How U.S. Export Controls Work

A Practitioner's Reference Guide to the EAR, the ITAR, and the OFAC Overlap

Jurisdiction • Classification • Licensing • FDP & De Minimis • End-Use/End-User • Enforcement

A foundational, item-neutral guide to the machinery common to U.S. export controls — which agency has jurisdiction, how the EAR decides whether a license is required, the Foreign Direct Product and de minimis rules, end-use and end-user controls, the ITAR defense-trade regime, where export controls meet OFAC sanctions, and how each regime is enforced.

Published by mrsanctions.com

Burnin', Briefly: Hot Takes from Mr. Sanctions

1. How to Use This Guide

HOW TO USE THIS GUIDE

Export controls are not one regime but several, run by different agencies. This guide explains the machinery common to all of them and shows where each fits. Use it as follows:

- **Figuring out which rules apply:** Section 2 (Jurisdiction) — always the first question.
- **Working a dual-use (EAR) item:** Section 3 (Scope), Section 4 (the license-required decision), Section 5 (FDP & de minimis), Section 6 (end-use/end-user), Section 7 (licensing & exceptions).
- **Working a defense (ITAR) item:** Section 8 (the ITAR).
- **Spotting the sanctions overlap:** Section 9 (OFAC and export controls together).
- **Penalties and self-disclosure:** Section 10 (Enforcement).

CRITICAL — JURISDICTION FIRST, ALWAYS

The single most consequential error in export controls is applying the wrong regime's rules. An item is generally controlled by **one** primary regime — the EAR (Commerce/BIS), the ITAR (State/DDTC), or a specialized agency — but OFAC sanctions can apply *on top of* whichever it is. Never assume an item is EAR (or ITAR) by analogy to a similar product; classification and a jurisdiction determination come first, and getting them wrong can turn a routine shipment into a criminal violation.

2. The Threshold Question: Which Agency Has Jurisdiction?

Before any license analysis, determine which U.S. regime governs the item, software, technology, or service. The three you will meet most often:

Regime	Agency	Covers	Authority
EAR (Export Administration Regulations)	Commerce — BIS	Dual-use and commercial items: most commodities, software, and technology; some purely military items not on the USML.	ECRA 2018 (50 U.S.C. 4801–)
ITAR (International Traffic in Arms Regulations)	State — DDTC	Defense articles, defense services, and related technical data on the U.S. Munitions List (USML).	AECA s. 38 (22 U.S.C. 2778)
OFAC sanctions	Treasury — OFAC	Embargoes and targeted sanctions; can prohibit a transaction regardless of the item's classification.	IEEPA / TWEA

Other agencies control narrower classes (Nuclear Regulatory Commission and Department of Energy for certain nuclear items, ATF for permanent imports of munitions, and so on). The EAR's own § 734.3 lists the carve-outs for items "exclusively controlled" by another agency — most importantly the ITAR. If an item is subject to the exclusive jurisdiction of another agency, it is *not* subject to the EAR.

2.1 EAR/ITAR boundary and commodity jurisdiction

The EAR/ITAR line is the highest-stakes boundary. The USML (22 CFR Part 121) enumerates defense articles; the EAR captures dual-use and "600 series" military items that are *not* USML. When jurisdiction is genuinely unclear, DDTC runs a formal **Commodity Jurisdiction (CJ)** process to decide — do not self-resolve a close call. BIS provides a parallel "is it subject to the EAR" analysis for items it controls.

KEY COMPLIANCE TAKEAWAY
Settle jurisdiction before anything else — EAR, ITAR, or another agency — because every downstream rule (license requirement, exceptions, penalties) depends on getting this first step right, and a close call belongs in a Commodity Jurisdiction request, not a guess.

3. The EAR: What Is "Subject to the EAR"?

Under the EAR, the threshold concept is whether an item is **"subject to the EAR"** — defined in § 734.3. If it is not subject to the EAR, the EAR's license requirements simply do not apply (though another regime's might).

3.1 What is subject to the EAR

Per § 734.2 and § 734.3, items subject to the EAR include: all items physically in the United States; all U.S.-origin items wherever located; foreign-made items with more than a de minimis amount of controlled U.S.-origin content (Section 5); and certain foreign-made direct products of U.S. technology or software under the Foreign Direct Product rules (Section 5). "Item" means commodities, software, and technology.

