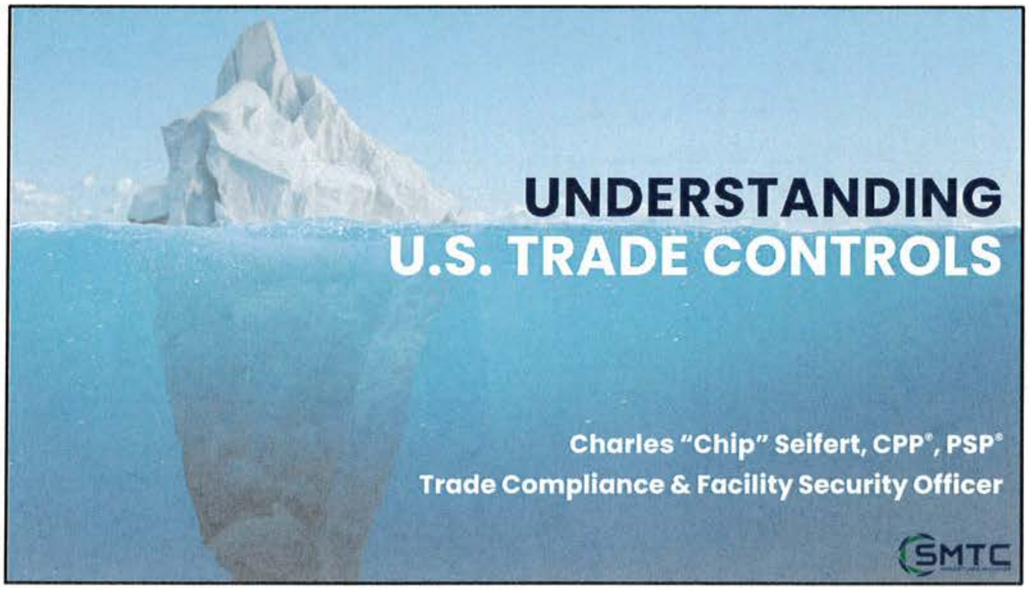
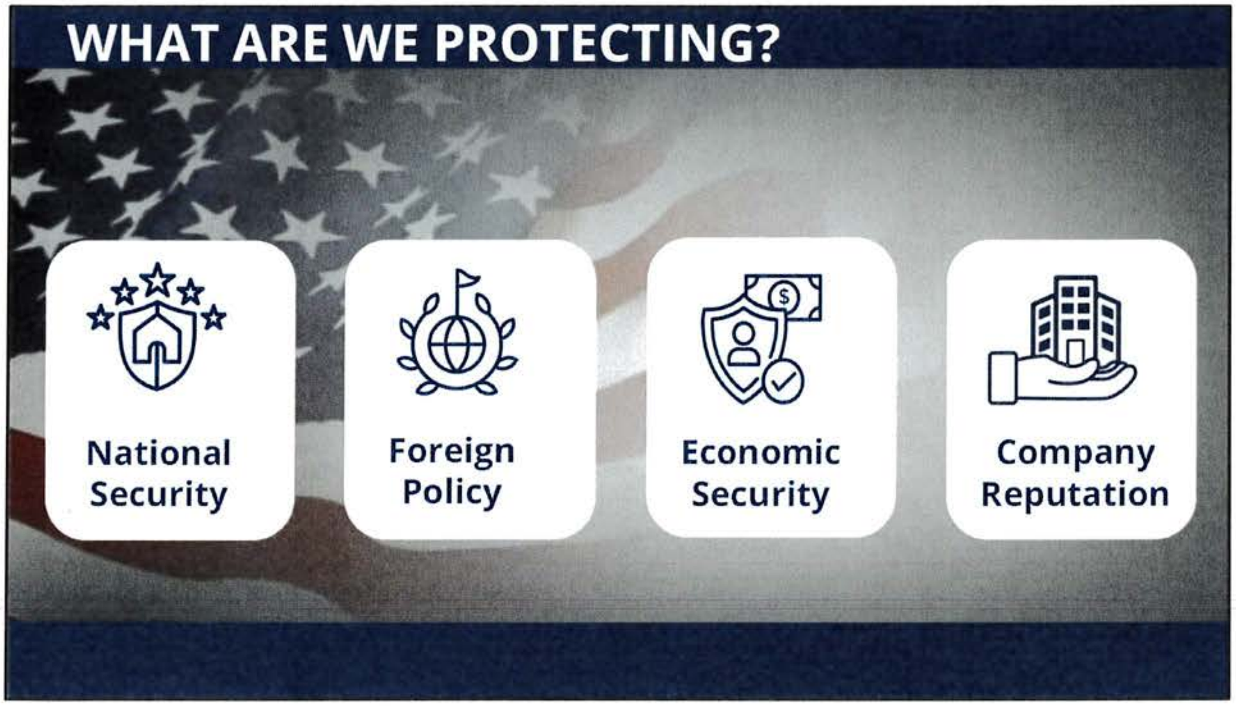


UNDERSTANDING U.S. TRADE CONTROLS

Charles "Chip" Seifert, CPP®, PSP®
Trade Compliance & Facility Security Officer

SMTC



WHAT ARE WE PROTECTING?

National Security

Foreign Policy

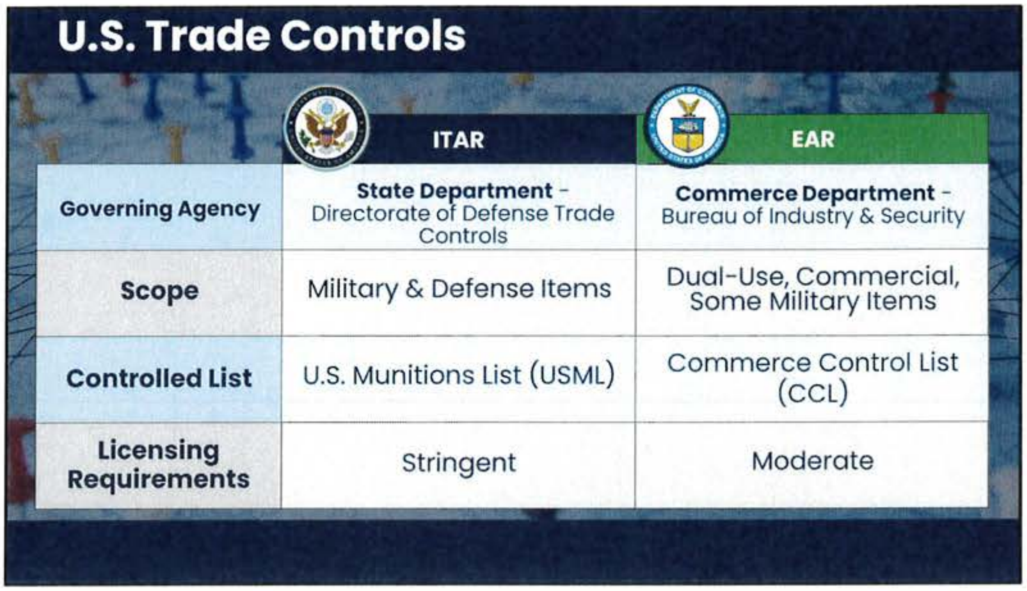
Economic Security

Company Reputation

Before we go any further, let's take a moment to remember why these regulations exist in the first place. They're not designed to make your job harder—although I understand it can sometimes feel that way. The real purpose behind ITAR and EAR is to protect sensitive U.S. technology and keep it out of the hands of our adversaries. That's the core National Security objective.

At the same time, the U.S. does want to share certain technologies with trusted allies and partners—to strengthen relationships and support foreign policy goals. These controls also protect our economic security. Much of this technology is developed and manufactured right here in the U.S. industrial base. We don't want to just give away that competitive advantage.

And lastly, these regulations protect our reputation. Your company wants to be known as a responsible and trusted defense contractor—not a company that cuts corners or mishandles sensitive data. Violations of these rules can result in severe penalties, both for companies and individuals. So it's in all of our best interests to take them seriously.



U.S. Trade Controls

	ITAR	EAR
Governing Agency	**State Department** - Directorate of Defense Trade Controls	**Commerce Department** - Bureau of Industry & Security
Scope	Military & Defense Items	Dual-Use, Commercial, Some Military Items
Controlled List	U.S. Munitions List (USML)	Commerce Control List (CCL)
Licensing Requirements	Stringent	Moderate

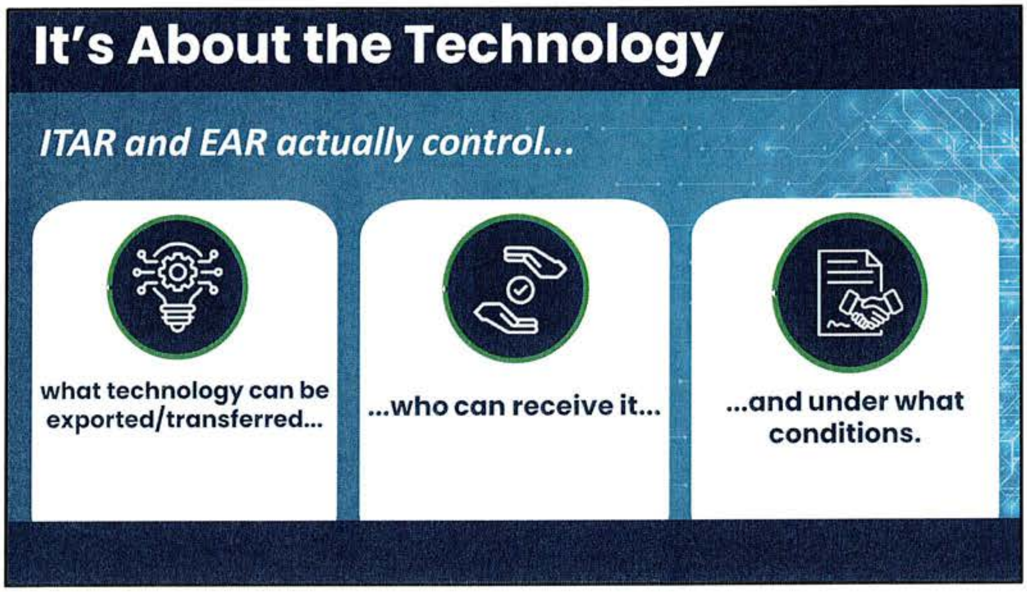
There are two different sets of regulations govern how items can be exported from the United States:

The ITAR—or International Traffic in Arms Regulations—covers military and defense articles, and is managed by the U.S. State Department. Items controlled under the ITAR are listed on the U.S. Munitions List.

