ROTORCRAFT SERVICES GROUP

Study Guide

New Employees

RSG New Employees Study Guide

Basic regulations and legislation

Much of our export licensing is now under the **Commerce Department's EAR system**. But some critical tech-data, especially regarding Techincal Assistance Agreements, remains under control of the ***International Traffic in Arms Regulations (ITAR),*** which implements **the Arms Export Control Act.** This is administered by the US State Department. In addition, however, we also operate under guidance and licensing (as needed) per the **Commerce Department's *Export Administration Regulations (EAR).*** Some of our products can fit under one or another of these, or even as a kind of hybrid. In all cases, you must check with our export compliance officer, Ms. Leah Purdom, to confirm the classification of any given contract, sensor or other deliverable. This includes tech data, software, hardware and services.

Documents required for an ITAR license application

The basic and most common ITAR license is the DSP-5 form, for the permanent export of hardware, tech data for marketing, and a number of other uses. **The minimum documentation for most export license applications is (i) a purchase order or the contractual equivalent, (ii) product description or brochures and (iii) an end-use/end-user statement.** In the case of Significant Military Equipment – identified by an asterisk in the ITAR's U.S. Munitions List ("USML") – you will need a special form for the end-user statement called a DSP-83.

Documents needed for recordkeeping where an export has No License Required ("NLR")

For licensed exports of ITAR or EAR controlled data or hardware, documentation covering the entire transaction, from invoice to shipping documentation is required. The regulations require export records be maintained for 5 years (the statute of limitations) from the expiration of any related export license. Since a "TAA"-type license can run 10 years, **RSG has a standard minimum records-retention policy of 15 years**, just to be sure, for all export transactions.

Even in the case of NLR exports, there are certain prohibited destinations, end-users/consignees, and purposes. Since it is not realistic to demonstrate to any State or Commerce auditor that a given export did not violate these end-use/end-user prohibitions without an "end-use statement", RSG requires essentially the same documentation for an NLR export as it does for a licensed export. Always check with our Empowered Official when there is any doubt.

Violations of the ITAR or EAR

This is a fundamental truth of working for RSG: violations of these regulations – even inadvertent ones – can come with severe penalties. Since 9/11 an earlier-prevailing spirit of *first-offense = "no harm/no foul"* has disappeared. There is not infrequently a Draconian penalty attached to violations of export-control law/regulation. **First offense in either case can carry penalties of, for example, a fine of more than $1,000,000** and 3 years debarment[1] (meaning, our company would be prohibited from exporting). And that's for *unintentional* infractions – the equivalent of clerical errors. Intentional or reckless disregard of the rules can bring criminal penalties, doubling the fines involved and adding up to 10 years in prison. *Plus* personal and corporate debarment. Remember, that is *per violation*. So above all, don't intentionally violate the law.

We don't want you to overreact here; errors that are obviously accidental or borne out of ignorance will not result in personal, criminal liability. But second or even first corporate offenses

---

[1] *These are the penalties from Part 127 of the ITAR and AECA. The penalties are a bit more complex under the EAR, but basically they are equally serious. Note: a new requirement to annually update fines for inflation raised the old standard $500,000 max. civil penalty initially to $1,111,908, and then to $1,134,602, etc. In this document, for convenience, we roughly state the max. fine as >$1,000,000.*

are sometimes met with strident reactions by the authorities, depending on details. In short, please know that in RSG we are very serious about following export-control procedures.

U.S. Person vs. Foreign Person

"U.S. Person" is defined as either a U.S. citizen, a permanent U.S. resident, a U.S. corporation or government entity, or a "protected person". "Foreign Person" is the opposite, and means the same as "Non-U.S. Person."

