U.S. Export Controls, Explained

A Plain-Language Guide to How U.S. Export Controls Work

For people who ship products, share technology, or work with people abroad — no prior experience assumed

If your work involves sending products overseas, sharing technical information with people in other countries, or even showing know-how to a foreign colleague at home, U.S. export controls may apply to you. This guide explains what they are, which agency does what, and what to check — in plain English, with every term defined the first time it appears.

Published by mrsanctions.com

Burnin', Briefly: Hot Takes from Mr. Sanctions

What Export Controls Are and Why They Exist

Export controls are U.S. laws that restrict sending certain products, software, and technology out of the country — and sometimes restrict who you can share them with, even inside the United States. The goal is national security and foreign policy: keeping sensitive items and know-how from going to the wrong countries, organizations, or people.

They are different from sanctions, though the two overlap. **Sanctions** (run by the Treasury's OFAC) are mostly about *who* you can do business with. **Export controls** are mostly about *what* you can send and *where* — and they are run by different agencies depending on the item.

The most important thing to understand up front is that there is **no single export-control law**. Which rules apply depends on *what the item is*. Commercial and "dual-use" items go through the Commerce Department; military items go through the State Department; and sanctions can apply on top of either. Sorting out which regime you're in is always the first step.

THE THREE THINGS TO TAKE AWAY

- Export controls restrict what you can send abroad (and who you can share technology with), and which rules apply depends on what the item is.
- "Exporting" is broader than shipping — emailing technical data or showing know-how to a foreign colleague can count.
- You can break these rules by accident and still be liable, so checking before you ship is everything.

Essential Concepts: The Vocabulary You Need First

A handful of terms come up constantly. Learn these and the rest gets much easier.

Export

Sending an item out of the U.S. — but also sharing controlled technology or software with a foreign person, even by email, cloud, or screen-share, and even inside the United States. Reexports (moving an item between two foreign countries) count too.

Dual-use item

Something with both civilian and military (or weapons-related) uses — like many electronics, chemicals, software, and machine tools. Most commercial products are dual-use or purely commercial, and go through the Commerce Department.

EAR (Export Administration Regulations)

The Commerce Department's rulebook for dual-use and commercial items, run by the Bureau of Industry and Security (BIS). Most exports fall here.

ITAR (International Traffic in Arms Regulations)

The State Department's rulebook for military items — weapons, defense equipment, and related technical data — run by the Directorate of Defense Trade Controls (DDTC). Stricter than the EAR.

OFAC sanctions

The Treasury's sanctions rules. They can prohibit a transaction based on *who* or *where* is involved, regardless of what the item is — so they apply on top of export controls.

ECCN and EAR99

Under the EAR, an item is either described by an Export Control Classification Number (ECCN) on a master list, or — if it's subject to the rules but not specifically listed — it's called EAR99 (a catch-all for most ordinary commercial goods).

Deemed export

Sharing controlled technology with a foreign national inside the U.S. The law "deems" this an export to that person's home country — no shipment required.

Entity List / denied parties

Lists of companies and people you generally can't export to without special permission (or at all). Being on a list can block exports even of low-tech items.

License and license exception

A license is government permission to make a specific export. A license exception is a pre-approved category that lets you skip the application if you meet all the conditions.

FDP rule and de minimis

Two rules that pull foreign-made items under U.S. control: the Foreign Direct Product (FDP) rule (the foreign item was made using U.S. technology) and de minimis (the foreign item contains enough U.S.-origin content). Either can apply.

First Question: Which Agency's Rules Apply?

Before anything else, figure out which regime governs your item. Getting this wrong is the most serious mistake in export controls, because each regime has different rules and different penalties.

If your item is…	It's usually governed by…	Run by…
Commercial or "dual-use" (most products, software, technology)	The EAR	Commerce — BIS
Military / defense (weapons, defense gear, related technical data)	The ITAR	State — DDTC
Any item, but a sanctioned party or country is involved	OFAC sanctions (on top of the above)	Treasury — OFAC

WATCH OUT — DON'T GUESS THE REGIME FROM A SIMILAR PRODUCT

Two products that look alike can fall under different regimes. If it's genuinely unclear whether something is a military (ITAR) or commercial (EAR) item, there's a formal process — a **Commodity Jurisdiction request** — to get the State Department to decide. Don't resolve a close call by guessing; the wrong choice can turn a routine shipment into a serious violation.

KEY COMPLIANCE TAKEAWAY

Always settle which regime applies — EAR, ITAR, or another agency, plus any OFAC overlay — before doing anything else, because every other rule depends on it.

What Counts as an "Export" (It's More Than Shipping)

People assume "export" means putting something on a truck or plane. It's much broader, and the surprises are where violations happen.

Under the EAR (see § 730.5), an export also includes **releasing controlled technology or software to a foreign person** — by email, by giving them access to a server or cloud folder, or even by showing it to them in person. And if you share controlled technology with a foreign national *inside the United States*, the law treats it as an export to their home country — a "deemed export."

