LATHAM & WATKINS

Number 1195 May 27, 2011

Client Alert

Latham & Watkins
Litigation Department

New Export Control Rules on Dual and Third-Country Nationality Not Likely to Ease ITAR Compliance Burdens on Non-US Entities

On May 16, 2011, as part of the Obama Administration's ongoing export controls reform initiative, the Department of State's Directorate of Defense Trade Controls (DDTC) published a final rule amending the International Traffic in Arms Regulations (ITAR) to reflect a new policy towards dual nationals and third-country nationals employed by approved foreign end-users.

The new rule, which will take effect on August 15, 2011, creates an exemption for intra-company transfers of ITAR-controlled defense articles (which includes technical data) by approved end-users and consignees (including authorized sub-licensees) to their dual and third-country national employees, provided that the foreign end-users screen their foreign employees for "significant contacts" with countries subject to US and multilateral arms embargoes, as listed in ITAR Section 126.1. This *Alert* highlights key elements of the new rule and assesses the practical improvements — or lack thereof — of the new rule over the State Department's current framework.

"This *Alert* highlights key elements of the new rule and assesses the practical improvements — or lack thereof — of the new rule over the State Department's current framework."

Shortcomings Under Current Framework

Under the State Department's current ITAR licensing framework, employees of foreign end-users who are "dual or third-country nationals" (DTCNs) are prohibited from participating in ITAR-controlled programs authorized under Technical Assistance Agreements (TAA) or Manufacturing License Agreements (MLA), unless the licensing agreements specifically authorize transfers to *each* nationality of such DTCNs. Because DDTC interprets the term "nationality" to include not only each citizenship held by an individual, but also the individual's country of birth, end-users must currently determine all citizenships and places of birth for employees working on ITAR-controlled programs, even if they are citizens or permanent residents of the end-user's country. This obligation often creates conflicts with local antidiscrimination and privacy laws that prohibit companies from making employment decisions based on one's national origin, or from collecting, storing or sharing personal information for employees.

Further, because the State Department is precluded from authorizing exports to the proscribed countries listed in ITAR Section 126.1, in most circumstances, employees who are DTCNs of so-called ITAR 126.1 countries could not receive State Department authorization to work on ITAR-controlled programs.

For example, a French citizen born in Côte d'Ivoire prior to that country's independence from France may be entitled under French law to work on defense programs, but would be precluded under the ITAR from working on ITAR-controlled programs due to the employee's birth in a country listed in ITAR Section 126.1. Similarly, a Chinese-born Canadian permanent resident or citizen would be precluded from working on programs involving access to ITAR-controlled technical data or hardware by virtue of his or her country of birth.

Non-US end-users have thus been caught in a legal "Catch-22," forcing them, in some circumstances, to choose between compliance with the ITAR versus domestic civil and criminal human rights or privacy laws. Not surprisingly, DDTC's approach has led to considerable compliance difficulties and friction between the United States and some of its closest trading partners.

New Approach Moves Away From Nationality-Based Licensing

At a January 2011 conference regarding the proposed rule, DDTC's Office of Defense Trade Control Policy acknowledged that nationality is not a valid indicator of loyalty or trustworthiness. Consistent with that recognition, the State Department's new rule moves away from using nationality or place of birth as criteria for establishing the risk of diversion to prohibited countries, in favor of individualized screening for such diversion risk.

In proposing the new rule in August 2010, DDTC acknowledged that most diversions of items subject to the ITAR do not occur within foreign companies or organizations providing access to "properly screened" DTCN employees, but rather occur outside the scope of approved licenses. Therefore, under the new exemption for intra-company transfers to DTCN employees and contract workers, a foreign end-user may transfer defense articles (including technical data) to any of its employees or long-term contract employees, regardless of nationality/ies, provided the employees either have been properly screened for diversion risk, or have received a security clearance from the host company. The new rule expressly authorizes transfers to DTCNs of countries proscribed under ITAR Section 126.1, provided the employees have been screened or cleared under one of these two methods.