Deemed Export

This concept may be a bit counterintuitive: it is possible to "export" something without anything crossing a border. For example, **if you disclose "controlled" data to a foreign national without an appropriate export license – even if you do it around a RSG conference room table in our facilities – this is "deemed" to be an export. The Commerce Department EAR actually terms this a "deemed export." The State Department's ITAR simply calls it an "export," like any other export.**

What's more a deemed export can occur overseas, and in fact in any country. If you are discussing tech data with a foreign national, then very possibly that is a deemed export, and if not controlled by an export license, it's also a violation. And while overseas you should assume that someone is not approved for tech data release until you know definitely that he/she is. **And here is a twist you should be aware of: let's say your best college friend from Stanford or NYU is now working for Aerospatiale in Toulouse. His being a US citizen means little now, because his employment by a "non-US Person" foreign company is presumed by US authorities to conflict his loyalties. Thus, it is possible to be guilty of an unlicensed export of tech-data, even when the data crosses no border, and the disclosure is to a US citizen. So be aware, <u>and</u> beware.**

Employee Licenses for Non-U.S. Person Employees

DDTC registrants like RSG are allowed to employ foreign persons, but special restrictions and/or employee licensing is required to prevent violations. Without a license or other authorization (e.g. a license exemption or exception), it is a violation to expose export-controlled data to a foreign person. Such disclosure is considered a kind of deemed export (defined above). If the employee is a citizen of, say, India, then that disclosure is considered the same as an export of the data to the country of India, even though it occurred totally within RSG's facility. Exposure of export-controlled data to a foreign-person employee must be covered by a special employee license in the name of that specific employee, and with an approve scope adequate to the task.

IMPORTANT: An RSG foreign-person employee will never be allowed to export or disclose any controlled data to anyone. The employee's license only permits RSG to disclose controlled-data to the employee. It is an authorization for RSG to disclose, not for the employee to disclose. So, if that employee is participating in, say, a technical meeting with foreign-person representatives from a customer country, where he is talking about sensitive data and therefore "exporting" to those other foreign persons in attendance, what is legally happening is that RSG itself is the entity doing the exporting. RSG's foreign-person employee is able to participate only if RSG has a license or other authorization in place with an adequate approved scope.

Defense Article

A "defense article" under the ITAR is any item or technical data on the U.S. Munitions List (USML). It is inaccurate to think "defense articles" means hardware that can be used by a military; Dell computers can be used by the military, but that doesn't make them defense articles. And software source code is sensitive from an export point of view, but it still can be EAR as much as ITAR. Then some people think a defense article is defined as having to do with firearms. But firearms are a very small subset of the world of defense articles. And anyway, certain firearms are given to the Commerce Department's EAR, like civilian shotguns, or antiques, and so are not under the ITAR at all. So "defense article" is a broad-brush

term than can best be understood by reviewing the USML in the ITAR. That's § 121. And remember, a "defense article" is an item or tech data on the USML.

When viewed under a microscope, however, the working definition of "defense article" is quite subtle. So for example, if a special electronic gyroscope was originally developed under DOD funding for, say, the F-117 stealth aircraft's navigation system, installing that gyroscope on many commercial planes *does not* make it commercial – it remains a defense article. Conversely, if the US DOD buys a COTS electronic gyroscope originally developed on private funds for commercial transports, that gyroscope remains commercial and does not become a defense article (unless it's modified specifically for a uniquely military application). So, when in doubt, please consult our Empowered Official / Export Compliance Officer.

Export violations can happen even without disclosure to anyone

The State Department's view is that merely crossing a border with defense articles (hardware or tech data) requires a license or exemption – even if you never transfer or disclose to any foreign party while on travel. It doesn't even matter if this was unintentional; e.g. traveling thoughtlessly with a "contaminated" laptop. Commerce does not share so strict a view, but at RSG we default to the stricter view, for the sake of prudence. See the "Laptop Computers" section, below, for more details.