WATCH OUT — SHARING KNOW-HOW CAN BE AN EXPORT

Emailing a controlled technical drawing to an overseas colleague, giving a foreign-national employee access to controlled software, or walking a foreign visitor through a controlled process can all be **exports** — with no product crossing a border. This "deemed export" trap is one of the most commonly missed rules, especially for companies with international teams.

KEY COMPLIANCE TAKEAWAY

Treat sharing controlled technology or software with any foreign person — by any means, anywhere — as a possible export, not just physical shipments.

How the EAR Decides Whether You Need a License

For commercial and dual-use items, the EAR works through a logical sequence. You don't need to master the details to understand the shape of it.

Step 1: Is the item even covered?

First, is the item **"subject to the EAR"**? Most U.S.-origin items are. Some things are not — published information, fundamental research, and items controlled exclusively by another agency (like ITAR military items). If it's not subject to the EAR, the EAR's license rules don't apply.

Step 2: What is it? (Classification)

Next, classify it. Either it matches an **ECCN** on the control list — which tells you *why* it's controlled (national security, anti-terrorism, and so on) — or it's **EAR99**, the catch-all for most ordinary goods.

Step 3: Where is it going, and does that need a license?

Then check the destination against the Commerce Country Chart. Matching the item's reasons for control against the destination country tells you whether a license is required — unless a license exception applies. EAR99 items usually need no license on this analysis, but read the next box carefully.

WATCH OUT — EAR99 IS NOT A FREE PASS

"It's just EAR99" is not a compliance conclusion. Even a low-tech item with no license requirement based on the country chart can still be **prohibited** if it's going to an embargoed country, to a banned end-user (like a company on the Entity List), or for a prohibited use (like weapons development). The destination and the parties matter as much as the item.

KEY COMPLIANCE TAKEAWAY

Work the EAR in order — is it covered, what is it, where is it going — but never stop at "EAR99," because end-user, end-use, and embargo rules can still require a license or block the deal entirely.

How U.S. Rules Reach Foreign-Made Products

Here's something that surprises a lot of non-U.S. companies: U.S. export controls can apply to products made entirely *outside* the United States. Two separate rules do this.

The de minimis rule: U.S. parts inside

If a foreign-made product *contains* enough controlled U.S.-origin content — generally more than 25% of its value (less for some destinations) — the whole product becomes subject to the EAR. See § 734.4.

The Foreign Direct Product rule: made with U.S. technology

Even with *zero* U.S. parts inside, a foreign product can be caught if it was *made using* certain U.S. technology or software, or by a factory built with U.S.-origin tooling. This is the Foreign Direct Product (FDP) rule, and it has expanded a lot for advanced chips and for Russia- and Iran-related controls.

GOOD TO KNOW — THESE ARE TWO DIFFERENT TESTS

De minimis asks "how much U.S. content is *inside*?" The FDP rule asks "was it *made with* U.S. technology?" A foreign product can pass the de minimis test (no U.S. parts) and still be caught by the FDP rule. If you make things abroad using U.S. inputs or tools, check both.

KEY COMPLIANCE TAKEAWAY

If you deal in foreign-made goods, run both tests — how much U.S. content is inside (de minimis) and whether U.S. technology was used to make it (FDP) — because either one can bring the item under U.S. control.

Who and What You Can’t Export To

Some restrictions are about the recipient or the use, not the item. These can stop even an ordinary EAR99 shipment.

- **The Entity List.** Companies and people who generally can’t receive exports without a license (often refused). See § 744.16. A recent rule also catches companies that are 50% or more owned by listed parties.
- **Banned end-uses.** Weapons of mass destruction, certain military uses in countries like China, Russia, and Belarus, and military-intelligence uses — even for otherwise-uncontrolled items.
- **Denied parties.** People who’ve lost their export privileges — you can’t deal with them at all.

WATCH OUT — DON’T SHIP PAST A "RED FLAG"

Many of these rules apply when you **know** — or *should know* — that something is headed for a banned use or user. Deliberately ignoring warning signs ("red flags") doesn’t protect you; it makes things worse. If something looks off about a customer or destination, you have to resolve it *before* shipping, not after.

KEY COMPLIANCE TAKEAWAY

Screen every customer and destination against the restricted-party lists and think about the end use — and if a red flag comes up, stop and clear it before you ship.

Military Items: The Stricter ITAR Rules

If your item is a military / defense article — on the U.S. Munitions List — the ITAR, run by the State Department, applies instead of the EAR. It’s tougher in a few ways worth knowing.

- **You must register first.** Anyone who makes, exports, or brokers defense articles has to register with the State Department (DDTC) and pay a fee — even if they never actually export.
- **"Defense services" are controlled too.** Helping or training a foreign person in connection with a defense article is itself controlled — a trap with no real EAR equivalent.
- **No de minimis.** Unlike the EAR’s 25% rule, even a tiny U.S. military component can make an entire foreign product ITAR-controlled. There’s no "small amount" exception.
- **Hard "no" destinations.** Exports of defense items to embargoed countries and State Sponsors of Terrorism are essentially prohibited (see § 126.1).