The EAR—Export Administration Regulations—covers commercial and dual-use items, and is overseen by the Commerce Department using the Commerce Control List, or CCL.

What's important here is that each regulation has its own rules, definitions, and licensing requirements. Understanding which one applies to the item or information you're handling is absolutely critical.

We'll break this down further as we move through the presentation.



It's About the Technology

ITAR and EAR actually control...

what technology can be exported/transferred...

...who can receive it...

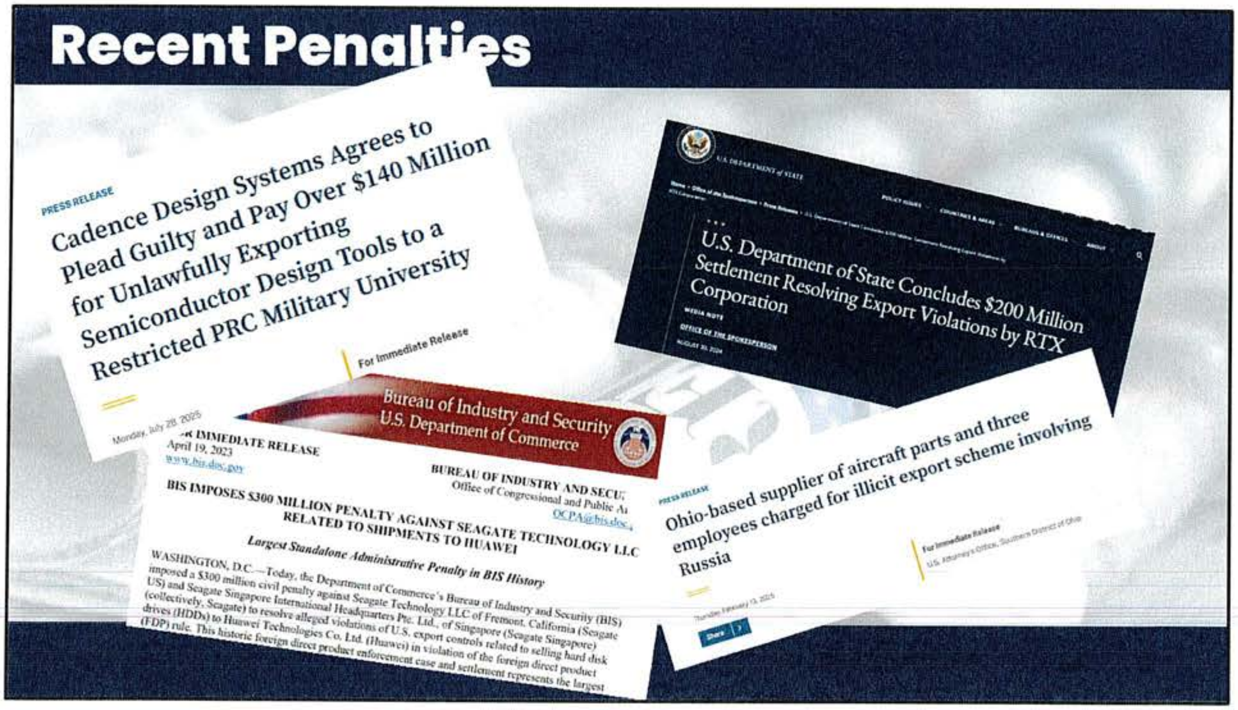
...and under what conditions.

A lot of people think trade compliance is all about hardware—missiles, weapons, or finished products. But in reality, it's often about the technology behind those products.

That includes things like:

Technical data
Schematics
Software
And engineering know-how

This is what the ITAR and EAR are really trying to protect—the knowledge and capability, not just the physical item. Now, I'll be the first to admit: these regulations can get very technical and very confusing. And to be clear—I'm not trying to turn you into a compliance expert today. But if you understand the goals behind the regulations, it becomes easier to understand why they're structured the way they are, and why certain things are tightly controlled while others aren't.



Recent Penalties

PRESS RELEASE

Cadence Design Systems Agrees to Plead Guilty and Pay Over $140 Million for Unlawfully Exporting Semiconductor Design Tools to a Restricted PRC Military University

For Immediate Release

Monday, July 28, 2025

U.S. DEPARTMENT of STATE

POLICY ISSUES COUNTRIES & AREAS BUREAUS & OFFICES ABOUT

U.S. Department of State Concludes $200 Million Settlement Resolving Export Violations by RTX Corporation

MEDIA NOTE

OFFICE OF THE SPOKESPERSON

AUGUST 30, 2024

Bureau of Industry and Security
U.S. Department of Commerce

…R IMMEDIATE RELEASE
April 19, 2023
www.bis.doc.gov

BUREAU OF INDUSTRY AND SECU…
Office of Congressional and Public A…
OCPA@bis.doc.…

BIS IMPOSES $300 MILLION PENALTY AGAINST SEAGATE TECHNOLOGY LLC RELATED TO SHIPMENTS TO HUAWEI

Largest Standalone Administrative Penalty in BIS History

WASHINGTON, D.C.—Today, the Department of Commerce's Bureau of Industry and Security (BIS) imposed a $300 million civil penalty against Seagate Technology LLC of Fremont, California (Seagate US) and Seagate Singapore International Headquarters Pte. Ltd., of Singapore (Seagate Singapore) (collectively, Seagate) to resolve alleged violations of U.S. export controls related to selling hard disk drives (HDDs) to Huawei Technologies Co. Ltd. (Huawei) in violation of the foreign direct product (FDP) rule. This historic foreign direct product enforcement case and settlement represents the largest

PRESS RELEASE

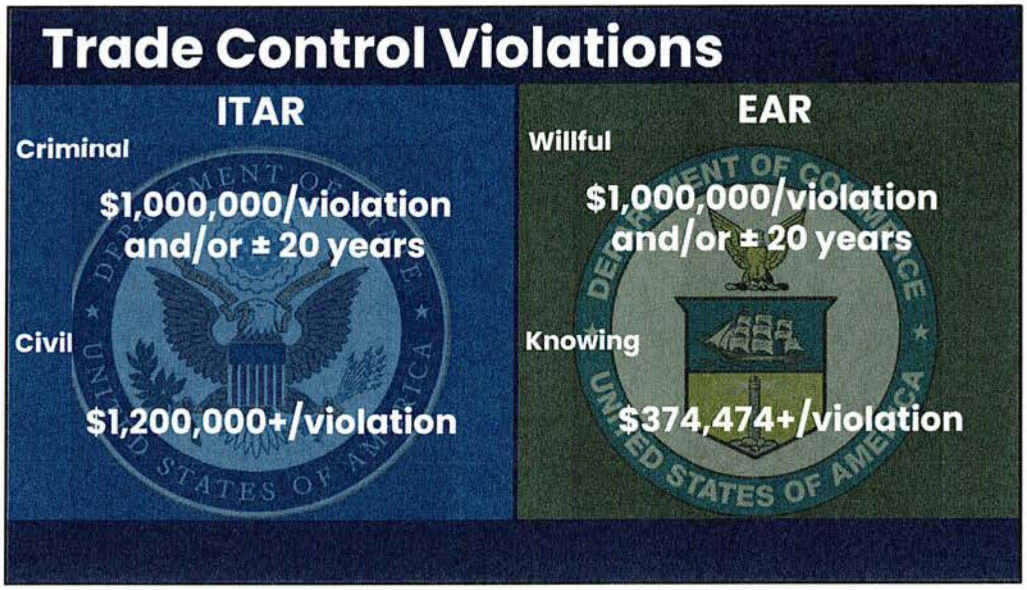
Ohio-based supplier of aircraft parts and three employees charged for illicit export scheme involving Russia

For Immediate Release
U.S. Attorney's Office, Southern District of Ohio

Thursday, February 13, 2025

Share

I know you understand that the U.S. government takes trade controls very seriously. But to underscore that fact, the government also attaches serious fines and penalties against companies and individuals who violate these regulations. These are just a few recent examples of defense contractors that were fined for ITAR violations.



Trade Control Violations

ITAR

Criminal

$1,000,000/violation and/or ± 20 years

Civil

$1,200,000+/violation

EAR

Willful

$1,000,000/violation and/or ± 20 years

Knowing

$374,474+/violation

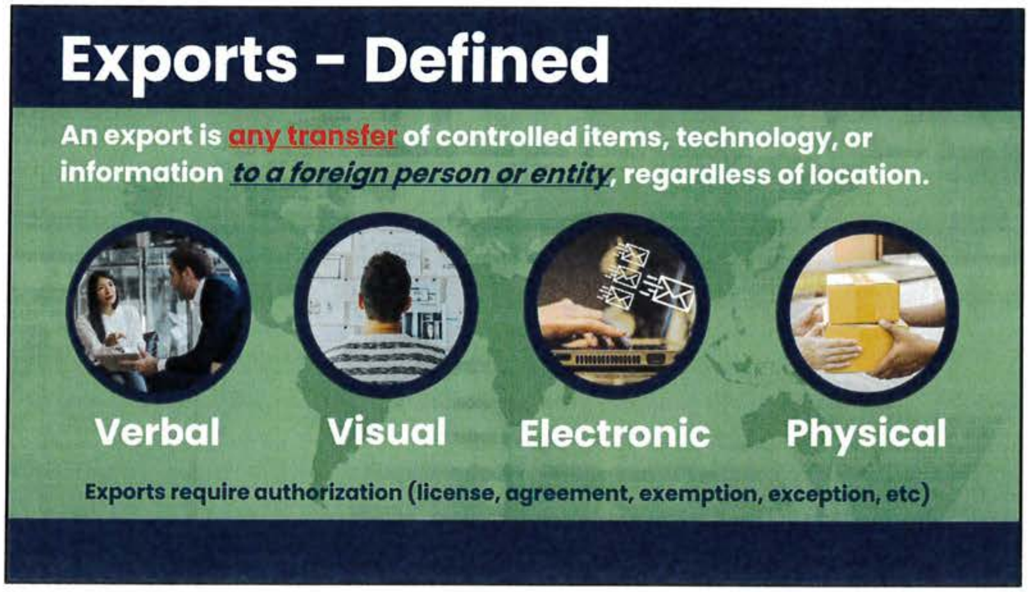
Items can be "captured" under the USML in one of two ways:

1. Because they are explicitly enumerated, or
2. Because they are "specially designed" for a military application.

Here's an example of a defense article—an end-item that is specifically enumerated in the USML. It's listed by name, so there's no ambiguity about whether it's controlled.