3.2 What "export" means — broader than shipping

As § 730.5 warns, the EAR reaches well beyond goods leaving the country. An **"export"** includes releasing technology or source code to a foreign person — even inside the United States (a **"deemed export"**), even by email, screen-share, or cloud access. Reexports (moving an item from one foreign country to another) and in-country transfers are also controlled.

CRITICAL — DEEMED EXPORTS AND INTANGIBLE TRANSFERS COUNT
Showing controlled technology to a foreign-national colleague in your U.S. office, or giving them access to it on a server, is an **export** to that person's country of nationality — no shipment required. Software uploads, technical-data emails, and cloud access are all exports. This is the most frequently overlooked trigger in the entire regime.

3.3 What is NOT subject to the EAR

Items exclusively controlled by another agency (notably ITAR-controlled defense articles) are outside the EAR, as are certain published/public-domain information, fundamental research, and patent-application data (§§ 734.7–734.10). Publicly available technology and software are generally outside the EAR's scope.

KEY COMPLIANCE TAKEAWAY
Determine "subject to the EAR" first, remember that intangible releases to foreign persons are exports, and check the public-domain/fundamental-research carve-outs before assuming a license analysis is even required.

4. The Core EAR Question: Is a License Required?

Once an item is subject to the EAR, the license question is answered by a structured analysis — the § 732.3 steps walk through it. The essential logic combines *what* the item is with *where* it is going, *who* will receive it, and *what* they will do with it.

4.1 Classify the item: the ECCN and the CCL

Every item subject to the EAR is either described by an **Export Control Classification Number (ECCN)** on the Commerce Control List (Part 774), or — if subject to the EAR but not listed — it is designated **EAR99** (a catch-all for most low-tech commercial goods). The ECCN tells you the **Reason(s) for Control** (national security, anti-terrorism, regional stability, etc.).

4.2 Apply the Commerce Country Chart

With the ECCN's reasons for control in hand, consult the Commerce Country Chart (Part 738). Cross-reference each reason-for-control column against the destination country: an "X" in the cell means a license is required for that reason to that destination, unless a License Exception applies. The § 738.4 walkthrough sets out the mechanics. EAR99 items generally need no license based on the Country Chart — but they can still be caught by end-use, end-user, or embargo controls (Sections 6 and 9).

4.3 The ten General Prohibitions

Underlying the whole analysis are the ten General Prohibitions in § 736.2. They are the things you may not do without a license or exception. The most important to internalize:

General Prohibition	In essence
GP1–GP3	Exporting/reexporting controlled items, controlled parts in foreign products, and foreign direct products (the FDP rule) without authorization. License Exceptions (Part 740) can overcome these three.
GP4	Acting contrary to a denial order (a denied party).
GP5	Exporting to a prohibited end-use or end-user (Part 744) — e.g., WMD, military end-use, Entity List parties.
GP6	Exporting to an embargoed destination (Part 746) without authorization — applies to all items including EAR99.
GP7–GP10	Support for certain proliferation activities; conduct relating to specified persons; violating license/order terms; and proceeding with knowledge a violation is about to occur.

CRITICAL — LICENSE EXCEPTIONS DO NOT OVERCOME EVERY PROHIBITION

Part 740 License Exceptions overcome General Prohibitions One, Two, and Three only. They do **not** override GP4 (denied parties), GP5 (prohibited end-uses/users), GP6 (embargoes), or the others unless a specific exception is expressly authorized in Part 744 or Part 746. So a transaction can be "license-exception eligible" on the item/destination analysis and still be flatly prohibited because of who the end-user is or where it is going.

KEY COMPLIANCE TAKEAWAY

Run the full chain — classify (ECCN/EAR99), read the reasons for control, apply the Country Chart, then test every transaction against all ten General Prohibitions — because the item-and-destination answer is only part of the picture.

5. Reaching Beyond U.S. Borders: FDP and De Minimis

Two rules extend the EAR to *foreign-made* items — and they are where U.S. export controls become genuinely extraterritorial. Both are recurring sources of liability for non-U.S. companies.

5.1 The Foreign Direct Product (FDP) rules

Under § 734.9, a foreign-produced item made *outside* the United States can be subject to the EAR if it is the "direct product" of specified U.S.-origin technology or software, or is produced by a plant (or major component of a plant) that is itself a direct product of such technology/software. If the product scope and the destination/end-user scope of an FDP rule are both met, the foreign item is pulled into the EAR — with **no U.S.-origin parts inside it at all**. The FDP rules have expanded dramatically for advanced computing, semiconductors, and Russia/Iran-related controls.