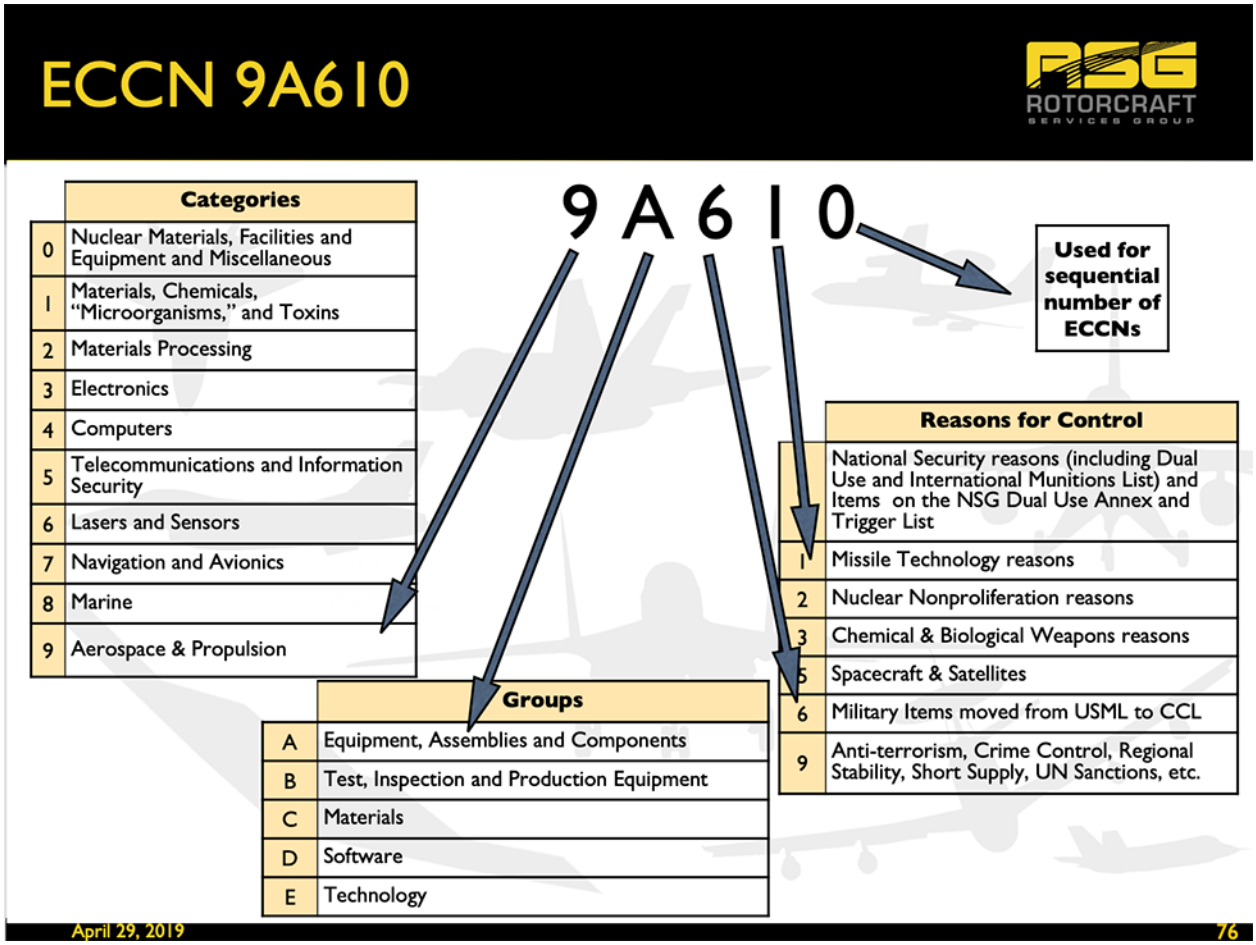
Red Flags

The EAR has a chart of some 14 "red flags." These are suspicious behaviors that are to be considered before making any export. These are not in the ITAR, but once you are sensitized to export control, they are very common sense. So we consider these red flags in the context of all exports, whether EAR or ITAR. **Important to know this: if a violation occurs, and a red-flag situation was ignored, that fact figures into the decision of whether and how intensely to punish the violator.**

ECCN and the CCL

This is a Commerce Department term under the EAR, and it stands for *Export Control Classification Number* **("ECCN")**. It's a 5-character code, e.g. 3A001 for some high-end commercial electronics, or 9A991 for low-level commercial aircraft parts.