But not all items are called out that clearly. Many defense articles are captured because they are specially designed—meaning they were engineered for military use and are not intended for commercial applications.

Take this connector cable as an example. It may look simple, but it's specially designed for use in a guided missile, based on features like its pin configuration and environmental hardening. Because of that, it falls under ITAR—it's captured by the USML—and must be handled and protected accordingly.



Exports - Defined

An export is any transfer of controlled items, technology, or information *to a foreign person or entity*, regardless of location.

Verbal **Visual** **Electronic** **Physical**

Exports require authorization (license, agreement, exemption, exception, etc)

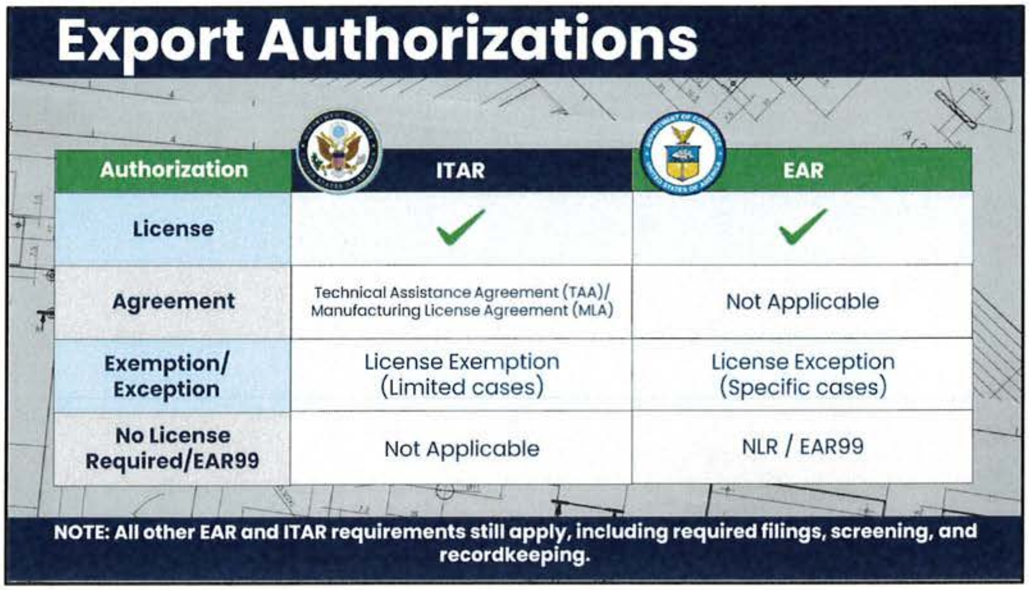
I touched on this earlier, but I want to revisit it—because it's important to understand just how easy it is to inadvertently "export" technology. The U.S. government doesn't care how protected information is transferred to a foreign person or entity—only that it happens.

An export can occur through:

- A conversation overheard in a meeting or on a phone call
- A visual transfer—a foreign national simply seeing controlled information on a screen, a whiteboard, a physical product, or a drawing on the shop floor
- An electronic transfer, like email, shared drives, or cloud uploads
- Or via a physical transfer—in person or through a shipment

And here's what surprises many people: An export doesn't have to cross a border. It can occur right here in the United States—even inside our own facilities—if a foreign national gains unauthorized access to controlled data or technology.

This is why facility tours can carry risk, and why we take extra precautions—like visual barriers, escorted access, and advance coordination with Trade Compliance and Facility Security.
The bottom line: Exports can happen anywhere, often unintentionally,
and it's up to all of us to stay aware and alert.



Export Authorizations

Authorization	ITAR	EAR
License	✓	✓
Agreement	Technical Assistance Agreement (TAA)/ Manufacturing License Agreement (MLA)	Not Applicable
Exemption/ Exception	License Exemption (Limited cases)	License Exception (Specific cases)
No License Required/EAR99	Not Applicable	NLR / EAR99

NOTE: All other EAR and ITAR requirements still apply, including required filings, screening, and recordkeeping.

Once you know what the item/data is and how it's classified, you choose the **authorization path**. There are four buckets:

1) License (ITAR & EAR).

The default for controlled items or technical data. It's specific—what, who, where, and why—and it takes time. For ITAR, the company must be registered with DDTC before applying.

2) Agreement (ITAR only).

Use a TAA for providing controlled technical assistance or a MLA for authorizing manufacture abroad. These are detailed, State-approved instruments—plan lead time.

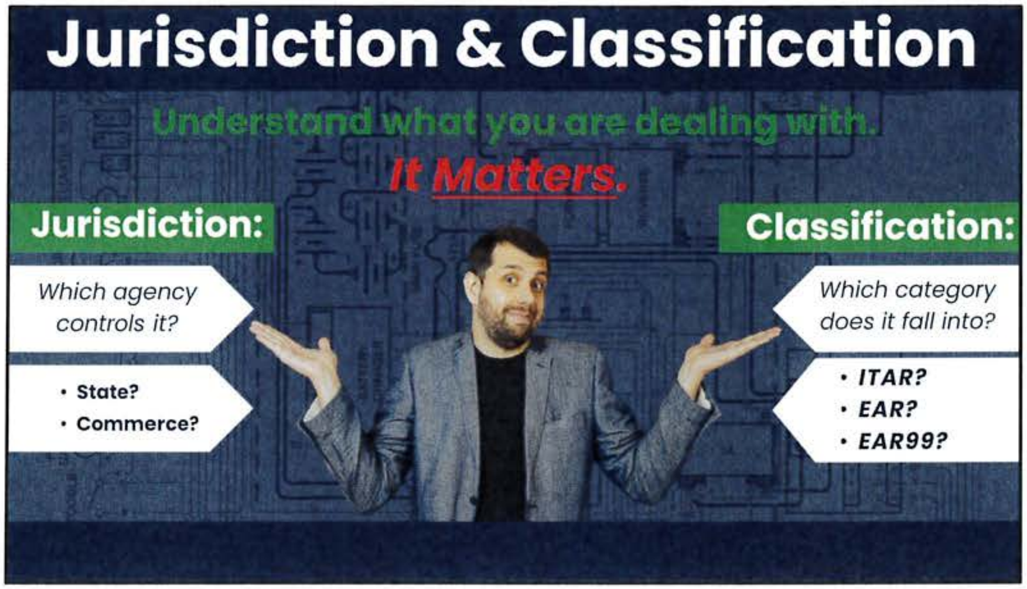
3) Exemption/Exception.

ITAR **exemptions** and EAR **license exceptions** can be powerful but are narrow and conditional. Use only when every eligibility condition is met—don't assume; verify with Trade.

4) NLR / EAR99 (EAR only).

Items not listed on the CCL are generally NLR, but that is not blanket approval. End-use, end-user, and destination controls still apply—and can flip NLR to "license required."

Key reminder: Using NLR, an exemption, or an exception does not waive other requirements—you still have screening, any required EEI filings/notations, and recordkeeping.



Jurisdiction & Classification

Understand what you are dealing with.

It Matters.

Jurisdiction:

Which agency controls it?

- State?
- Commerce?

Classification:

Which category does it fall into?

- ***ITAR?***
- ***EAR?***
- ***EAR99?***

As you can see, one of the most important steps in export compliance is understanding exactly what you're dealing with.

This is where jurisdiction and classification come into play—and it's a crucial first step.

If these determinations are made incorrectly, it can lead to serious compliance violations and potential penalties.

Let's break those terms down:

Jurisdiction refers to which U.S. government agency controls the item or data.

As we covered earlier:

The State Department has jurisdiction over sensitive military technology, governed by the ITAR.

The Commerce Department oversees most commercial and dual-use items, including some less sensitive military equipment, under the EAR.

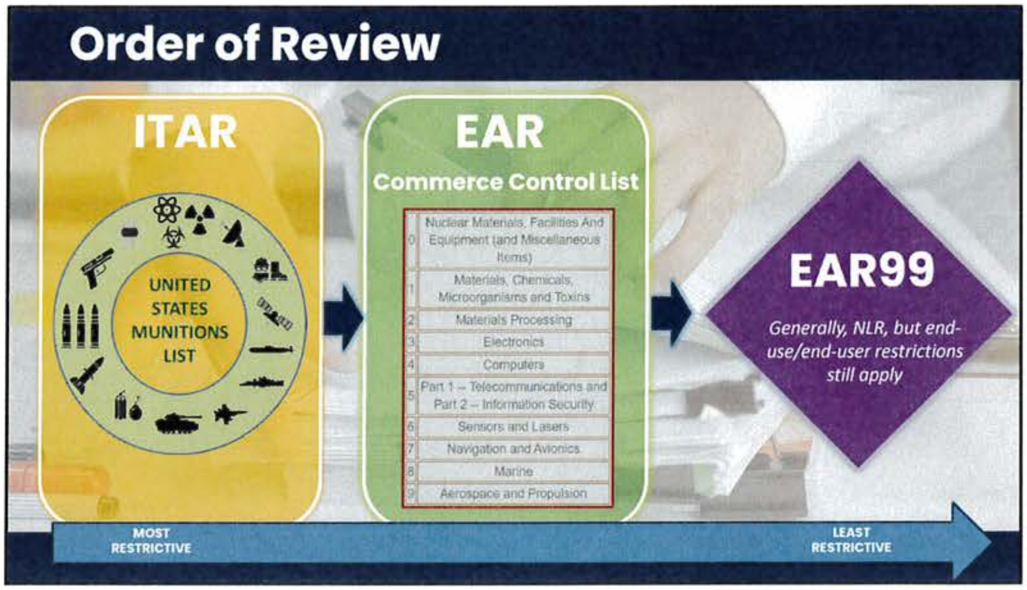
Determining jurisdiction is vital, because it tells you which regulation applies—and which agency handles the licensing.

Classification refers to the specific identification of the item or technology.

