Final US ITAR Rule on Dual and Third Country Nationals Raises New Challenges for Canadian Business

Today, the U.S. State Department's Directorate of Defense Trade Controls (DDTC) published in the Federal Register the final rule containing its long-awaited amendments to the *International Traffic in Arms Regulations* (ITAR) governing the access of dual and third-country nationals to ITAR-controlled defence articles, including technical data – see [http://www.gpo.gov/fdsys/pkg/FR-2011-05-16/pdf/2011-11697.pdf]. These, together with ongoing changes to Canada's Controlled Goods Program (CGP) generally covering similar goods and technology, are anticipated to have a significant effect on Canadian companies in the aerospace, defence and satellite sectors, and in particular on their security, compliance and screening processes.

Up to now, Canadian firms have faced numerous difficulties with ITAR rules that prohibit employees of certain nationalities or born in certain proscribed countries from accessing US-controlled defence goods and technology in Canada. In order to comply with these restrictions, Canadian companies have had to risk violating provincial and federal anti-discrimination laws, as well as exposure to human rights complaints, when denying employees access to projects involving ITAR-controlled items because of their nationality or country of birth. Companies in affected sectors have had to address, defend and settle costly, and in some cases very public, anti-discrimination claims arising from ITAR compliance.

DDTC officials have stated that the final rule is intended to move away from nationality-based screening and avoid the human rights conflicts that have plagued trade partners in Canada and other countries.

These proposed changes were first released on a preliminary basis for comment by DDTC in August of 2010. Our legal update discussing the preliminary rule can be found at *Proposed US Defence Control Changes Aim to Resolve Conflicts with Canadian Human Rights Law*. The final rule retains the essence of what was initially proposed, with some minor changes to the text and some other more significant revisions referred to below.

ITAR Defence Articles May Now be Transferred to 3rd Country or Dual National Employees

Under new ITAR section 126.18, DDTC approval will not be required for the transfer of defence articles, including technical data, to a foreign business entity, foreign government entity, or international organization that is an approved end-user or consignee for those items, "including the transfer to dual nationals or third-country nationals who are bona fide regular employees, directly employed by the foreign consignee or end-user." This exemption will apply provided the transfer takes place completely within the territories where the end-user is located or where the consignee operates, and must be within the scope of an approved export licence, other export authorization, or licence exemption.

Key Condition – Effective Procedures to Prevent Diversion

As a condition of transferring to foreign person employees under this provision, the recipient of the defence article is required to have in place "effective procedures to prevent diversion to destinations, entities, or for purposes other than those authorized by the applicable export licence or other authorization in order to comply with the US *Arms Export Control Act* and the ITAR."

In order to be considered to have such effective procedures, Canadian firms that are consignees or end-users of the defence articles must either (i) require a security clearance approved by the Canadian government for its employees or (ii) implement a screening process for their employees and execute Non-Disclosure Agreements that provide assurances that employees will not transfer any information to persons or entities unless specifically authorized by the employer.

Under the new rule, Canadian firms will be required to screen **all** employees who are to access controlled items for "substantive contacts" with the 25 restricted or prohibited countries under the ITAR – including China, Vietnam, Haiti, Venezuela and other countries subject to US military sanctions. The final rule has expanded upon what is meant by substantive contacts - these now include:

(i) regular travel to those countries;

(ii) recent or continuing contact with agents, brokers and nationals of those countries;

(iii) continued demonstrated allegiance to those countries;

(iv) maintenance of business relationships with persons from those countries;

(v) maintenance of a residence in those countries;

(vi) receiving salary or other continuing monetary compensation from those countries; or

(vii) acts otherwise indicating a risk of diversion.

The amendments provide that, although an employee's nationality is not in and of itself a determinative factor prohibiting access to defence articles, if an employee is determined to have substantive contacts with persons from the ITAR-restricted or prohibited countries, this is presumed to raise a risk of diversion "unless DDTC determines otherwise".

Companies are also required to maintain a technology security/clearance plan that includes procedures for screening employees' substantive contacts and maintaining records of the same for five years. The technology security/clearance plan and screening records are to be made available to DDTC or its agents for civil or criminal law enforcement upon request.

Other Significant Aspects of the New Rule

The final rule and DDTC's accompanying commentary address a number of additional significant issues for Canadian companies:

1. Perhaps most significant from the Canadian perspective is that, despite requests from parties commenting on the proposed changes, DDTC did not agree to an explicit exemption for companies that comply with other countries' domestic industrial security programs that provide for effective screening and other security measures for the protection of these controlled items. This means that Canadian companies that are registered and comply with Canada's Controlled Goods Program (which applies to essentially the same items) must still review and revise existing security measures to ensure compliance with this new ITAR rule for all their employees that will access ITAR-controlled goods or technology.

