AKIN GUMP
STRAUSS HAUER & FELD LLP

International Trade Alert

New ITAR Exemption for Dual and Third Country National Employees at Non-U.S. Companies Also Creates Extraordinary New Compliance Requirements

May 16, 2011

On May 16, 2011, the U.S. Department of State issued a final rule (available here) that dramatically changes the compliance landscape for companies involved in defense trade with respect to the use of dual and third-country nationals (DTCN) by non-U.S. business partners, including suppliers and customers. Citing the large administrative burden and conflict with "foreign human rights laws," including non-U.S. data privacy and labor laws, State's new rule is intended to eliminate prior requirements that effectively compelled the gathering and managing of information about the nationalities and countries of birth of the employees of non-U.S. business partners in order to ensure compliance under the International Traffic in Arms Regulations (ITAR). However, the new rule also creates certain conditions (and ambiguities) with respect to screening and technology security/clearance plan (TSCP) requirements and imposes corresponding risks and burdens on both the U.S. exporter and non-U.S. licensee. Consequently, companies that export or receive defense articles (including technical data) under the ITAR must now re-examine and restructure their compliance programs to incorporate this new rule, which will be effective on August 15, 2011.

BACKGROUND AND OLD RULES

A dual national employee is one who is a citizen or national of the country of his employer and also a citizen or national of another country – other than the United States. A third-country national employee is one who is a citizen or national of a country that is not the United States or the country of his employer. In recent years, State has required U.S. companies seeking ITAR authorizations, including manufacturing license agreements (MLAs) and technical assistance agreements (TAAs), to identify the nationalities and country of birth for all employees at non-U.S. business partners who may access defense articles, including technical data.

As a result, unless an exemption applied (i.e., the § 124.16 exemption for nationals of NATO/EU countries, Australia, Japan, Switzerland and New Zealand), non-U.S. business partners, including their sub-tier suppliers and services providers, have been required to gather nationality and country of birth information for all employees who would have access to defense articles, including technical data, under an agreement. The U.S. applicant was then required to submit this information to the State Department for approval. The effect of this requirement has not only created a large administrative burden for the U.S. applicants and non-U.S. business partners, but is also in conflict with the data privacy, labor and other "human rights" laws of many countries. Consequently, it has been difficult for many companies to ensure compliance with this ITAR requirement.

© 2011 Akin Gump Strauss Hauer & Feld LLP This document is distributed for informational use only; it does not constitute legal advice and should not be used as such.

NEW RULES

New Section 126.18 Exemption

The most significant change is the introduction of an exemption through a new section in the ITAR, 22 C.F.R. § 126.18. Under this new section, U.S. applicants are no longer required to seek approval from State for authorized end users or consignees, including companies, governmental entities and international organizations, to transfer unclassified defense articles, including technical data, to their DTCN full-time regular employees, so long as "effective procedures" are in place to prevent diversion to unauthorized parties and destinations or for unauthorized purposes. The "effective procedures" requirement may be satisfied by: (i) a security clearance approved by the host nation government for its employees or (ii) the employer screening the employee for "substantive contacts" with restricted countries (i.e., § 126.1 countries), maintaining a TSCP and requiring that the employee sign a nondisclosure agreement (NDA). With respect to this second option, the final rule provides more detail as follows—

- **Screening Requirement**. The screening process should evaluate the employee for substantive contacts with restricted countries under ITAR § 126.1(a). According to the new rule, this evaluation takes into consideration the employee's regular travel destinations, business and personal contacts, residential or commercial interests, financial connections, continued citizenship or allegiance and any other relationship or action indicating a risk of diversion. Employees found to have substantive contacts are presumed to raise a risk of diversion unless DDTC determines otherwise.

- **Technology Security/Clearance Plan**. The rule requires that the non-U.S. business partners maintain a TSCP that includes procedures for screening the employees for substantive contacts with restricted countries. These companies must maintain this record for five years and provide it to the State Department upon request for enforcement purposes.

In addition, any transfer under this exemption must: (i) take place either completely within the territory of the end-user or where the foreign governmental entity/international organization conducts official business or where the consignee operates and (ii) be within the scope of the approved export license or authorization.

Other Changes

- **Definition of Regular Employee**. The ITAR now defines a "regular employee" as either: (i) an individual permanently and directly employed by the non-U.S. entity or (ii) a long-term contract employee who meets certain criteria. The contract employee must work full-time, on-site, exclusively for, and under control of, the non-U.S. employer and also must execute a nondisclosure certificate. The contract employee provider must have no role in the contract employee's work and may not have access to any controlled technology, unless other authorization exists for such access.

- **Clarification of § 124.16**. The language of this provision, which grants special retransfer authorization for unclassified technical data and defense services to countries of NATO/EU, Australia, Japan, New Zealand and Switzerland, was expanded to apply to the newly defined "regular employees."