5.2 The de minimis rule

Separately, under § 734.4, a foreign-made item that *incorporates* controlled U.S.-origin content is subject to the EAR if that content exceeds the de minimis threshold — generally 25% of the item's value (10% for certain destinations, and 0% / no de minimis for some controlled technologies and destinations). The exporter must calculate and document the U.S.-content percentage.

KEY DISTINCTION — FDP vs. DE MINIMIS

They answer different questions. **De minimis** asks how much controlled U.S.-origin *content is inside* a foreign item. **FDP** asks whether the foreign item was *made using* U.S.-origin technology/software or U.S.-origin-tooled plant — even with zero U.S. content in the final item. A foreign product can be caught by FDP while having 0% U.S. content and thus passing de minimis. Run both analyses.

KEY COMPLIANCE TAKEAWAY

For any foreign-made item, run de minimis (how much U.S. content is inside) and the FDP rules (was it made with U.S. technology/software or tooling) as separate tests — a clean de minimis result does not rule out FDP capture.

6. End-Use and End-User Controls

Even a low-tech EAR99 item with no Country-Chart license requirement can require a license — or be flatly prohibited — because of *who* the recipient is or *what* the item will be used for. These controls live in Part 744 and operate independently of the item's classification.

6.1 The Entity List

The Entity List (§ 744.16, Supplement No. 4) names parties believed to pose a national-security or foreign-policy risk. Each entry sets out the license requirements and a license-review policy (often a presumption of denial) for exports to that party — frequently for **all items subject to the EAR**, EAR99 included. A 2025 BIS rule extended certain Entity List controls to entities *50% or more owned* by listed parties — an ownership-aggregation concept echoing OFAC's 50% Rule.

6.2 Prohibited end-uses and end-users

Part 744 also imposes license requirements based on *end-use* and *end-user*: WMD (nuclear, missile, chemical/biological) end-uses; **military end-use/end-user (MEU)** controls for China, Russia, Belarus, and other listed countries; and military-intelligence end-user controls. These can require a license even where the item and destination otherwise would not.

CRITICAL — "IS INFORMED" AND "KNOWLEDGE" TRIGGERS, AND THE DUTY NOT TO PROCEED ON RED FLAGS

Many Part 744 controls bite when the exporter **"knows" or "is informed"** that an item is destined for a prohibited end-use or end-user. "Knowledge" includes willful blindness and an awareness of a high probability. General Prohibition Ten forbids proceeding with a transaction when you know a violation is about to occur. Unresolved **red flags** must be cleared before shipping — proceeding past them is itself a basis for liability.

KEY COMPLIANCE TAKEAWAY

Screen every party against the Entity List and denied-party lists and assess end-use/end-user controls even for EAR99 items — and never ship past an unresolved red flag, because knowledge-based controls make doing so a violation regardless of the item's classification.

7. EAR Authorizations: Licenses and License Exceptions

When the analysis shows a license requirement, there are two ways forward: qualify for a License Exception, or apply to BIS for a license.

7.1 License Exceptions (Part 740)

A License Exception authorizes an otherwise-license-required transaction without an application, if every condition is met. Each ECCN lists the ECCN-driven exceptions that may apply; others are not ECCN-driven. License Exceptions overcome only General Prohibitions One, Two, and Three (Section 4.3), and many carry destination and end-user exclusions — so confirm the exception's terms *and* that no other prohibition independently applies.

7.2 BIS licenses

If no exception fits, apply to BIS for a license. BIS reviews against the licensing policy for the applicable reason(s) for control and end-use/end-user concerns; some categories carry a policy of denial. A license authorizes the specific transaction on its stated terms only.

SAFE HARBOR — EAR99 IS NOT A FREE PASS

Classifying an item as EAR99 means it is not on the CCL and usually needs no license on the item/destination analysis — but it remains **subject to the EAR** and fully exposed to embargoes (GP6), end-use/end-user controls (Part 744), and denied-party prohibitions. "It's just EAR99" is not a compliance conclusion.

KEY COMPLIANCE TAKEAWAY

Work the authorizations in order — an applicable License Exception (conditions met, no excluded destination/end-user), otherwise a BIS license — and never treat EAR99 status as removing end-use, end-user, or embargo exposure.