The new exemption, implemented by the newly-created ITAR Section 124.18, shifts the compliance burden to the end-user to perform satisfactory screening of its employees and long-term contract workers for diversion risk, which is defined as "substantive contacts" with proscribed countries. The rule allows those end-users a degree of discretion in determining if an employee has connections with ITAR Section 126.1 countries that rise to the level of "substantive contacts," and provides the following that would be presumed to constitute a risk of diversion:

- Regular travel to ITAR Section 126.1 countries
- Recent or continuing contact with agents, brokers, and nationals of ITAR Section 126.1 countries
- Continued demonstrated allegiance to ITAR Section 126.1 countries
- Maintenance of business relationships with persons from ITAR Section 126.1 countries
- Maintenance of a residence in ITAR Section 126.1 countries
- Receiving salary or other continuing monetary compensation from ITAR Section 126.1 countries
- Acts otherwise indicating a risk of diversion

In addition to screening, the end-user would need to implement a technology

security/clearance plan, maintain records of screenings for five years, and require all relevant employees to execute a non-disclosure agreement.

The new rule provides end-users an additional avenue for sharing ITAR-controlled data with DTCN employees. This is in addition to the existing exemption under ITAR Section 124.16, which allows end-users in NATO or European Union countries, Australia, Japan, New Zealand, or Switzerland to transfer ITAR-controlled technical data to employees who are DTCNs of such countries (DTCNs of such countries who were also nationals of ITAR Section 126.1 countries were ineligible to receive ITAR-controlled goods or technical data under that exemption). In August 2010, DDTC proposed eliminating the ITAR Section 124.16 exemption in favor of the new rule. In publishing the final rule, DDTC adopted the recommendation from industry to retain the existing Section 124.16 exemption. The State Department also adopted recommendations to expand coverage of the exemptions to long-term contract employees of the foreign end-users, in addition to *bona fide* employees.

Under the new rule, foreign end-users under a TAA or MLA that have DTCN employees or long-term contract workers thus will have four options for sharing ITAR-controlled items or technology with such individuals: (1) pursuant to specific authorization in a TAA or MLA for all the countries of nationality; (2) under the ITAR Section 124.16 exemption for DTCNs from NATO or European Union countries, Australia, Japan, New Zealand, or Switzerland; (3) obtaining a government security clearance for the individuals; or (4) screening the individuals for substantive contacts with ITAR Section 126.1 countries. DTCNs of ITAR Section 126.1 countries are ineligible to receive access to ITAR-controlled articles or technical data under the first two avenues, but will now be eligible to obtain authorization to work on ITAR-controlled programs under the latter two exemption vehicles.

Questionable Utility of the New Exemption

A significant criticism of the current framework is that it requires end-users to make determinations regarding their employees' citizenships and national origins that are prohibited or are irrelevant under local law. The new approach purportedly takes a nationality neutral approach, by framing eligibility for the exemption solely on the presence of substantive contacts with proscribed countries. An end-user could, in theory, perform screening of all its employees considered for participation in ITAR-controlled programs and eliminate concerns that the rule discriminated against DTCNs. Indeed, by proposing to eliminate the ITAR Section 124.16 exemption, it is likely DDTC sought to push foreign end-users to require the individualized screening contemplated under the new exemption to *all* employees, regardless of nationality.

While the rule represents a theoretical improvement over the *status quo*, in practice, the new rule will require end-users to make detailed, subjective, and intrusive inquiries of employees and contract workers regarding their personal lives, and judge the nature and significance of any contacts identified by those answers. Private companies will likely not possess the resources to validate the answers they receive (for example, some European countries grant their citizens a "right to lie" about certain information deemed to be beyond the scope of what an employer can legally request), and it is unclear whether local laws will permit the nature of inquiries mandated under the new rule, particularly since the screening will not be required by the host country's security laws (with at least one exception, discussed below). Further, DDTC has not yet issued any guidance regarding what an adequate technology security plan would look like, or what kind of screening program would meet State Department muster. Practical and effective implementation of the new rule is thus the major question mark for industry.

