MILLER CANFIELD

Export Control Compliance Sharing Sensitive Technologies Between International Affiliates General Concepts and Transfer Patterns

September 19, 2013

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 intercompany 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. In other words, U.S. export control laws are not limited in scope to the defense industry.

The intent 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 THAT WILL BE TRACKED AND CONTROLLED BY THE U.S. GOVERNMENT

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).[i]

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;[ii] and

"Defense Services," which includes assistance for design, development, production, operation/use, repair, and maintenance of an item listed as a Defense Article under a USML category.[iii]

Under EAR, a controlled technology is one that is listed as one of the 10 general item categories of the EAR Commerce Control List (CCL).[iv] Within the 10 general CCL categories, specifically controlled items are further classified in five groups lettered A through E.[v] Of these five groups, EAR-controlled technologies are identified as either:

Continued

"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;[vi] and

"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.[vii]

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.

MAKING LICENSED/AUTHORIZED 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.[viii]

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.[ix]

ITAR-Authorized Transfers under Collaborative Agreements. For ITAR-Controlled Technology furnished as Defense 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 Defense 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.[x] TAAs 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.[xi] 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.[xii]

A Good General Rule to Use 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.[xiii]

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.[xiv]

Continued

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.[xv]

EAR License Exception TSU (Technology and Software Unrestricted). This exception authorizes unlicensed transfers of EAR-Controlled software and technology to a foreign affiliate[xvi] if the controlled items are comprised of sales and operations software and technology, other mass market software, or encryption source code that is "publically available"[xvii] (e.g., open source) and its corresponding object code.[xviii]

EAR License Exception STA (Strategic Trade Authorization). This exception authorizes unlicensed transfers of EARControlled software and technology to a foreign affiliate if: (a) only national security (NS) controls, chemical and biological (CB) controls, nuclear non-proliferation (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 (d) a Consignee Statement is procured from the end-user.[xix] If the EAR-Controlled software and technology is controlled only for national security (NS) reasons, then transfer to an additional 8 destination countries is permitted.[xx]

EAR License Exception CIV (Civil End-Users and EndUsers). 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 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) semiannual 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.[xxi]

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 traveling to the foreign affiliate; and (b) with a laptop or other tool, instrument, or equipment and technology used in their employment.[xxii]

EAR License Exception ENC (Encryption). This exception authorizes unlicensed transfers of EAR-Controlled software and technology to a foreign affiliate[xxiii] 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.[xxiv]

Continued

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:

(a) U.S. and foreign affiliates engaging in remote sharing and collaboration that may cause the intentional or inadvertent transfer of Controlled Technology;

(b) Controlled Technology that may be transferred for IT computing and storage purposes to a foreign affiliate's server located abroad;

(c) 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

(d) Controlled Technology that may be transferred under the doctrine of "deemed export" to foreign affiliate employees visiting or working at U.S. affiliate locations.

About the Author

Joseph D. Gustavus is a Senior Principal at Miller Canfield who represents multinational clients and those in the automotive, defense, aerospace, software and information technology sectors. He has served as an attorney in Europe and speaks fluent German and is also a Certified Public Accountant. He is a member and leader of Miller Canfield's Export Controls Group. He represents clients on complex domestic and international acquisitions and commercial transactions and on ITAR and other export control compliance issues. In relation to export controls, he assists clients with controlled asset identification and classification, commodity jurisdiction requests, implementation of export control compliance programs, export license applications, drafting of government-approved Technical Assistance Agreements, Manufacturing License Agreements, other export control-compliant collaboration agreements, performing export control audits and rendering benchmark reports, performing export control due diligence on acquisitions targets, drafting Export Control Manuals and Technology Control Plans, drafting voluntary disclosures on export control violations, and employment of foreign nationals subject to export controls.

This article was originally published in The Michigan International Lawyer, *a State Bar of Michigan International Law Section publication.*

---

[i] 22 C.F.R § 121.1 (2012).

[ii] 22 C.F.R. § 120.10; "Technical Data" includes software as defined in 22 C.F.R. § 121.8(f).

[iii] 22 C.F.R. § 120.6; see also 22 C.F.R. § 121.1(which states that "Defense Services" includes furnishing Technical Data.)

[iv] See 15 C.F.R. § 738, Supp. 1 (2012).

[v] 15 C.F.R. § 738.2(b).

[vi] 15 C.F.R. § 738.2(b); see definition of "Software" under 15 C.F.R. § 772.1; see also 15 C.F.R. § 774, Supp. 2.

[vii] 15 C.F.R. § 738.2(b); see definition of "Technology" under 15 C.F.R. § 772; see also 15 C.F.R. § 774, Supp. 2.

[viii] 22 C.F.R. § 123.1(a).

[ix] 22 C.F.R. § 123.1(a)(1) and (4).

[x] 22 C.F.R. § 124.1(a).

[xi] Id.

[xii] 22 C.F.R. § 124.3(a) and (b).

[xiii] 15 C.F.R. § 730.7.

[xiv] 15 C.F.R. § 730.7.

[xv] 15 C.F.R. § 740.6.

[xvi] The destination must not be a country listed in Country Group E:1 of the EAR (i.e., Cuba, Iran, North Korea, Sudan, Syria).

[xvii] This may also apply to software that may contain some encryption function but is written for a purpose other than encryption.

[xviii] 15 C.F.R. § 740.13.

[xix] See 15 C.F.R. § 740.20 generally; see also 15 C.F.R. § 740.20(c)(1).

[xx] 15 C.F.R. § 740.20(c)(2).

[xxi] 15 C.F.R. § 740.5; see also 15 C.F.R. §743.1.

[xxii] 15 C.F.R. § 740.14.

[xxiii] 15 C.F.R. § 740.17(a)(2).

[xxiv] 15 C.F.R. § 740.17(a)(2).