8. The ITAR: Controlling Defense Articles and Services

Where an item is a defense article or service on the USML, the ITAR (22 CFR 120–130) — administered by the State Department's DDTC under AECA section 38 — governs instead of the EAR. The ITAR is stricter and more categorical than the EAR.

8.1 The U.S. Munitions List and defense services

The USML (Part 121) enumerates defense articles by category (firearms, aircraft, spacecraft, and so on), including parts, components, and related **technical data**. The ITAR also controls **defense services** — furnishing assistance (including training) to foreign persons in connection with defense articles — which has no clean EAR equivalent and catches many companies by surprise.

8.2 Registration is mandatory — before any license

Under AECA section 38 and the ITAR, every person who **manufactures, exports, or brokers** defense articles or services must **register** with DDTC and pay a registration fee — even if they never export. Registration is a prerequisite to licensing, not a substitute for it.

8.3 No de minimis; "see-through" control

CRITICAL DISTINCTION — THE ITAR HAS NO DE MINIMIS RULE

Unlike the EAR, the ITAR generally has **no de minimis exception**: a U.S.-origin defense article incorporated into a foreign end-item can render the *entire* foreign item ITAR-controlled, regardless of how small the U.S. component is ("see-through"). A practitioner who carries the EAR's 25% de minimis intuition into ITAR analysis will badly under-scope it.

8.4 Prohibited destinations (§ 126.1)

§ 126.1 sets out a policy of denial for exports of defense articles/services to embargoed destinations, countries subject to UN Security Council arms embargoes, and State Sponsors of Terrorism. These prohibitions are categorical and apply irrespective of the item's origin.

KEY COMPLIANCE TAKEAWAY

Treat the ITAR as a stricter regime than the EAR: register before exporting, watch for defense-service and technical-data triggers, and remember there is no de minimis — a small U.S. defense component can taint an entire foreign item.

9. Where Export Controls Meet OFAC Sanctions

Export controls and OFAC sanctions are separate regimes that frequently apply to the same transaction. Clearing one does **not** clear the other — and missing the overlap is a classic compliance failure.

9.1 Two regimes, one transaction

The EAR and ITAR control the *item* (its export, reexport, and transfer); OFAC controls the *transaction and the parties* (dealings with sanctioned persons and embargoed jurisdictions). A shipment can be perfectly licensed under the EAR yet prohibited because the buyer is an OFAC-blocked person; conversely an OFAC general license may authorize a dealing that still needs a BIS license for the item. The EAR's § 734.3 expressly notes that OFAC administers separate, overlapping embargo controls.

9.2 Concrete intersections

- **Embargoed destinations:** comprehensive OFAC programs (Cuba, Iran, North Korea, Syria, Crimea) pair with EAR Part 746 and ITAR § 126.1 — expect requirements under both.
- **Blocked persons:** a counterparty on OFAC's SDN List may also be on the BIS Entity List or a denied-party list; screen against all of them.
- **Russia/Iran controls:** recent measures deliberately combine OFAC sanctions, expanded EAR FDP rules, and end-user controls — the regimes were designed to reinforce each other.
- **The SDN-EAR link:** certain SDNs carry EAR license requirements directly (e.g., via § 744.8), so an OFAC listing can itself create an export-control prohibition.

NOTE — THREE SCREENS, NOT ONE

For any cross-border transaction, run three independent analyses: (1) the export-control classification and license analysis (EAR or ITAR); (2) an OFAC sanctions/blocked-party screen; and (3) a denied/restricted-party screen across BIS, DDTC, and OFAC lists. BIS maintains pointers to the other agencies' resources; OFAC similarly lists non-Treasury export-control resources.

KEY COMPLIANCE TAKEAWAY

Treat export controls and OFAC sanctions as parallel, independently binding regimes on the same deal — run the item analysis, the sanctions screen, and the restricted-party screen separately, because authorization under one never implies authorization under the other.

10. Enforcement: Penalties, Agencies, and Voluntary Disclosure

Each regime has its own enforcement track, and all carry both civil and criminal exposure. Liability does not require intent for civil purposes, and the penalties are severe.