Once you know which agency has jurisdiction:

1. If it's State, you classify it using the U.S. Munitions List (USML) under the ITAR.
2. If it's Commerce, you refer to the Commerce Control List (CCL) to find the appropriate ECCN or determine if it's EAR99.

Each regulation—ITAR and EAR—has very different rules, restrictions, and license requirements. So everything else flows from that initial jurisdiction and classification decision. Getting this part right is foundational.



Order of Review

ITAR

UNITED STATES MUNITIONS LIST

EAR

Commerce Control List

0	Nuclear Materials, Facilities And Equipment (and Miscellaneous Items)
1	Materials, Chemicals, Microorganisms and Toxins
2	Materials Processing
3	Electronics
4	Computers
5	Part 1 – Telecommunications and Part 2 – Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

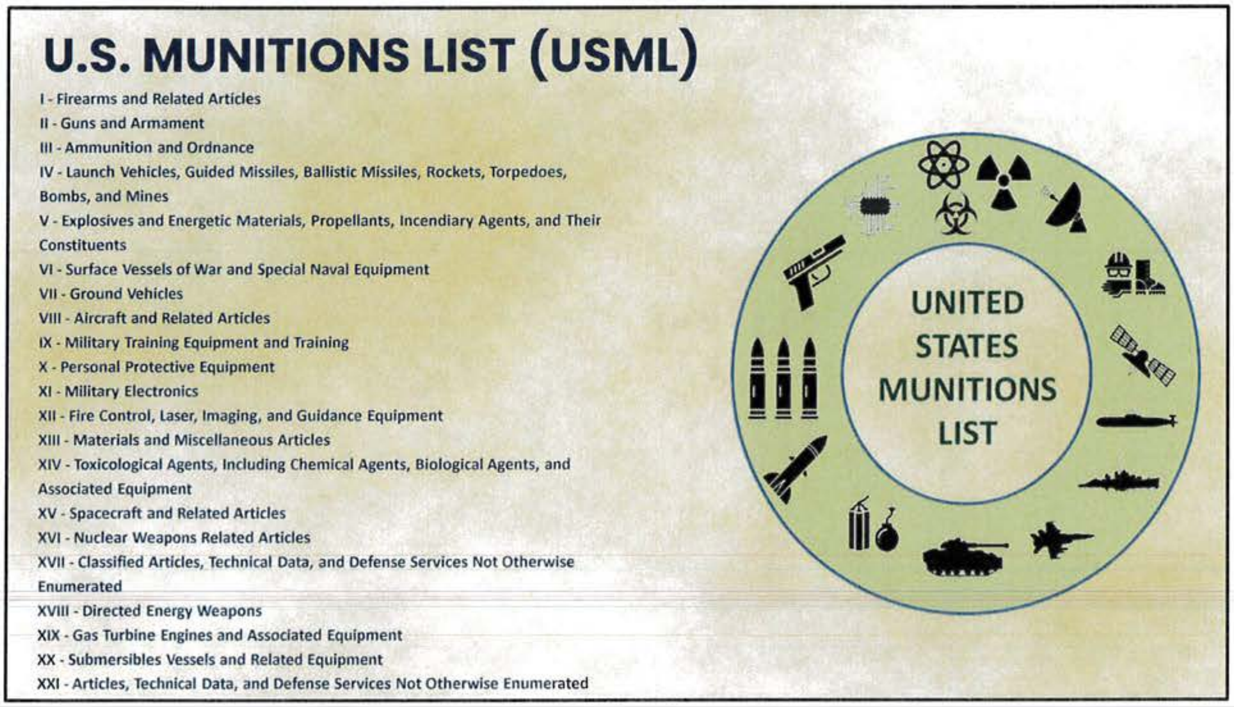
EAR99

Generally, NLR, but end-use/end-user restrictions still apply

MOST RESTRICTIVE

LEAST RESTRICTIVE

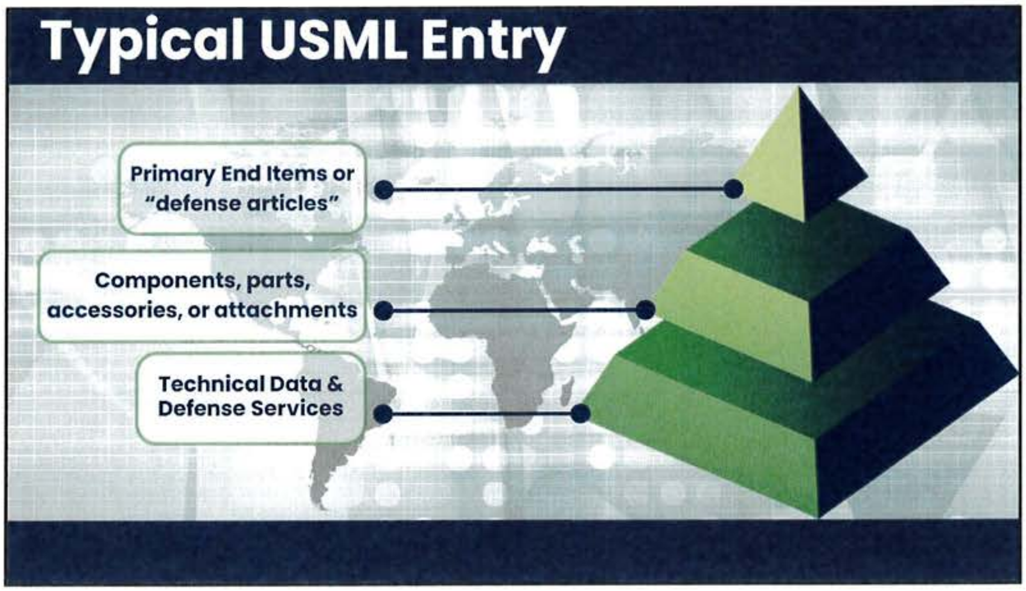
This order of review highlights the hierarchy of trade regulations. The ITAR is the most restrictive regulation and as a result protects the most critical U.S. Defense technology. If an item isn't classified or "captured" under the ITAR, then the next step is to check the EAR to see if that item is listed there. The EAR can contain defense products that are routinely moved from protection under the USML, but also includes lots of other items. The EAR is much more expansive than the ITAR. If an item cannot be found in the ITAR's USML or in the EAR's CCL, then that item is considered "EAR99". We will discuss EAR99 a little later.



U.S. MUNITIONS LIST (USML)

I - Firearms and Related Articles
II - Guns and Armament
III - Ammunition and Ordnance
IV - Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
V - Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents
VI - Surface Vessels of War and Special Naval Equipment
VII - Ground Vehicles
VIII - Aircraft and Related Articles
IX - Military Training Equipment and Training
X - Personal Protective Equipment
XI - Military Electronics
XII - Fire Control, Laser, Imaging, and Guidance Equipment
XIII - Materials and Miscellaneous Articles
XIV - Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
XV - Spacecraft and Related Articles
XVI - Nuclear Weapons Related Articles
XVII - Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
XVIII - Directed Energy Weapons
XIX - Gas Turbine Engines and Associated Equipment
XX - Submersibles Vessels and Related Equipment
XXI - Articles, Technical Data, and Defense Services Not Otherwise Enumerated

I just wanted to briefly show you which items are listed in the ITAR's USML. There are 21 categories of defense items and technology. We will peel this back a little and look under the hood to see how these categories are arranged.



Typical USML Entry

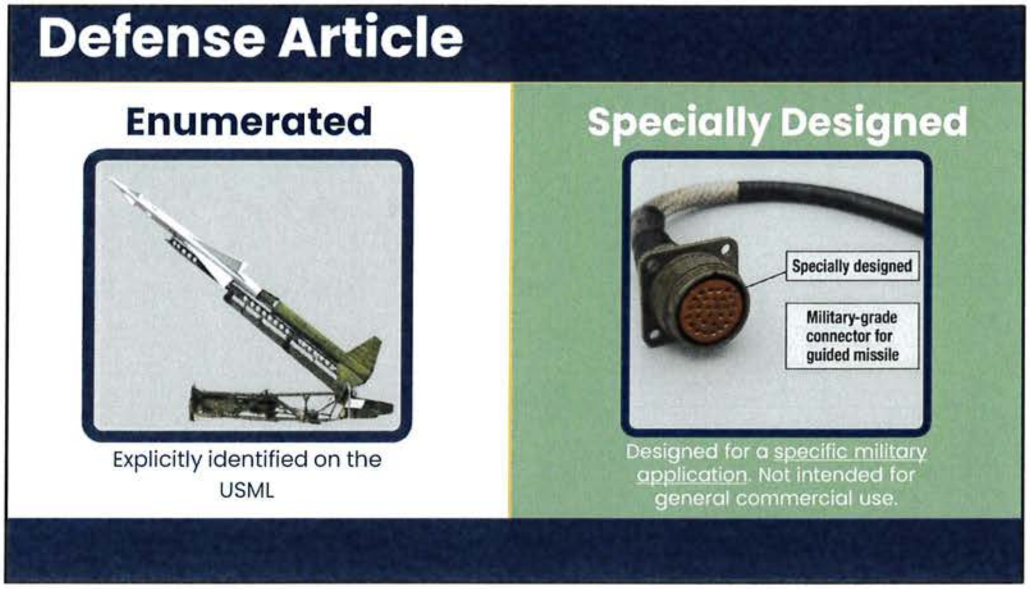
Primary End Items or "defense articles"

Components, parts, accessories, or attachments

Technical Data & Defense Services

The U.S. Munitions List doesn't just cover complete systems or weapons. Each category starts with the major end-item, also known as a "defense article"—things like aircraft, missiles, or electronics.

But it doesn't stop there. The USML also extends to:
Components, Parts, Accessories, and Attachments that are specifically designed for those end-items.
In addition, it may control the technical data and defense services related to the development, production, or use of those items.
In other words:
If it supports, enables, or enhances a defense article—and especially if it's specially designed—it may be ITAR-controlled. We'll look at examples of that next.