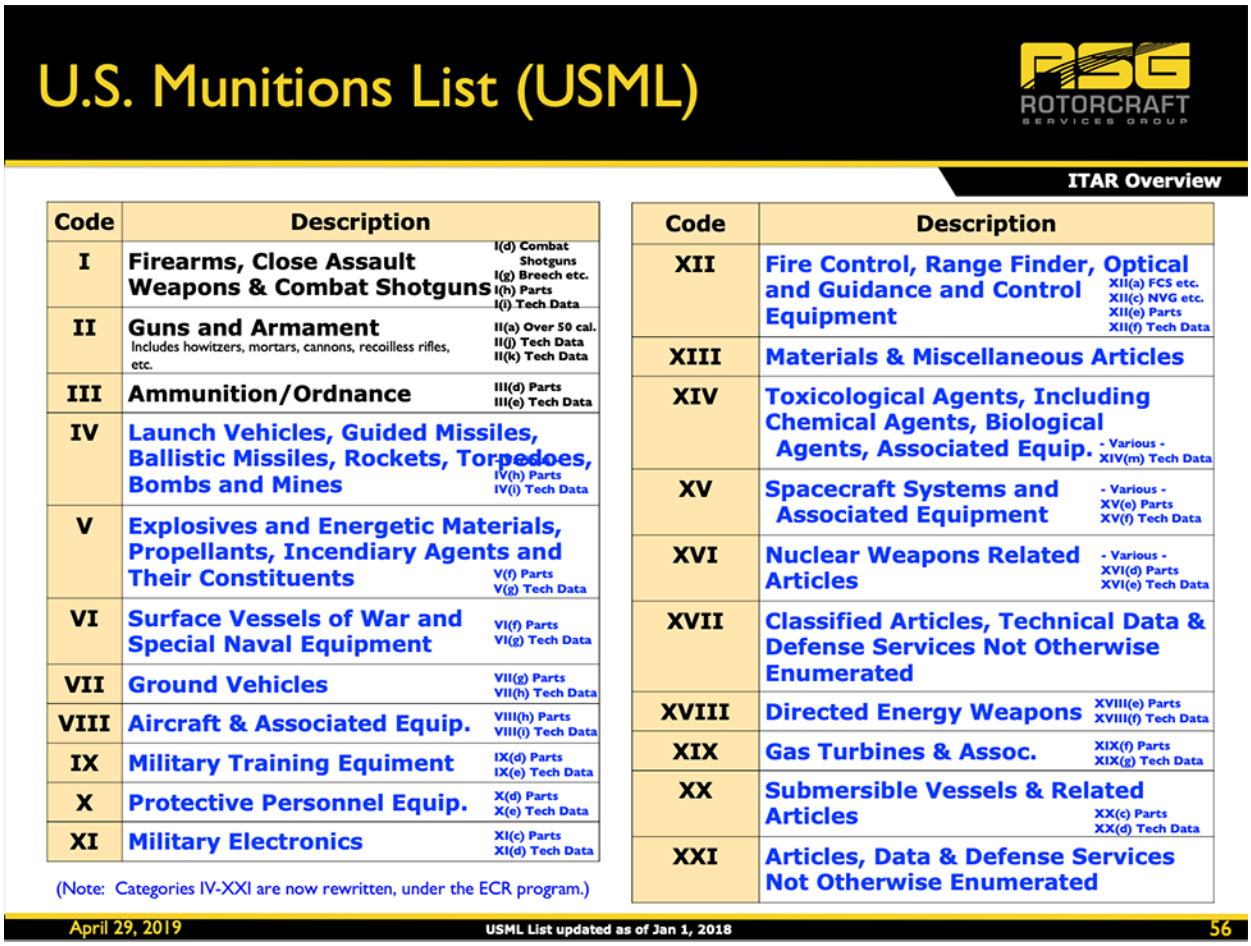
The *Commerce Control List* **("CCL")** is **comprised of some 590 separate ECCNs, ranging from 0A002 to 9E993.** An ECCN can tell you something about itself, since it is built from "Categories", "Groups" and "Reasons for Control", as seen in the illustration below. A **"Group A"** license is for hardware, **"Group D"** is for software, and **"Group E"** is for tech data or technology, as for example in license production. "**EAR99"** is a catch-all when a non-ITAR, EAR-controlled item does not meet the specifications or reasons for control in any of those 527 ECCNs. **Thus, the lowest classification of all under EAR jurisdiction is "EAR99," which can export to most countries in the world without any license.**



