

Sharing Sensitive Technologies Between International Affiliates

March 11, 2015

[This article originally appeared in the November/December 2014 issue of World ECR.]

In the normal course of operations between U.S. and foreign affiliates, inter-company communications and data conveyances are frequent and occur both intentionally and inadvertently. The U.S.-foreign affiliation can be in the form of a parent company, on one end, and a wholly owned subsidiary, joint venture, minority interest or other intercompany affiliation, on the other end.

When sensitive technologies are involved in these inter-company exchanges, U.S. export control laws likely apply to the controlled technology transfer and export control law violations can occur.

U.S. export control laws include U.S. International Traffic in Arms Regulations ('ITAR'), U.S. Export Administration Regulations ('EAR'), and those U.S. executive orders, U.S. statutes, and U.S. treasury regulations comprising the country, person, and entity sanctions that are administered and enforced by the U.S. Office of Foreign Asset Control ('OFAC'). While the ITAR applies predominately (but not exclusively) to companies in the defense and aerospace industries, U.S. export control laws under EAR and OFAC apply to companies in the software, IT, telecommunications, and automotive industries and potentially to any transfer (export) of a sensitive technology from the U.S.

The intention of this article is to explain how U.S. export control issues affect the sharing of technologies between U.S. and foreign affiliates.

How to identify sensitive technology transfers

The first step is to identify whether a technology is a controlled technology, and thus subject to U.S. export laws upon transfer (export) from the U.S. to a foreign affiliate. Under ITAR, a controlled technology is one that is listed as one of the 20 general item categories of the ITAR U.S. Munitions List ('USML'). Specifically, ITAR-controlled technology would appear under paragraphs (g), (h), or (i) of each general item category of the USML. ITAR-controlled technologies are identified as either:

- Technical data, which includes drawings, plans, instructions, documentation for the design, development, production, operation/use, repair, and maintenance of an item listed as a defense article under a USML category; and
- Defense services, which include assistance for design, development, production, operation/use, repair, and maintenance of an item listed as a defense article under a USML category.

Under EAR, a controlled technology is one that is listed as one of the ten general item categories of the EAR Commerce Control List ('CCL'). Within the ten general CCL categories, specifically controlled items are further classified in five groups lettered A through E. Of these five groups, EAR-controlled technologies are identified as either:

- Software – under product group D, whereby the software may correspond to product groups A (equipment, assemblies and components), B (related test, inspection and production equipment), or C (materials) of a given general item category under the CCL; and

Continued

- Technology – under product group E, which includes specific information necessary for the ‘development’, ‘production’, or ‘use’ of a controlled item listed under related product groups A, B, or C; and technology can be furnished in the form of technical data or technical assistance.

The transfer of any of the above ITAR technical data or defense services or EAR software or technology to a foreign affiliate would constitute a ‘controlled technology’ transfer under ITAR or EAR.

Licensed transfers of controlled technology under ITAR and EAR

The following export control compliance rules are useful for lawfully transferring controlled technologies to foreign affiliates. They may be applied to most of the common technology transfer scenarios arising between international affiliates.

A GOOD GENERAL RULE FOR TRANSFERS OF ITAR-CONTROLLED TECHNOLOGY

Absent an available exemption under ITAR, a U.S. export control license or other explicit authorization is required to transfer an ITAR-controlled technology to a foreign affiliate.

ITAR-LICENSED TRANSFERS

For an ITAR-controlled technology constituting technical data, a simple transfer to a foreign affiliate (without technical assistance) is permitted via a DSP-5 license for ‘unclassified’ technical data and a DSP-85 license for ‘classified’ Technical Data.

ITAR-AUTHORIZED TRANSFERS UNDER COLLABORATIVE AGREEMENTS

For ITAR-controlled technology furnished as defence services, such a transfer to a foreign affiliate is permitted via one of the stipulated collaborative service agreements under the ITAR, which are (i) technical assistance agreements (‘TAAs’) for the performance of defence services and disclosure of technical data and (ii) manufacturing license agreements (‘MLAs’) for a grant of a license to a foreign affiliate to enable the foreign affiliate to manufacture an item that is a Defense Article under the USML.

TAA and MLAs between U.S. and foreign affiliates must be approved by the U.S. Directorate of Defense Trade Controls (‘DDTC’), which is the U.S. State Department agency charged with administering and enforcing ITAR export controls. ITAR license exemptions under ITAR sections 124.3(a) and (b) permit the transfer (export) of corresponding ‘Unclassified’ and ‘Classified’ technical data in furtherance of the TAA or MLA.

A GOOD GENERAL RULE FOR TRANSFERS OF EAR-CONTROLLED TECHNOLOGY

A U.S. export control license or (if available) an EAR license exception will be required to transfer (export) an EAR-controlled technology to a foreign affiliate.