Defense Article

Enumerated

Explicitly identified on the USML

Specially Designed

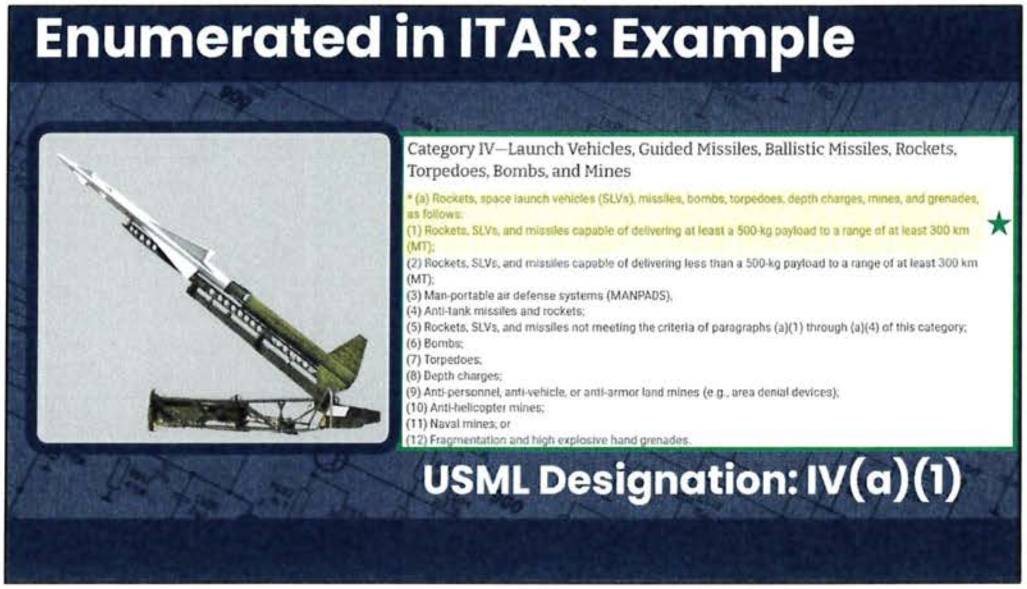
Designed for a specific military application. Not intended for general commercial use.

Items can be "captured" under the USML in one of two ways:

1. Because they are explicitly enumerated, or
2. Because they are "specially designed" for a military application.

Here's an example of a defense article—an end-item that is specifically enumerated in the USML. It's listed by name, so there's no ambiguity about whether it's controlled. But not all items are called out that clearly. Many defense articles are captured because they are specially designed—meaning they were engineered for military use and are not intended for commercial applications. Take this connector cable as an example. It may look simple, but it's specially designed for use in a guided missile, based on features like its pin configuration and environmental hardening.

Because of that, it falls under ITAR—it's captured by the USML—and must be handled and protected accordingly.



Enumerated in ITAR: Example

Category IV—Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines

* (a) Rockets, space launch vehicles (SLVs), missiles, bombs, torpedoes, depth charges, mines, and grenades, as follows:

(1) Rockets, SLVs, and missiles capable of delivering at least a 500-kg payload to a range of at least 300 km (MT); ★

(2) Rockets, SLVs, and missiles capable of delivering less than a 500-kg payload to a range of at least 300 km (MT);

(3) Man-portable air defense systems (MANPADS),

(4) Anti-tank missiles and rockets;

(5) Rockets, SLVs, and missiles not meeting the criteria of paragraphs (a)(1) through (a)(4) of this category;

(6) Bombs;

(7) Torpedoes;

(8) Depth charges;

(9) Anti-personnel, anti-vehicle, or anti-armor land mines (e.g., area denial devices);

(10) Anti-helicopter mines;

(11) Naval mines; or

(12) Fragmentation and high explosive hand grenades.

USML Designation: IV(a)(1)

This is what an enumerated entry in the USML looks like. On the right, you'll see Category IV, which covers launch vehicles, guided missiles, rockets, and similar munitions. I've highlighted the paragraph that directly applies to the missile shown in the image. But notice—this is just one part of a long list of possible subcategories within this section. This is why it's so important to understand exactly what technology you're dealing with. If you land in the wrong part of the list—or overlook a key feature—you could end up misclassifying an item or failing to protect it properly. You'll also see the specific USML paragraph designation at the bottom of the slide:

Category IV(a)(1)

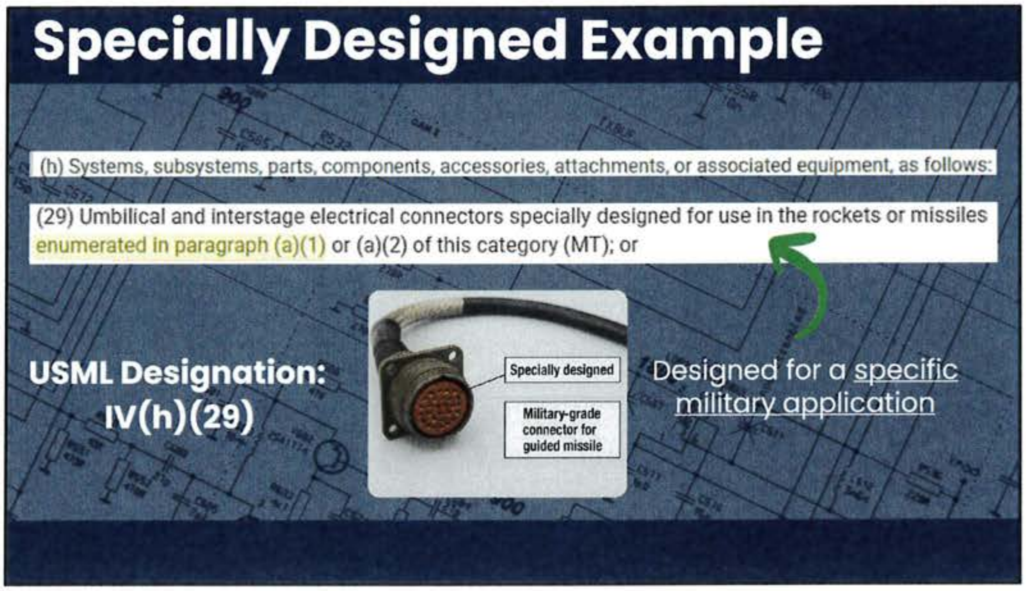
This kind of reference is what you should expect to see on any item marked as ITAR-controlled.

Why does this matter?

Because once you know the exact USML category and paragraph, you'll be able to:

- Determine licensing requirements
- See if any exemptions apply
- Understand any handling or transmission restrictions

In short, this information is the key to compliance.



Specially Designed Example

(h) Systems, subsystems, parts, components, accessories, attachments, or associated equipment, as follows:

(29) Umbilical and interstage electrical connectors specially designed for use in the rockets or missiles enumerated in paragraph (a)(1) or (a)(2) of this category (MT); or

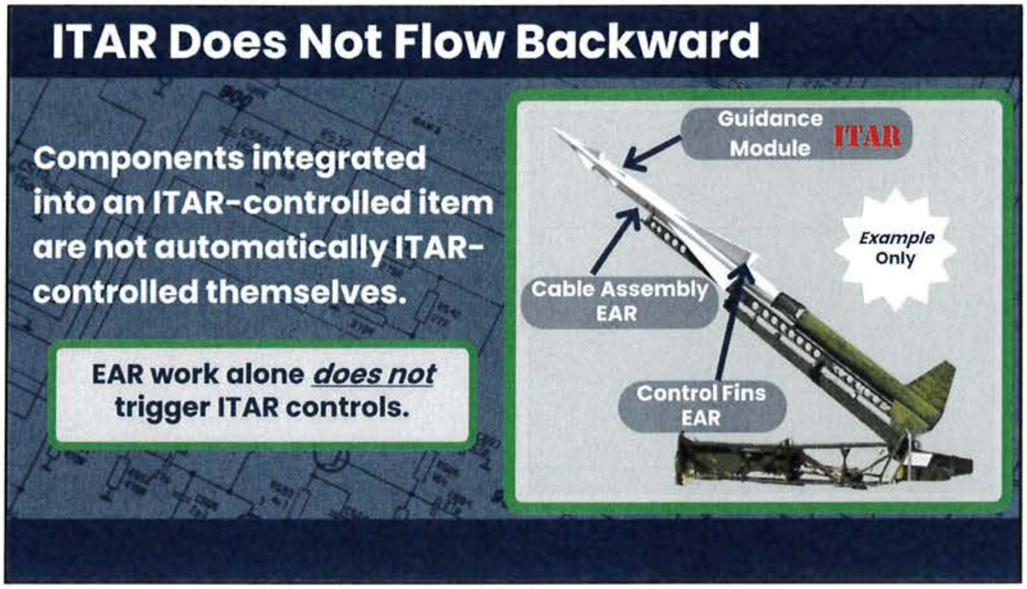
USML Designation: IV(h)(29)

Specially designed
Military-grade connector for guided missile

Designed for a specific military application

Now here's an example of a "specially designed" entry in the USML. We're revisiting the connector cable from earlier—but this time, we're looking at how it's categorized under the regulation. You'll see it falls under Category IV, subparagraph (h), which covers systems, parts, components, and accessories. Specifically, it's captured under paragraph (29)—which addresses electrical connectors specially designed for use in rockets or missiles.
Here's the key point:
Because the end item—the missile—is enumerated in paragraph (a)(1), and this connector is specially designed for that item, it too becomes ITAR-controlled.

That's why its USML designation is **IV(h)(29).** Even though this is a subcomponent, and might look like a generic part, it's the military-specific design and application that bring it under ITAR. So again, it's not just about what something is—it's about what it's designed for.



ITAR Does Not Flow Backward

Components integrated into an ITAR-controlled item are not automatically ITAR-controlled themselves.

EAR work alone *does not* trigger ITAR controls.