10.1 EAR enforcement

BIS's **Office of Export Enforcement (OEE)** investigates EAR violations. The violations are defined in § 764.2; the response menu under Part 766 runs from no action, to a warning letter, to an administrative civil penalty, to denial of export privileges (a denial order), to criminal referral to the Department of Justice. Civil penalties under ECRA are substantial and inflation-adjusted (the statutory maximum is the greater of a set dollar amount or twice the transaction value, per violation); willful criminal violations carry large fines and imprisonment.

10.2 EAR voluntary self-disclosure

Under § 764.5, BIS **strongly encourages** voluntary self-disclosure (VSD) to OEE, and treats a VSD as a significant *mitigating* factor — while a deliberate decision *not* to disclose a significant apparent violation is an *aggravating* factor. BIS sharpened this policy in 2024, making the disclose/don't-disclose calculus more consequential.

10.3 ITAR enforcement

DDTC and its Office of Defense Trade Controls Compliance enforce the ITAR; violations are set out in Part 127. Penalties include civil fines per violation, criminal prosecution under AECA section 38 (substantial fines and imprisonment), **debarment** (loss of export privileges), and seizure/forfeiture. The ITAR also has a voluntary-disclosure mechanism (§ 127.12) that DDTC weighs in mitigation.

10.4 Coordinated enforcement

NOTE — STRICT CIVIL LIABILITY AND CONVERGED ENFORCEMENT

Civil export-control liability is generally **strict** — a good-faith mistake is still a violation, bearing only on the penalty. BIS, OFAC, and DOJ increasingly coordinate enforcement, and DOJ has designated sanctions and export-control evasion a national-security priority. The protective posture is the same across all three regimes: prevent through classification and screening, clear red flags, and disclose promptly when something goes wrong.

KEY COMPLIANCE TAKEAWAY

Assume strict civil liability and converged BIS/OFAC/DOJ enforcement: prevent through rigorous classification and party screening, resolve red flags before shipping, and preserve mitigation through prompt voluntary self-disclosure when a violation surfaces.

11. Compliance Quick-Reference Checklist

A transaction-level sequence for any cross-border movement of items, technology, or services.

1. **Determine jurisdiction.** EAR, ITAR, or another agency? Use a Commodity Jurisdiction request for close calls. (§ 2)
2. **Confirm the item is subject to the EAR (or ITAR).** Check public-domain/fundamental-research carve-outs; remember intangible/deemed exports. (§ 3)
3. **Classify.** Assign an ECCN (or EAR99) under the EAR, or a USML category under the ITAR. (§§ 4, 8)
4. **Run the license analysis.** Reasons for control → Country Chart → the ten General Prohibitions (EAR). (§ 4)
5. **Run FDP and de minimis for any foreign-made item.** They are separate tests. (§ 5)

6. **Assess end-use and end-user controls.** Entity List, MEU/MILEU, WMD end-uses — even for EAR99. Clear all red flags. (§ 6)
7. **Run the OFAC and restricted-party screens.** Separate from the item analysis; three screens, not one. (§ 9)
8. **Find authorization if required.** License Exception → BIS license (EAR); DDTC registration + license (ITAR); OFAC authorization if sanctions apply. (§§ 7–9)
9. **Keep records and disclose if needed.** Retain classification and screening records; consider voluntary self-disclosure if a violation surfaces. (§ 10)

12. Official Document Index

Statutes

- Export Control Reform Act of 2018 (ECRA), 50 U.S.C. 4801–4852
- Arms Export Control Act (AECA) section 38, 22 U.S.C. 2778
- International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1701–

EAR (15 CFR 730–774)

- EAR — subchapter C overview
- § 734.3 — Items subject to the EAR • § 734.4 — De minimis • § 734.9 — FDP rules
- § 736.2 — The ten General Prohibitions
- Part 738 — CCL overview & Country Chart • Part 740 — License Exceptions • Part 774 — the CCL
- Part 744 — End-use/end-user controls • § 744.16 — Entity List
- Part 746 — Embargoes • Part 764 — Enforcement • § 764.5 — Voluntary self-disclosure

ITAR (22 CFR 120–130)

- Part 120 — Purpose and definitions • Part 121 — U.S. Munitions List
- § 126.1 — Prohibited destinations • Part 127 — Violations and penalties

Agencies & lists

- Bureau of Industry and Security (BIS) • BIS — the EAR
- Directorate of Defense Trade Controls (DDTC) • DDTC public portal
- OFAC Sanctions List Search • OFAC — non-Treasury export-control resources