IMPACT ON MULTINATIONALS ENGAGED IN DEFENSE TRADE

The Good News

Specific nationality information for each DTCN no longer required for unclassified defense articles. Once the new rule takes effect on August 15, non-U.S. companies will no longer be required to undertake the difficult task of compiling—and U.S. companies will no longer have to include in their applications to State—detailed nationality and country of birth information for the non-U.S. entity's employees and those of its sub-tier suppliers and service providers. Rather, U.S. companies can now rely on their foreign suppliers and customers to alert them when specific authorization for an individual is needed. However, the exemption only applies so long as "effective procedures" to prevent diversion are in place. Both the U.S. applicant (who remains liable for compliance of all parties to the

© 2011 Akin Gump Strauss Hauer & Feld LLP This document is distributed for informational use only; it does not constitute legal advice and should not be used as such.

agreement) and the non-U.S. business partner (who must also adhere to contractual commitments to the U.S. party and implement these procedures) will have good reason to give careful consideration to that standard. As discussed more thoroughly below, it is not clear that this shift will actually alleviate the burden on either party.

Process streamlined for governmental entities. This new exemption may have the most positive impact for U.S. applicants in their dealings with governments or ministries of defense. As many U.S. companies are aware, making requests of non-U.S. governments can often prove frustrating and be associated with a delayed response time. Now, under the new exemption, the ITAR will no longer require governmental entities to obtain nationality information from employees as long as they are subject to that government's standard security clearance.

The Not-So-Good News

Increased diligence requirement on non-U.S. business partners. For business partners outside the United States whose employees do not have security clearance, the good news may be limited. These non-U.S. end-users or consignees must now develop and maintain a TSCP containing an "effective procedure" for determining risk of diversion before allowing transfers of U.S. defense articles to DTCN employees. Based on State's guidance on what constitutes "substantial contacts" with restricted countries, this procedure must be robust and involve a series of relatively intrusive questions. Considering that many non-U.S. employers already struggle to implement existing technology control plans, the addition of an ambiguous screening standard will likely create more confusion and work for these companies. Moreover, it remains to be seen how these new requirements may be reconciled with data privacy, labor and other laws in countries around the world.

Lack of clarity. While a chronic source of conflict with laws of other countries, the old rule provided a clear objective standard based on nationality. The new rule, however, is centered around the concept of screening for "substantial contacts" with restricted counties. In practice, it will likely be less clear what constitutes a substantial contact that could raise a "risk of diversion." Unless further information is provided, non-U.S. employers are left to make these difficult judgments, placing them, as well as the U.S. applicant, in a precarious compliance position.

U.S. applicants continue to be responsible for unauthorized transfers under the agreement. Even though many of the responsibilities appear to fall to the foreign business partners, the new exemption makes clear that U.S. companies are still liable for all activities under an agreement. Accordingly, it would be prudent for U.S. companies to ensure their non-U.S. partners understand the conditions of the rules and, where appropriate, assist in the implementation of the TSCP and decisions relating to diversion risks. By the same token, non-U.S. licensees can expect their U.S. business partners to scrutinize their compliance measures and are likely to be subject to broad contractual provisions that reflect the U.S. business partner's potential liability. As a consequence, non-U.S. companies that want to attract or maintain such relationships have a strong incentive to evaluate the practical issues they may face in implementing the new rule and ensure appropriate procedures are in place for managing associated risks.

CONCLUSION

In issuing this rule, State attempted to lessen the burden of compliance with the ITAR on U.S. and non-U.S. parties for exports of unclassified defense articles. While this new exemption removes the onerous task of collecting nationality information, it requires non-U.S. parties to develop a TSCP, implement a screening process based on a relatively ambiguous new standard and maintain this information in the event DDTC requests it. These are not small tasks and will take great cooperation between all parties involved to ensure compliance. It also remains to be seen how this new rule will be reconciled with the various laws of countries around the world.

As of today, State has not yet issued further guidance on its Web site or any changes to the Guidelines for Preparing Electronic Agreements, although these can surely be expected in the near future.

© 2011 Akin Gump Strauss Hauer & Feld LLP This document is distributed for informational use only; it does not constitute legal advice and should not be used as such.

CONTACT INFORMATION

If you have any questions concerning this alert, please contact —

Edward L. Rubinoff
erubinoff@akingump.com
202.887.4026
Washington, D.C.

Thomas James McCarthy
tmccarthy@akingump.com
202.887.4047
Washington, D.C.

Christian C. Davis
chdavis@akingump.com
202.887.4529
Washington, D.C.

Wynn H. Segall
wsegall@akingump.com
202.887.4573
Washington, D.C.

Tamer A. Soliman
tsoliman@akingump.com
(971)2.4068531
Adu Dhabi

Rebekah M. Jones
rjones@akingump.com
202.887.4489
Washington, D.C.

© 2011 Akin Gump Strauss Hauer & Feld LLP This document is distributed for informational use only; it does not constitute legal advice and should not be used as such.