Guidance Module ITAR
Example Only
Cable Assembly EAR
Control Fins EAR

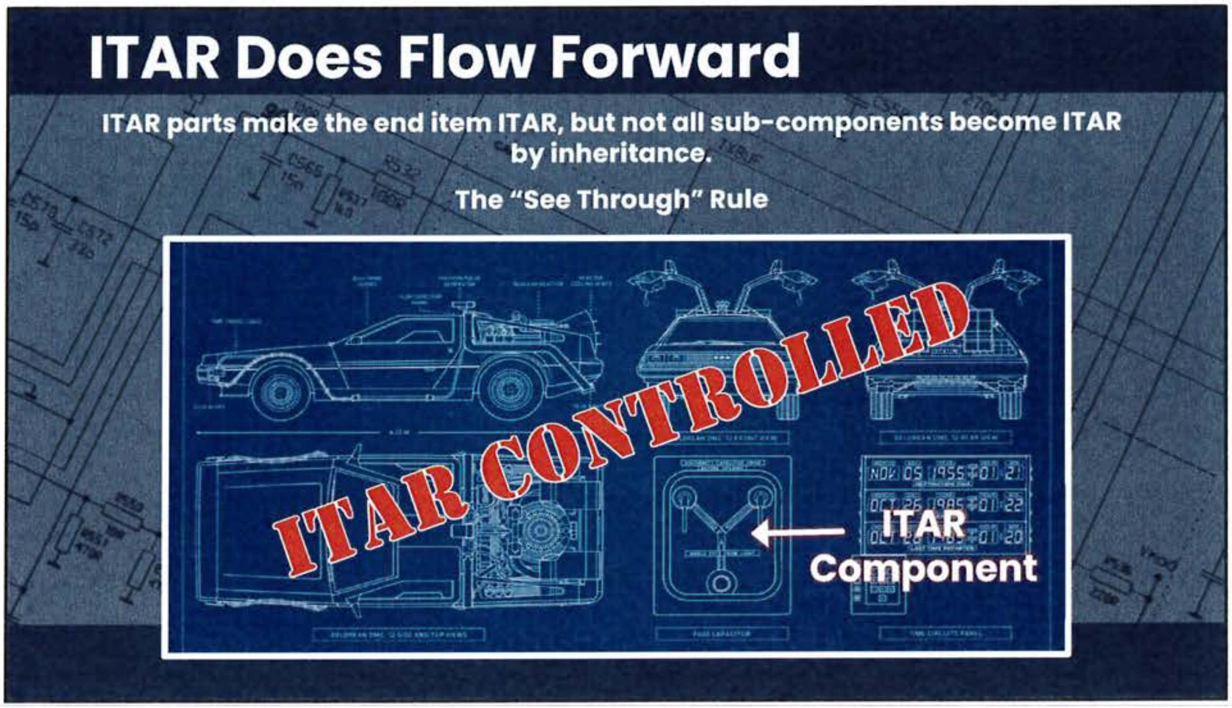
We should always remember that ITAR end items are often made up of subcomponents that are not themselves ITAR-controlled. Let's continue with our missile example. A guided missile might contain hundreds or thousands of components. Some of them—like a guidance module—might be explicitly enumerated in the USML, making them clearly ITAR-controlled.

But other components—like a commercially available cable assembly or control fins that are also used in commercial rockets—may not be specially designed or explicitly listed in the USML. In those cases, those parts would not be captured under the ITAR. Instead, they would fall under the EAR, and we'd review the Commerce Control List (CCL) to determine their classification and any applicable controls.

So, if a manufacturer is asked to produce only the cable assembly or only the fins, they're working with an EAR-controlled item, even if it will eventually be integrated into an ITAR-controlled missile.

This distinction matters. Just because a part is going into an ITAR end item doesn't mean it's ITAR itself. ITAR doesn't flow backward. Now, let me add an important caveat: If we are given technical data—like schematics, drawings, or BOMs—that includes ITAR-controlled components, then that data is ITAR-controlled, even if we are only manufacturing the EAR-controlled portion. We are still legally obligated to protect that information according to ITAR standards. That's why it's so important to understand:

- Exactly what you're building
- What regulation applies
- And how to properly protect the associated data



ITAR Does Flow Forward

ITAR parts make the end item ITAR, but not all sub-components become ITAR by inheritance.

The "See Through" Rule

ITAR CONTROLLED

ITAR Component

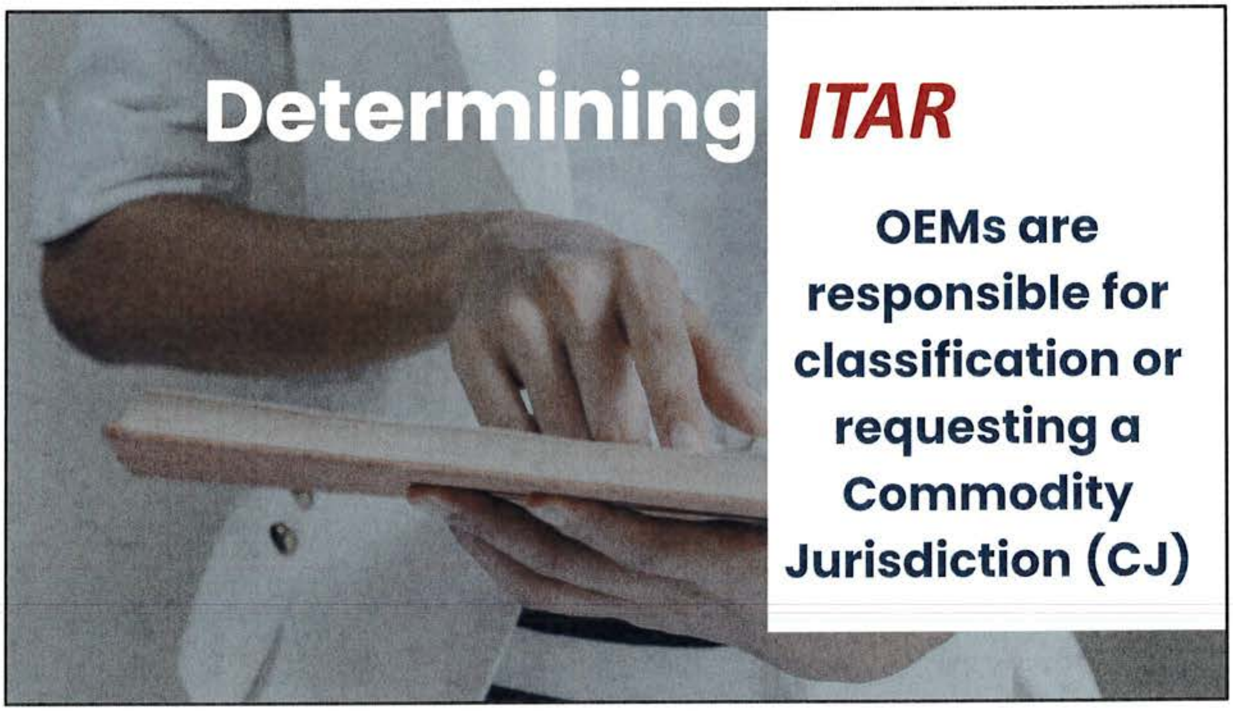
So while ITAR doesn't flow backward, it does flow forward. This means that if an item contains an ITAR-controlled part, component, or assembly, then the entire end-item becomes ITAR-controlled—even if the rest of the system wouldn't normally be.

This is known as the "see-through" rule. The purpose of the see-through rule is to prevent companies from trying to obscure or embed ITAR components into larger, uncontrolled assemblies in an attempt to sidestep the regulations.

Let's illustrate this with a fun example:
Here we have a DeLorean—a commercially available vehicle, (at least at one point). As originally built, the DeLorean would be EAR-controlled—just a standard car. But if we were to install an ITAR-controlled "flux capacitor" into this vehicle...[click]

Well, now the entire vehicle becomes ITAR-controlled—because it contains a critical defense component that falls under the USML. [click]

This principle applies even if the controlled component is just a small part of the overall system. Once an ITAR-controlled component is embedded, the entire end-item inherits that control. That's the see-through rule in action—and it's a key concept for engineers, program managers, and anyone classifying hardware.



Determining *ITAR*

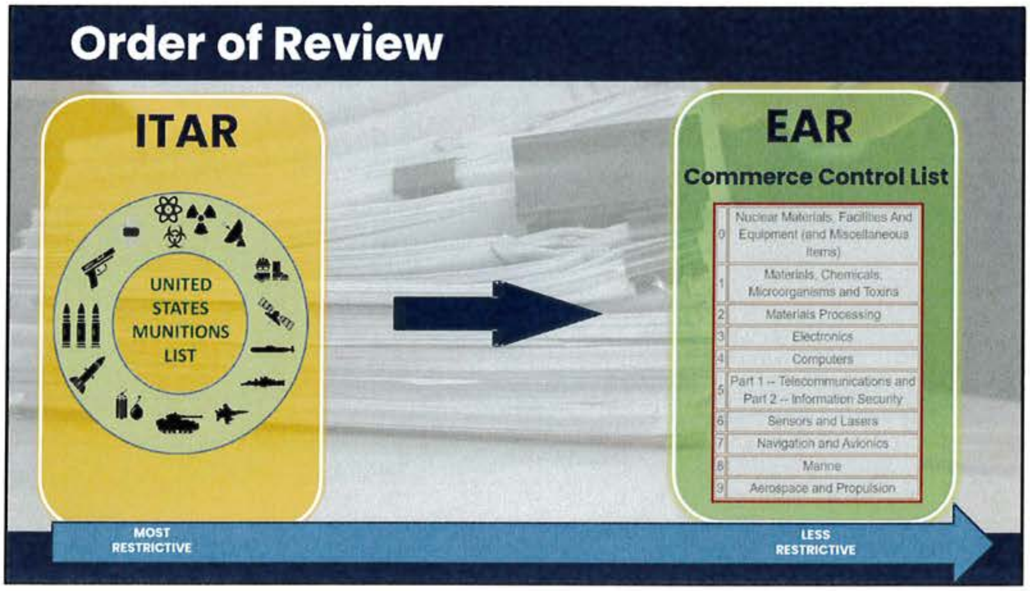
OEMs are responsible for classification or requesting a Commodity Jurisdiction (CJ)

Original Equipment Manufacturers (OEMs) are responsible for making classification determinations—or for requesting the government to classify an item on their behalf.

Because classification requires a deep understanding of the item's technical details, OEMs and designers are in the best position to provide the necessary information for an accurate determination. [click]

Even when the government is asked to make a ruling—through a Commodity Jurisdiction (CJ) request with the State Department or a CCATS request with the Commerce Department—the applicant still must provide sufficient technical detail for a decision to be made.

Both the State Department and the Commerce Department offer this service, and their decisions are considered binding and final unless formally appealed.



