive due diligence to determine the level of risk that an unauthorized transfer might result. Such due diligence must be guided by the ambiguous “substantive contacts” factors laid out in the rule, which will doubtlessly require extensive background checks and interviewing. Such foreign end-users will also be required to maintain a security clearance plan and employee screening records, and make them available to the DDTC upon request.

U.S. companies will also face new administrative burdens. U.S. companies will remain ultimately liable for unauthorized transfers of technical data by their foreign business partners under MLAs and TAAs. As such, U.S. companies should ensure that their foreign business partners understand the new rule and even assist them in their compliance efforts. U.S. companies should also undertake extensive due diligence to ensure that their foreign business partners have implemented the employee screening procedures required by new rule and are in compliance with all other provisions of the rule. Moreover, U.S. companies should consider insisting on broad contractual language reflecting the foreign business partner's commitment to compliance with the new rule and the foreign business partner's liability for non-compliance.

In the end, the new rule correctly moves away from restrictions based solely on nationality. However, while the new rule on its face appears to alleviate the concerns raised by the current rule related to conflicts with foreign laws and administrative burden, the new rule itself may lead to the very same complaints.

Authored by:

John M. Hynes
(213) 617-5430
jhynes@sheppardmullin.com