Continued

EAR-LICENSED TRANSFERS

For an EAR-controlled technology constituting software or general technology under EAR, a transfer to a foreign affiliate (with or without technical assistance) is permitted via an EAR export license, unless a license is not required for the foreign affiliate's country or an EAR license exception applies.

EAR-AUTHORIZED TRANSFERS UNDER LICENSE EXCEPTIONS

In lieu of obtaining an EAR export control license, U.S. affiliates may be authorized to transfer EAR-controlled technology to a foreign affiliate via an EAR license exception, provided that the transfer qualifies for the license exception and proper reliance upon the exception is documented. While not exhaustive, the following EAR license exceptions are some common exceptions that may be used to facilitate transfer of EAR-controlled technology to a foreign affiliate without an export control license:

EAR LICENSE EXCEPTION TSR (TECHNOLOGY AND SOFTWARE RESTRICTED)

This exception authorizes unlicensed transfers of EAR-Controlled software and technology to a foreign affiliate if: (a) only national security (NS) controls imposed by EAR are present; (b) the destination country is listed in Country Group B of the EAR; and (c) a written assurance on a limited scope of use is obtained from the end-user.

EAR LICENSE EXCEPTION TSU (TECHNOLOGY AND SOFTWARE UNRESTRICTED)

This exception authorizes unlicensed transfers of EAR-Controlled software and technology to a foreign affiliate if the controlled items are comprised of sales and operations software and technology, other mass market software, or encryption source code that is 'publicly available' (e.g., open source) and its corresponding object code.

EAR LICENSE EXCEPTION STA (STRATEGIC TRADE AUTHORISATION)

This exception authorizes unlicensed transfers of EAR-controlled software and technology to a foreign affiliate if:

a) only national security ('NS') controls, chemical and biological ('CB') controls, nuclear nonproliferation ('NP') controls, regional stability ('RS') controls, crime controls ('CC'), or significant item ('SI') controls imposed by EAR are present;

b) the destination is one of 36 listed destination countries in this exception;

c) the end-user is notified of the ECCN(s) designation(s), the items shipped, and use of the STA exception prior to transfer; and

a consignee statement is procured from the end-user.

If the EAR-Controlled software and technology is controlled only for national security ('NS') reasons, then transfer to an additional eight destination countries is permitted. A more detailed eligibility analysis can be performed using the Strategic Trade Authorisation interactive compliance tool located at <http://www.bis.doc.gov/seminarsandtraining/stacompliancetool.html>.

Continued

EAR LICENSE EXCEPTION CIV (CIVIL END-USERS AND END USES)

This exception authorizes unlicensed transfers of EAR-controlled software and technology to a foreign affiliate if:

- a) only national security controls imposed by EAR are present and the exception is designated as available for the controlled item;
- b) the destination country is listed in Country Group D:1 of the EAR, which includes China and Russia;
- c) the controlled item is destined for civilian-only 'end-users' and 'end-uses'; and
- d) semi-annual reports of the transfers under this EAR license exception are submitted to the U.S. Bureau of Industry and Security ('BIS'), which is the U.S. Commerce Department agency charged with administering and enforcing EAR export controls.

EAR LICENSE EXCEPTION BAG (BAGGAGE)

This exception authorizes unlicensed transfers of EAR-controlled software and technology to a foreign affiliate if:

- a) the transfer is in the context of a U.S. affiliate's employees travelling to the foreign affiliate; and
- b) with a laptop or other tool, instrument, or equipment and technology used in their employment.

EAR LICENSE EXCEPTION ENC (ENCRYPTION)

This exception authorizes unlicensed transfers of EAR-controlled software and technology to a foreign affiliate if:

- a) the controlled items are encryption items classified under ECCN 5D002 or 5E002;
- b) the foreign affiliate is a U.S. subsidiary as defined in the EAR; and
- c) the foreign affiliate uses the software and technology for its internal use.

The above export control compliance rules for lawfully transferring controlled technologies to foreign affiliates may be used in the context of the following transfer scenarios:

- U.S. and foreign affiliates engaging in remote sharing and collaboration that may cause the intentional or inadvertent transfer of controlled technology;
 - Controlled technology that may be transferred for IT computing and storage purposes to a foreign affiliate's server located abroad;
 - Controlled technology that may be intentionally or inadvertently transferred via laptops and other electronic devices by U.S. affiliate employees who travel to and work at foreign affiliate locations; and
 - Controlled technology that may be transferred under the doctrine of 'deemed export' to foreign affiliate employees visiting or working at U.S. affiliate locations.
-

Continued

Joseph D. Gustavus is a partner in the Troy office of Miller Canfield where he advises clients primarily in the automotive, defense, aerospace, software and information technology sectors on corporate and export control matters.