Order of Review

ITAR

UNITED STATES MUNITIONS LIST

EAR

Commerce Control List

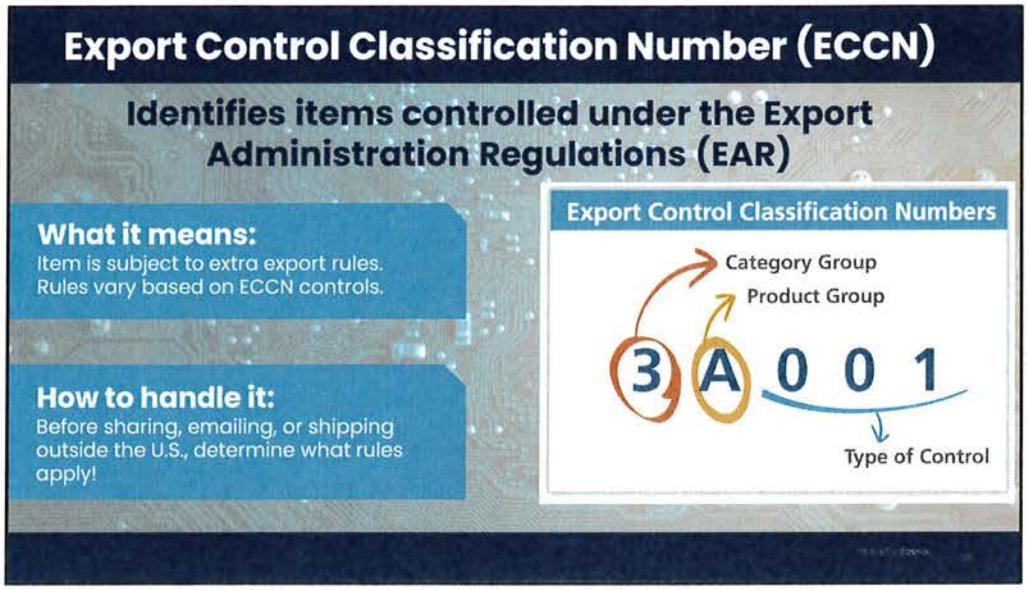
0	Nuclear Materials, Facilities And Equipment (and Miscellaneous Items)
1	Materials, Chemicals, Microorganisms and Toxins
2	Materials Processing
3	Electronics
4	Computers
5	Part 1 -- Telecommunications and Part 2 -- Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

MOST RESTRICTIVE

LESS RESTRICTIVE

Let's go back to the Order of Review. Remember, the ITAR is always the first stop to see if an item is captured by this regulation. If it isn't then the EAR, and specifically the Commerce Control List or CCL, would be the next stop. So let's now open up that regulation and see how it's organized and how it functions.

The CCL is divided into 10 main classification areas. These can also get very detailed, very quickly. Again, the CCL is a very expansive document.



Export Control Classification Number (ECCN)

Identifies items controlled under the Export Administration Regulations (EAR)

What it means:
Item is subject to extra export rules. Rules vary based on ECCN controls.

How to handle it:
Before sharing, emailing, or shipping outside the U.S., determine what rules apply!

Export Control Classification Numbers

Category Group

Product Group

3 A 0 0 1

Type of Control

Why it matters:

It helps determine if an item requires an export license, which is needed for certain goods, software, or technology when exported from the US.

How it works:

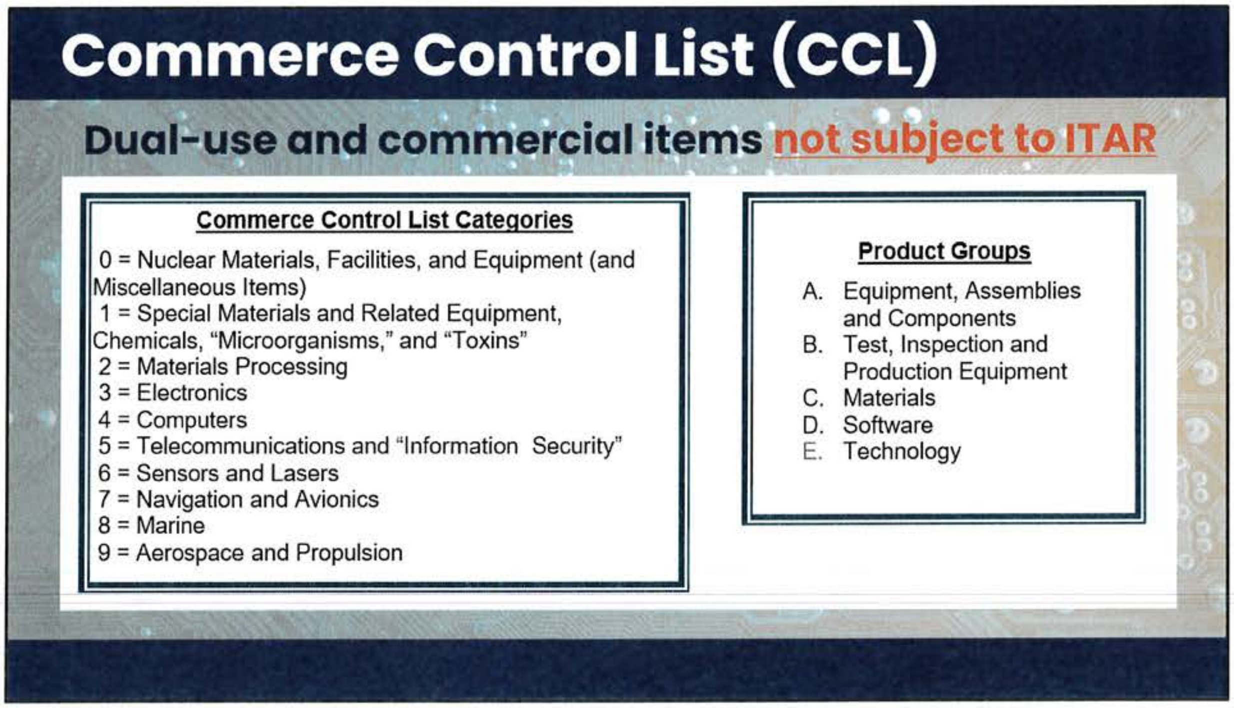
The ECCN categorizes items based on their type, technology, or software and its technical parameters.

Structure:

The first character is a number indicating the broad category (e.g., Electronics, Nuclear, etc.).

The second character is a letter indicating the product group (e.g., Equipment, Software, Technology).

The last three characters are numbers that further specify the item.



Commerce Control List (CCL)

Dual-use and commercial items not subject to ITAR

Commerce Control List Categories

0 = Nuclear Materials, Facilities, and Equipment (and Miscellaneous Items)
1 = Special Materials and Related Equipment, Chemicals, "Microorganisms," and "Toxins"
2 = Materials Processing
3 = Electronics
4 = Computers
5 = Telecommunications and "Information Security"
6 = Sensors and Lasers
7 = Navigation and Avionics
8 = Marine
9 = Aerospace and Propulsion

Product Groups

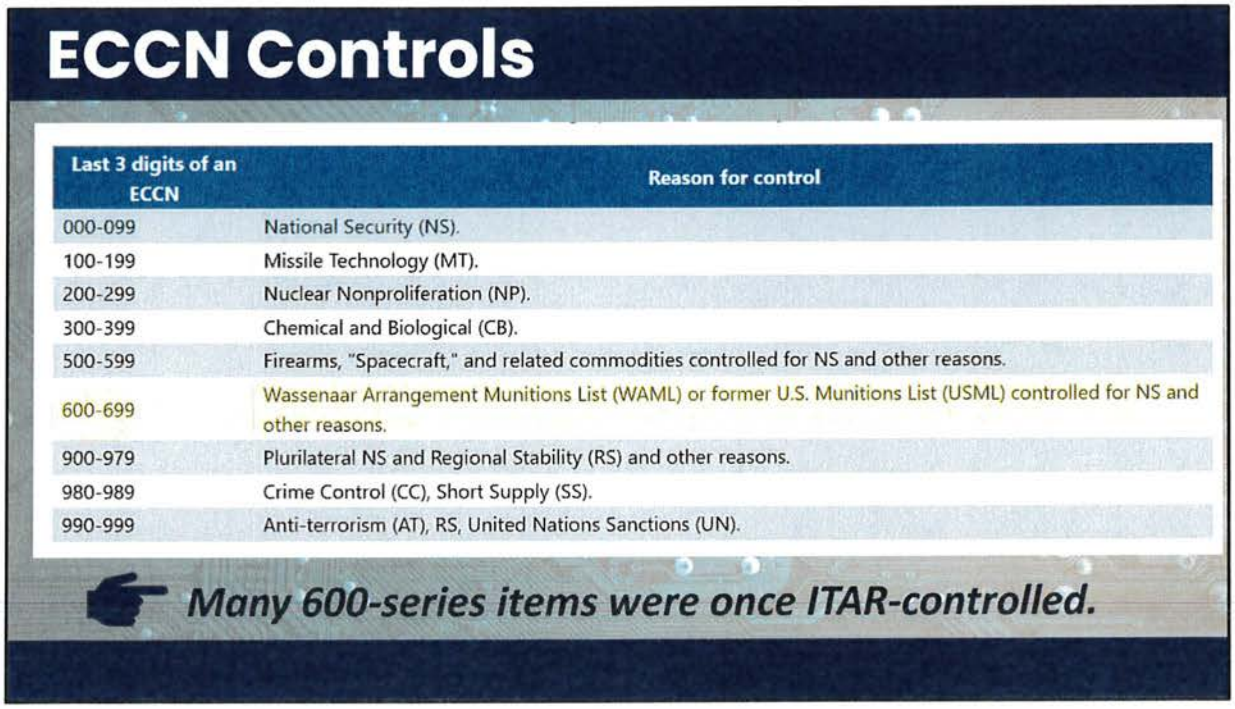
A. Equipment, Assemblies and Components
B. Test, Inspection and Production Equipment
C. Materials
D. Software
E. Technology

The EAR further organizes these categories into specific Product Groups, which you can see here.

Remember, the EAR covers a broad range of items—dual-use, commercial, and some less-sensitive military goods. Because of this broad scope, the EAR is a much larger and more complex regulation than the ITAR.

Most items traded globally—especially those not strictly military—fall under the EAR.

One last key point:
When determining export controls, the EAR is always the second source you check. If an item isn't found on the ITAR's USML, then we review the EAR to see if it's controlled.