"While the new Section 126.18 exemption could reduce the complexities of licensing for US manufacturers and exporters by eliminating the need constantly to update their TAAs and MLAs, foreign end-users may decide that implementing an effective proscribed country screening program is even more burdensome than complying with the requirements under the former regulations and opt not to take advantage of the intra-company exemption."

While the new Section 126.18 exemption could reduce the complexities of licensing for US manufacturers and exporters by eliminating the need constantly to update their TAAs and MLAs, foreign end-users may decide that implementing an effective proscribed country screening program is even more burdensome than complying with the requirements under the former regulations and opt not to take advantage of the intra-company exemption.

Can Companies Look to Canada for Guidance?

The Canadian government has been critical of the current nationality-based approach, which conflicts with Canadian federal and provincial human rights guarantees and has led to costly litigation for some Canadian defense contractors. Since DDTC proposed the new exemption in August 2010, the Canadian Government has been working with the US State Department and key Canadian stakeholders to ensure that Canada's Controlled Goods Program would be capable of meeting the requirements of the new rule. Simultaneously, the Canadian Controlled Goods Directorate (CGD) was preparing to implement an Enhanced Security Strategy (ESS) being developed as a result of a 2008-2009 Controlled Goods Program security threat and risk review.

Even prior to publication of DDTC's final rule, the Canadian CGD announced that, as part of the forthcoming ESS, it was developing a risk matrix to identify individuals who pose a risk of unauthorized transfer of controlled goods. Persons exceeding the risk threshold will be subjected to a broader security assessment in conjunction with Canadian federal governmental agencies, such as the Department of Foreign Affairs and International Trade, the Canadian Security Intelligence Services, and the Department of National Defence, among others. The Canadian CGD has reportedly even begun discussions with DDTC on assessing persons that exceed the risk threshold. The factors to be considered in the risk matrix are similar to the factors for determining if "substantive contacts" with a proscribed country exists under the new ITAR exemption, *e.g.*, contacts with government officials, agents, or proxies; business and/or family contacts; continuing allegiance to a foreign country; relationship with a foreign country government (*e.g.*, employment); frequent travel; residence and/or bank accounts in a foreign country or affiliations within or outside of Canada.

One of the professed goals of the Canadian ESS is to ensure uniform application of the program across all Controlled Goods Program stakeholders. In furtherance of this goal, the Canadian CGD announced on May 17, 2011 (*i.e*, immediately following and likely in response to publication of the new ITAR exemption) that it was developing a set of standards and procedures to be followed when assessing security for anyone examining, possessing or transferring controlled goods. The announcement explicitly noted the augmented security assessment standards would meet the standards outlined in the new ITAR Section 126.18, including concerns regarding foreign "substantive contacts." The CGD indicates that it will be issuing notices regarding the parameters of its ESS in the coming weeks, as well as its corresponding implementation plan. It is expected that the plan will include a questionnaire to identify substantive contacts, as an implementation of the ESS risk matrix.

Given the coordination and close cooperation between the State Department and the Canadian government in developing the new intra-company transfer exemption, the Canadian ESS implementation plan and risk matrix questionnaire may provide

useful guidance for implementing the technology security plan and diversion screening required by the State Department's new rule. In the absence of clearer guidance from DDTC, the CGD guidance could become a *de facto* template for developing sufficient screening programs, well beyond Canadian shores.

If you have any questions about this *Client Alert*, please contact one of the authors listed below or the Latham attorney with whom you normally consult:

William M. McGlone
+1.202.637.2202
william.mcglone@lw.com
Washington, D.C.

Les P. Carnegie
+1.202.637.1096
les.carnegie@lw.com
Washington, D.C.

Kevin P. DiBartolo
+1.202.637.2290
kevin.dibartolo@lw.com
Washington, D.C.

Jessica K. Thibodeau
+1.202.637.1071
jessica.thibodeau@lw.com
Washington, D.C.