The 7 Deadly Sins of Technology Export Controls

Common mistakes – and how to avoid them

By George W. Thompson
Thompson & Associates, PLLC
Introduction

• Compliance with technology controls is among the most difficult export control challenges.

• Technology can take many forms, including written, electronic and verbal, which are easy and cheap to duplicate and difficult to track.

• There are many different ways in which technology can be exported. This makes it easy to bypass a compliance gatekeeper.
Introduction

• These risks contrast with those for tangible goods, which typically are exported through specific channels.

• Any plan to safeguard against improper technology exports must take account of the following common errors.
1. **Misunderstanding the terms “technology” and “technical data”**

- Both the Commerce (Export Administration Regulations) and State (International Traffic in Arms Regulations) Departments have adopted detailed definitions of the information they control.

- The EAR refer to controlled information as “technology”, which is identified on the Commerce Control List. In most cases, such controlled technology relates to “development”, “production” or “use” of hardware or software that also is listed on the CCL.
CCL Technology

• CCL technology also may be identified through relationship to a specified process, or to named products, without reference to other CCL provisions.

• Example: ECCN 2E003

• b. “Technology” for metal-working manufacturing processes, as follows:
  • b.1. “Technology” for the design of tools, dies or fixtures specially designed for any of the following processes:
    • b.1.a. “Superplastic forming”;
ITAR-Controlled Technical Data

• In the ITAR, controlled information is called “technical data”, and defined as “Information . . .which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.”

• ITAR-controlled technical data relates to hardware covered by the United States Munitions List, and is specifically identified in individual USML categories.
EAR Technology Errors

• A common error under the EAR is failing to realize when information relating to a product is described by the CCL. Proprietary documents concerning production techniques, for example, may be covered if they are for a product on the CCL.

• Another error is not recognizing when information is “required” for a controlled product’s development, production or use.
EAR Technology Errors

• *Required*. (General Technology Note): As applied to “technology” or “software”, refers to only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions.

• Advisory Opinion Regarding Technology for the Development or Production of Carbon Fiber/Organic Resin Items (Dec. 27, 2010): “ECCN 1E001 does not purport to control *all* technology that in any way relates to or that is merely capable for use in the ‘production’ or ‘development’ of composite items.”
EAR Technology Errors

• Misapplying the “required” standard can lead to over-control or under-control: either the exporter may consider information falling outside the definition to be controlled, or conversely, may fail to treat information meeting the definition as covered.
EAR Technology Errors

• A third common error is overlooking the revised exclusion for published information adopted in June 2016.

• The old rule limited the exclusion to publications, information and software “available for general distribution ... either free or at a price that does not exceed the cost of reproduction and distribution.”

• This meant that most subscription and other paid materials were within EAR coverage.
The revised rule excludes technology and software “made available to the public without restrictions upon its further dissemination”, including through paid subscriptions.

Also excluded is information for “Public dissemination (i.e., unlimited distribution) in any form . . . including posting on the Internet on sites available to the public.”

Open question: does OFAC screening negate “unlimited distribution” requirement?
EAR Technology Errors

• “Commingled” published and unpublished technology remains subject to the EAR.

• Advisory Opinion Regarding Technology for the Development or Production of Carbon Fiber/Organic Resin Items (Dec. 27, 2010): “However, unpublished technology or a combination of published and unpublished technology associating items that constitutes a recipe or part of a recipe peculiarly responsible for achieving a lA002.a-controlled structure or laminate is considered to be "required" technology subject to the EAR unless that association itself is also published.
EAR Technology Errors

• Finally, while information derived from “fundamental research” is outside of the EAR, the exclusion is limited to data that “arises during or results from” the research.

• There is no “blanket exemption” for all information that is transferred in the context of such research, a point often overlooked by researchers in academia.

• The revised rule eliminated distinctions among university, government-sponsored and corporate research.
EAR Technology Errors

• The revised definition is that “fundamental research” “means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.”

• Once a decision is made to maintain such “technology” or “software” as restricted or proprietary, the “technology” or “software,” if within the scope of § 734.3(a), becomes subject to the EAR. 15 C.F.R. § 734.8(a), Note 2.
ITAR Technical Data Errors

• Perhaps the most common error under the ITAR is not realizing that ITAR technical data commingled with non-controlled information is captured by the regulations. There is no de minimis rule; a small percentage of ITAR-controlled information will suffice to “taint” the entire dataset.

• One developing issue is the status of mixed ITAR and EAR “600 series” technology: which set of regulations covers the commingled data?
ITAR Technical Data Errors

• Additionally, while the ITAR definition of “technical data” excludes information in the public domain, the State Department takes a restrictive view of when the exclusion applies.

• Unlike under the Commerce rule, the fact that particular information is readily available on the Internet does necessarily mean it is removed from ITAR coverage.

• Example: design plans for “3D printer gun” posted on the Internet.
2. Failing to identify controlled information at every stage

- Both the EAR and ITAR control information for design and development of products.
- Accordingly, it is commonplace to generate technology or technical data before there is a tangible article.
- This means that the control status of particular information must be identified at the outset of a project, by anticipating the nature and attributes of the product to which it will relate and working backward to determine whether the information is covered as well.
Identify Control Status

• The goal is to ensure that ineligible persons do not receive improper access to controlled technology at the incipient stage or beyond.