USML

The United States Munitions List, in Part 121 of the ITAR, lists the categories of all defense articles. Unlike an ECCN in the EAR's CCL, a USML category tells you nothing about itself, since the category numbering is arbitrary. That is, there are 21 Categories in the USML, expressed in top-level Roman numerals, plus subcategories. For example, Cat. XI(a) items are military electronics, while XI(c) are parts & components of military electronics. Cat. VIII(a) are military aircraft, while most military aircraft parts and components are Cat. VIII(h). *A case in point is the Raytheon's APX 119 IFF (with Mode IV), which is classified under USML Cat. XI(a)(5), and thus counts as not only a defense article under ITAR jurisdiction, but is also Significant Military Equipment ("SME"). SME hardware requires extra documentation in the context of ITAR export licensing. Remember, in the USML at Part 121, paragraphs that start with an asterisk (like this: *) contain SME.*

Note: Because we are now in the midst of major amendments to the USML, with many types of goods transferring export jurisdiction from the ITAR's USML to the EAR's CCL, we expect some of our previous USML classifications to change to the CCL. But not yet, since the change of export classification from the USML to the CCL is a formal procedure RSG has not yet performed. We will keep you posted.



Types of Export Licenses

Some of what we currently plan for export is under the jurisdiction of the Commerce Department. In particular, certain of our cameras are non-ITAR, and are in fact under the lowest EAR category, EAR99, which for most purposes and destinations can be exported without any license at all. For any of our products or technologies that remain ITAR controlled, however, we might need any of a number of different types of ITAR-jurisdiction license. **Most commonly we would use a TAA, or Technical Assistance Agreement, a complicated umbrella export license to cover extensive tech data exchange.** If we export any hardware, that requires a **DSP-5 form license** (called this because you must fill out a form). **Other licenses we may utilize are DSP-73 licenses for the temporary export of hardware for demo or trade shows. Note that by definition, an export/disclosure of tech data to a foreign person is permanent, so a DSP-73 is appropriate only for hardware, not tech data.** Then there are **DSP-61 licenses** for the temporary import of hardware. There are also numerous **licensing exemptions** available to us, depending on the circumstances. Fortunately, in the future, we believe that ITAR-jurisdiction items will be of diminished importance to RSG, with most export-jurisdiction falling under the Department of Commerce, and not the Department of State.

Current classifications include USML Cat. XIII(a) for our F-16 HUD cameras, EAR99 for our Remote-Head cameras, USML Cat. XII(a) for our Nano-Sextant Tracking system, XII(e) for its parts and components, and XII(f) for associated tech data or engineering services.

US Person

If someone is a US citizen, then normally one needs no license to cover the transfer of hardware or tech data to that person. One exception to this rule is when a US citizen is employed by a foreign company, in which case his loyalties are presumed to be compromised, no matter where he is phyRSGally. Under the

ITAR, a permanent US resident, or green-card holder, is identical to citizens in this respect, i.e. generally one can transfer hardware (assuming it does not cross a border) or tech data without a license. **The actual definition of "US Person" is a bit complicated, since it also includes US corporations and other business forms, foreign business entities if they are authorized to do business in the US, federal/state/local US government entities, and "protected persons" who, essentially, are certain kinds of refugees. But your working definition of "US Person" should just be US citizens and green-card holders. Anyone else, whether visitor or employee must prudently be treated as a "non-US Person" or "foreign person" (two terms for the same status).**

Exports

Under the ITAR, to "export" is to:

- Send or take a defense article out of the US, or to transfer registration, title or control of a defense article aircraft, boat or satellite, whether or not the hardware crosses a border.
- Disclose controlled tech data or transfer hardware *inside the US* to a foreign person or to an embassy or any other entity of a foreign government.
- Perform a defense service on behalf of any of the above entities.

"Export" is defined nearly identically in the EAR.

Laptop Computers

If you have any export-controlled tech data on your computer, which is a near-certainty, then you cannot take that computer with you unless you have an export license covering the export of that particular data to that particular country, or unless you carefully "scrub" your hard disk of any controlled data or drawings. This includes emails and attachments. Having an encryption protocol in place on your hard disk does not change this rule. Furthermore, you need not disclose any of the contents to any non-US person while overseas in order to incur a violation. Simply passing through Customs with it is considered a violation by the strictest interpretation of the rules. By the way, this applies also to USB thumb drives, smartphones, etc.