KEY COMPLIANCE TAKEAWAY

> Treat anything military as ITAR — a much stricter regime: register before exporting, watch for the "defense services" and technical-data traps, and remember even a small U.S. defense part can control an entire foreign product.

Don’t Forget Sanctions: The OFAC Overlap

Export controls and OFAC sanctions are **separate** rules that often apply to the same deal. Passing one doesn’t clear the other.

Export controls are mostly about the *item*; sanctions are mostly about the *people and places*. A shipment can be perfectly licensed for the product but still illegal because the buyer is on OFAC’s sanctions list — or vice versa. For sanctions to embargoed countries (Cuba, Iran, North Korea, Syria) and dealings with blocked parties, you usually have to satisfy **both** regimes.

> **GOOD TO KNOW — RUN THREE SCREENS, NOT ONE**
>
> For any cross-border deal, check three things separately: (1) the export-control rules for the item (EAR or ITAR); (2) OFAC sanctions on the people and country involved — screen names against the OFAC sanctions list; and (3) the restricted-party lists across all the agencies. Clearing one screen doesn’t clear the others.

> **KEY COMPLIANCE TAKEAWAY**
>
> Treat export controls and sanctions as two independent checks on the same transaction — and always run a separate sanctions and restricted-party screen, because a green light on the item never means a green light on the parties.

What Happens If You Get It Wrong

Export-control penalties are serious, and — like sanctions — you can be liable for an honest mistake.

Strict liability and big penalties

For civil (non-criminal) purposes, the government generally doesn’t have to prove you *meant* to break the rules — an accidental violation still counts, affecting only the size of the penalty. Civil fines are large (and inflation-adjusted), and deliberate violations can bring criminal charges, including prison. On the EAR side, **BIS’s Office of Export Enforcement** investigates; on the ITAR side, the State Department’s DDTC does, and can **debar** you — strip your export privileges entirely.

Telling the government first helps

> **GOOD TO KNOW — VOLUNTARY DISCLOSURE IS A MITIGATING FACTOR**
>
> Both BIS (under § 764.5) and the State Department **strongly encourage** you to report a violation yourself if you discover one. A voluntary self-disclosure is treated as a major point in your favor — and a deliberate decision *not* to disclose a serious violation counts against you. BIS tightened this policy in 2024, making prompt disclosure more important than ever.

The agencies work together

BIS, OFAC, and the Justice Department increasingly coordinate, and the Justice Department has made export-control and sanctions evasion a top enforcement priority. The practical lesson is the same across all of it: get the classification and screening right up front, clear any red flags, and report promptly if something goes wrong.

> **KEY COMPLIANCE TAKEAWAY**

> Assume you can be penalized for honest mistakes, so prevent them through careful classification and screening — and if a violation surfaces, consider reporting it yourself, because prompt voluntary disclosure is the most reliable way to reduce the consequences.

Official Answers to Common Questions

Plain-language answers to questions that come up constantly. The bottom line comes first.

Q: Which rules apply to my product?

Bottom line: It depends on what the item is.

Commercial/dual-use items go through the EAR (Commerce/BIS); military items go through the ITAR (State/DDTC); sanctions (OFAC) can apply on top. If it's a close call between military and commercial, use a Commodity Jurisdiction request.

Q: Is emailing a drawing to an overseas colleague really an "export"?

Bottom line: Yes, if the technology is controlled.

Releasing controlled technology or software to a foreign person — by email, cloud, or in person, even inside the U.S. — is an export. This is the "deemed export" rule.

Q: My item is EAR99 — am I free to ship it?

Bottom line: Not necessarily.

EAR99 usually needs no license based on the item and destination, but it can still be blocked by embargoes, banned end-users (like the Entity List), or prohibited uses. Check the parties and destination too.

Q: Can U.S. rules apply to a product made abroad?

Bottom line: Yes — through two separate rules.

De minimis (enough U.S. content inside) and the FDP rule (made using U.S. technology). Either can pull a foreign-made item under U.S. control — see § 734.4 and § 734.9.

Q: I cleared the export-control side — do I still need a sanctions check?

Bottom line: Yes, always.

Export controls (the item) and OFAC sanctions (the people and places) are separate. Run a sanctions and restricted-party screen even after the item analysis clears.

Q: What if I discover we made a mistake?

Bottom line: Consider reporting it yourself.

A voluntary self-disclosure to BIS or the State Department is treated as a strong mitigating factor; choosing to hide a serious violation makes things worse.

Where to Find Official Information

When you need the real, current rule, go to the source. These are the official government pages — always check them rather than relying on summaries (including this one) for an actual decision.

If you need…	Go to…
The commercial / dual-use rules (EAR)	Bureau of Industry and Security — the EAR
To check if your item is covered by the EAR	BIS — determine what is subject to the EAR
The military rules (ITAR)	Directorate of Defense Trade Controls
ITAR registration and licensing	DDTC public portal

If you need…	Go to…
The control list of items (ECCNs)	Commerce Control List (Part 774)
Restricted-party / Entity List rules	End-use and end-user controls (Part 744)
To screen names against sanctions	OFAC Sanctions List Search
How export controls and sanctions connect	OFAC — other (non-Treasury) resources