2. A number of commenting parties had expressed concern that contract employees would not be subject to the new rule. Although DDTC resisted applying the rule to all contract employees, they agreed to narrowly extend it to workers who have a long-term employment relationships with licensed end-users. This is reflected in a new definition of "regular employee". In addition to an individual permanently and directly employed by the company, "regular employee" now also includes "an individual in a long term contractual relationship with the company where the individual works at the company's facilities, works under the company's direction and control, works full time and exclusively for the company, and executes nondisclosure certifications for the company, and where the staffing agency that as seconded the individual has no role in the work the individual performs (other than providing that individual for that work) and the staffing agency would not have access to any controlled technology (other than where specifically authorized by a license)".

3. Many Canadian companies currently benefit from ITAR section 124.16 special retransfer authorizations. They permit retransfers of defence articles and technical data to employees of foreign (including Canadian) entities who are nationals exclusively of NATO or EU countries or Australia, Japan, New Zealand or Switzerland. DDTC initially proposed to eliminate 124.16 with the implementation of the new rule. In its final rule, however, DDTC reconsidered its position and noted a major concern expressed by commenting parties was that the proposed dual national rule did not include transfer to approved sub-licencees (which are included under section 124.16). Under the new amendments, section 124.16 is now retained and its definition of "regular employee" has been amended to include workers who have long-term employment relationships with end-users as discussed above.

4. Academic institutions in Canada have encountered particular challenges with compliance issues arising in the context of ITAR-controlled goods and technology. Any uncertainty regarding the application of the new rule to Canadian universities was put to rest by DDTC when it noted in its commentary that it is not prepared to extend the exemption to academic institutions at this time.

Interaction with Canada's Controlled Goods Programs

Despite DDTC's refusal to allow an explicit exemption for CGP-registrants at this time, Canada is developing measures to accommodate these new ITAR requirements in an attempt to facilitate compliance for Canadian companies. Following a security threat and risk review, Canada's Controlled Goods Directorate at Public Works and Government Services (CGD) recently implemented its Enhanced Security Strategy which includes the development of a risk matrix for identifying individuals at risk of unauthorized transfer of controlled goods.

New Questionnaire Developed for Canadian Companies

CGD has indicated that a screening questionnaire is being developed and will be provided to Canadian companies to assist them to identify risks during the security assessment of their employees under the CGP. Factors to be considered in such an assessment are not unlike those in the "substantive contact" analysis under the new ITAR rule and include the following:

(i) contacts with government officials, agents or proxies;

(ii) business and/or family contacts;

(iii) continuing allegiance to a foreign country;

(iv) relationship with a foreign country government (e.g., employment);

(v) frequent travel;

(vi) residence and/or bank accounts in a foreign country; and

(vii) affiliations within or outside Canada.

CGD has also indicated that the nature and substance of these contacts will be used to determine if an individual should be subject to broader security assessment or denied registration. Where the risk threshold is exceeded, CGD, working with a number of other government departments, will undertake a risk assessment of the individual to determine whether or not access should be granted.

Additional Measures Under the Enhanced Security Strategy

Also included in CGD's Enhanced Security Strategy are measures to tighten security requirements for Canadian registrants under the CGP in a number of areas, including: students, interns and collectors; broader security assessments of foreign temporary workers and visitors; broader security assessments of transportation companies (together with Transport Canada); additional requirements for a company's security plan, especially relating to cyber-security risks; more in-depth inspection processes; and the development of a list of debarred individuals and companies.

Next Steps

The new ITAR rule becomes effective August 15, 2011. This, along with Canada's new CGP requirements, will require Canadian companies to implement enhanced security measures, including screening of all employees requiring access to controlled items. What this exactly entails will have to be determined on a case-by-case basis for each particular employer. It is expected that there will be challenges for Canadian companies undertaking these measures to ensure their procedures satisfy the diligence required by ITAR but at the same time do not expose them to risk of non-compliance with human rights and privacy laws in Canada.

It will be important for Canadian companies in the military, aerospace and satellite sectors that access controlled goods and technology to work closely with their US and Canadian counsel to ensure compliance with the applicable defence control regimes in both countries as well as the requirements for employment, privacy and human rights laws.

McCarthy Tétrault's International Trade and Investment Law Group has extensive experience in dealing with defence trade control measures and is available to advise on related enforcement, compliance and strategic planning issues.