• The common error lies in failure to determine information's control status at the earliest possible moment.
3. Misinterpreting regulatory definitions of export and transfer

• Both sets of regulations define “export” as we would expect: the physical movement of products or technology outside the United States to another country.

• There are additional, non-intuitive definitions that apply to technology and technical data exports.

• The first is the “deemed export” rule, under which provision of controlled information to a foreign person in the United States qualifies as an export. It is so-called because an export transaction is deemed to have taken place, even though the information never leaves the U.S.
Deemed Exports

• A deemed export can take place in numerous different ways, for example, through document transfer, physical demonstration and plant tours and accessing of electronic systems, and can involve employees, consultants, contractors, customers and visitors.

• Regardless of whether a company exports commodities, it must be mindful of the circumstances in which it may qualify as an exporter of controlled information.

• Both Commerce and State consider that a foreign person’s mere access to electronic information constitutes an export, regardless of whether that person in fact observes such information. The rule is not specifically stated in the regulations, and can be easy to overlook.
Deemed Exports

• The agencies clarified that position in 2016 notices.
• “A foreign person’s having theoretical or potential access to technology or software is similarly *not* a ‘release’ because such access, by definition, does not reveal technology or software. A release would occur when the technology or software is revealed to the foreign person.”
Deemed Exports

• Note “however, a release will have occurred if a foreign person does actually access technical data, and the person who provided the access is an exporter for the purposes of that release.”

• Therefore, the best practice remains denying unlicensed foreign persons the ability to “actually access technical data”, through denial of electronic network credentials, entry to document storage areas and other circumstances in which controlled information is maintained.
4. Failing to obtain appropriate license or other authorization

• Exports of technology, including deemed exports, require Commerce or State Department authorization when made to a controlled destination, or to a citizen of a controlled destination.

• The EAR set out myriad reasons for control applicable to CCL with the controls varying by country of destination. Even when the destination is controlled, an export may be authorized using a license exception.
License Requirements

• Failing to understand the Commerce matrix of different levels of control and different types of authorization is a common error. The exporter may not realize that particular information is controlled to a particular destination or properly understand the authorization required.

• In particular, license exceptions for technology exports may impose preconditions that the exporter fails to meet; even though a transaction may otherwise have qualified, the failure to comply with prerequisites is a common cause of violations.
License Requirements

• The ITAR present a simpler approach, with the general rule being that most USML technical data is controlled to most destinations and requires a State Department license for export.

• The ITAR provide a couple of different licensing options (DSP-5 licenses and agreements). A common error is not choosing the proper licensing vehicle for the type of export transaction being considered.
5. Not maintaining adequate safeguards against exports

• Information is found in numerous locations, including computers, servers, intranet, internet, proprietary documents such as design and production instructions, manuals, test data and reports, whether in paper or electronic form, and personal knowledge.

• Technology exports can occur in many different ways, for example, by carrying a laptop computer out of the U.S., providing plant tours, discussions or demonstrations to foreign persons, through e-mail or fax transmissions telephone calls and face-to-face conversations, provision of internet access and by application of personal knowledge.
Information Exports

• BIS has adopted a new provision defining “Activities that are not exports, reexports, or transfers.”

• One carve-out is for “Sending, taking, or storing “technology” or “software” that is: (i) Unclassified; (ii) Secured using ‘end-to-end encryption;’ (iii) Secured using cryptographic modules (hardware or “software”) compliant with Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors [with certain additional requirements] . . . ; and (iv) Not intentionally stored in a country listed in Country Group D:5.
5. Not maintaining adequate safeguards against exports

• Not establishing a technology control plan that provides for identifying the control status of information, and that covers all the locations where information is held and all the means by which it can be exported, is a leading cause for violations.

• A second is management or employee failure to follow the requirements of a technology control plan.

• Once a plan is established, ongoing training and auditing are essential.
6. Improper data administration

- Errors can occur even when an exporter recognizes that its information is controlled, and implements a control plan.

- Often, such errors arise from misunderstanding or oversight of the facts. For example, a company may grant computer system access, or provide a plant tour, to an ineligible person because it failed to determine the country of citizenship.
6. Improper data administration

• Another widespread error is leaving controlled information unprotected in open areas (physical or electronic), or improperly disposing of it in a manner that permits access by ineligible persons.

• An effective compliance program must ensure not only that controls are in place, but that they also are followed.
7. Disregarding rules applicable to foreign products and technology

• The EAR and ITAR have extraterritorial effect, meaning that they continue to apply even after goods or technology have been exported from the United States.

• Reexports of controlled U.S. technology, including deemed reexports, are subject to requirements similar to those that applied to the initial exportation.
7. Disregarding rules applicable to foreign products and technology

• Foreign technology developed with controlled U.S.-origin EAR technology may remain subject to the EAR. Foreign technology that incorporates ITAR-controlled technical data will, in most instances, remain subject to the ITAR.

• The same is true for foreign products made with controlled EAR or ITAR technology.

• Foreign companies frequently run afoul of these restrictions because they are unaware that U.S. controls apply to them, or fail to correctly understand and apply the rules.