Foreign Customs officials are increasingly seizing laptops and other digital devices, copying the contents, and then returning the devices to the traveler. If such devices contain export-controlled material, this obviously can create unintended export violations. Note that this can also happen to you while clearing U.S. Customs. Should this ever happen to you, you must immediately report the incident to RSG's export-compliance officer. Due to this trend, RSG is evaluating ways to encrypt the entire storage on the device, while minimizing user disruptions – commonly referred to as decryption on the fly. We will keep you advised on the protocol, once decided.

There is an exemption in the ITAR (§ 124.2 "Basic O&M") and an exception in the EAR (§ 740.9 "TMP") that provide some relief. However, since the details are tricky, don't apply in all cases, and must in any event be documented, **you must therefore have *written* permission from our Export Compliance Officer/Empowered Official in order to carry your laptop overseas on business.** (A point to keep in mind for Trivial Pursuit: the ITAR says license *"exemption"* and the EAR says license *"exception"*.)

Safeguarding Laptop Computers While Overseas

If RSG permits you to take your laptop overseas, the proviso is that you must exercise appropriate due diligence to guard against loss or theft. Leaving the computer or thumb drive under your hotel bed is bad. Lock them up in the hotel safe instead. **In short, just treat these electronic devices as if they were a big wad of your personal cash. If you do so, then even if the device is lost or stolen, this will likely not count as an export control violation. The rules require you to be prudent; however, they do not require that you be omniscient, or impervious to theft or muggings.**

Note: RSG's use of an exemption or exception for this purpose, like every such use, must be documented by our Export Compliance Officer. Remember, the basic rule of prudence in export compliance is, *"If you don't have it in writing, it didn't happen."*

Defense Service

Under the ITAR, a "defense service" includes:

- **Furnishing of assistance to foreign persons in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles, whether in the United States or abroad;**

- **Furnishing to foreign persons of any technical data controlled by the ITAR;**

- **Military training of foreign units and forces, regular and irregular, whether in the United States or abroad, including by correspondence courses, and through media of all kinds, training aids, exercises and through the furnishing of military advise.**

Technical Data

This study guide has referred several times to "technical data." Here is a working definition of a hard-to-pin-down term, in the form of hallmarks, drawn from the ITAR and the EAR: (i) it was generated by new R&D for a military application, (ii) it is a genuine engineering scale drawing, not a "cartoon," (iii) it provides meaningful insight into the areas of design or manufacturing, (iv) it goes beyond general scientific, mathematical or engineering principles commonly taught in universities, and perhaps most importantly (v) you would not feel comfortable sharing it with your competitor.

***Note*:** If technical data is controlled under the ITAR or EAR, then normally it must have a special form of license to export or disclose to foreign persons. Under the ITAR this is called a **TAA** (discussed above), a "license" that looks more like a contract, with the usual "WHEREAS..." and "NOW THEREFORE..." you normally find in a contract. And if manufacturing know-how is part of the disclosure, then the more complex **MLA**, or "Manufacturing License Agreement", is required. TAAs and MLAs are Department of State licenses to cover the export or disclosure of ITAR-controlled data or defense services. Under the EAR this can be called a **"Group E"** license, a reference to the letter in the ECCN that means technology or tech data. See, for example, the "ECCN 9A610" graphic, above. So Department of Commerce "Group E" licenses can be used for technical manuals, drawings, license-production contracts, employee licenses, disclosing controlled data to foreign visitors, and so on.

Accessing Technical Data—If Offered by RSG Teaming Partners

Occasionally a RSG teaming partner, typically OEMs such as L3Com, may notify an RSG employee that he/she is being given access-permissions for that teammate's server. **Before accepting that access, any RSG employee must first notify in writing the RSG empowered official, and only access such data *after* receiving written permission in return from that RSG empowered official.** The reason for this procedure is that there are ITAR and EAR disclosure factors that may apply. These factors can apply to any RSG employee, but especially to any foreign-person RSG employee (i.e. a non-citizen without a green card).

##