ECCN Controls

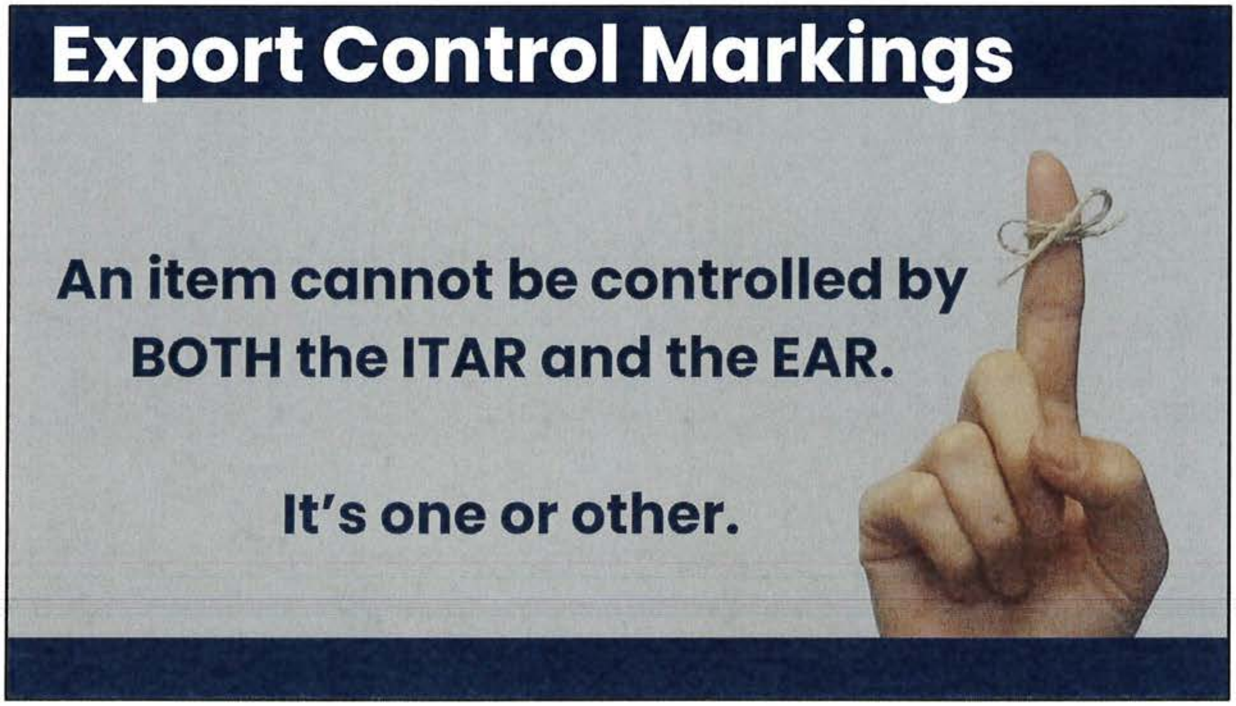
Last 3 digits of an ECCN	Reason for control
000-099	National Security (NS).
100-199	Missile Technology (MT).
200-299	Nuclear Nonproliferation (NP).
300-399	Chemical and Biological (CB).
500-599	Firearms, "Spacecraft," and related commodities controlled for NS and other reasons.
600-699	Wassenaar Arrangement Munitions List (WAML) or former U.S. Munitions List (USML) controlled for NS and other reasons.
900-979	Plurilateral NS and Regional Stability (RS) and other reasons.
980-989	Crime Control (CC), Short Supply (SS).
990-999	Anti-terrorism (AT), RS, United Nations Sanctions (UN).

☛ ***Many 600-series items were once ITAR-controlled.***

The last part of an ECCN is the reason for control—this three-letter code tells you why a commodity is regulated (for example, National Security, Anti-Terrorism, or Regional Stability).

You'll also see some ECCNs in the 600-series. These are military-related items that were once ITAR-controlled but have moved to the EAR, or they're governed by international agreements like the Wassenaar Arrangement.

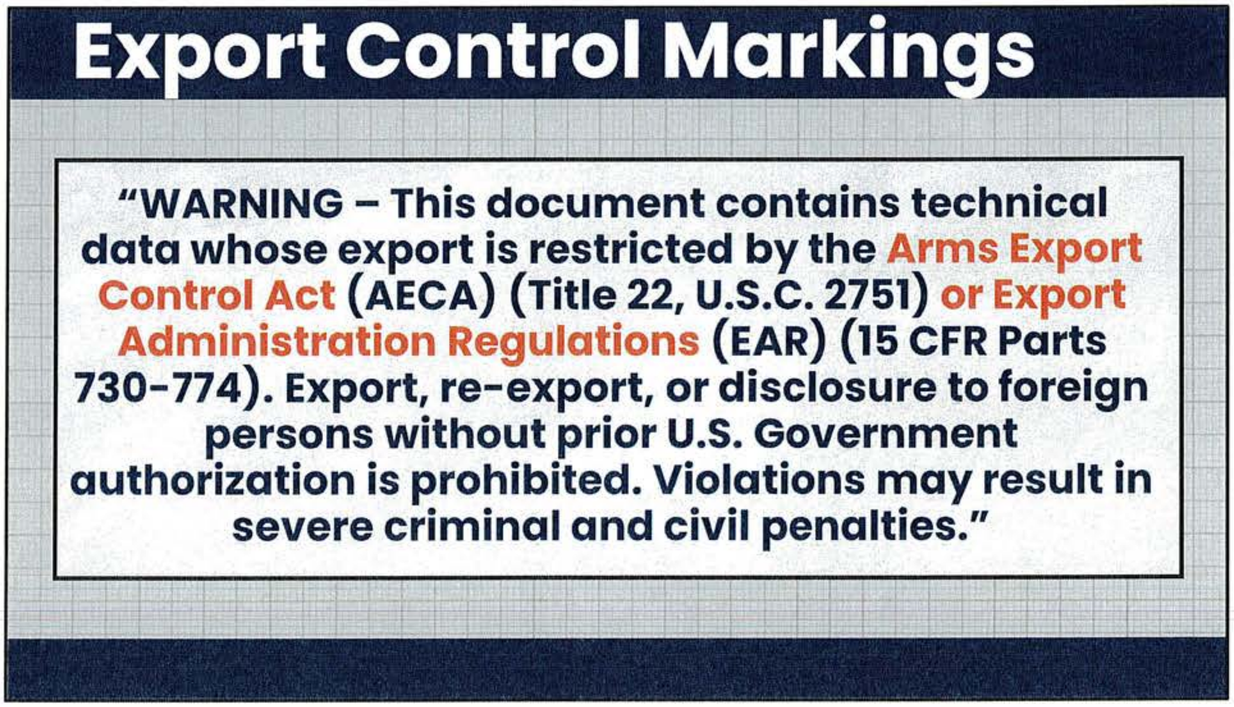
It's important to note:
Some technology gets moved from the USML to the CCL—typically into the 600-series.
That means you might find some defense and military items covered under the EAR, not the ITAR.
Generally, these items are a bit easier to handle and transfer because the EAR is less restrictive.



Export Control Markings

An item cannot be controlled by BOTH the ITAR and the EAR.

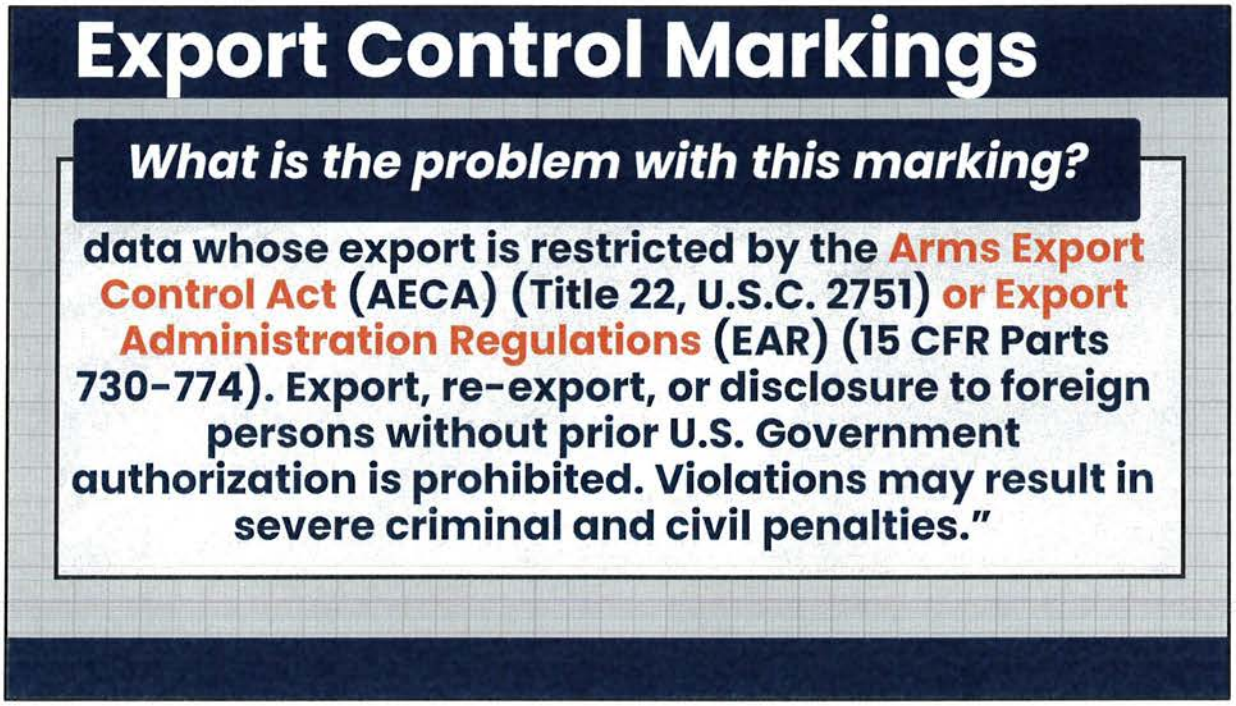
It's one or other.



Export Control Markings

"WARNING – This document contains technical data whose export is restricted by the Arms Export Control Act (AECA) (Title 22, U.S.C. 2751) or Export Administration Regulations (EAR) (15 CFR Parts 730-774). Export, re-export, or disclosure to foreign persons without prior U.S. Government authorization is prohibited. Violations may result in severe criminal and civil penalties."

This is a real-world example of a common marking. You might see something like this on a schematic, a BOM, or other technical documentation. I've highlighted the relevant areas in red.

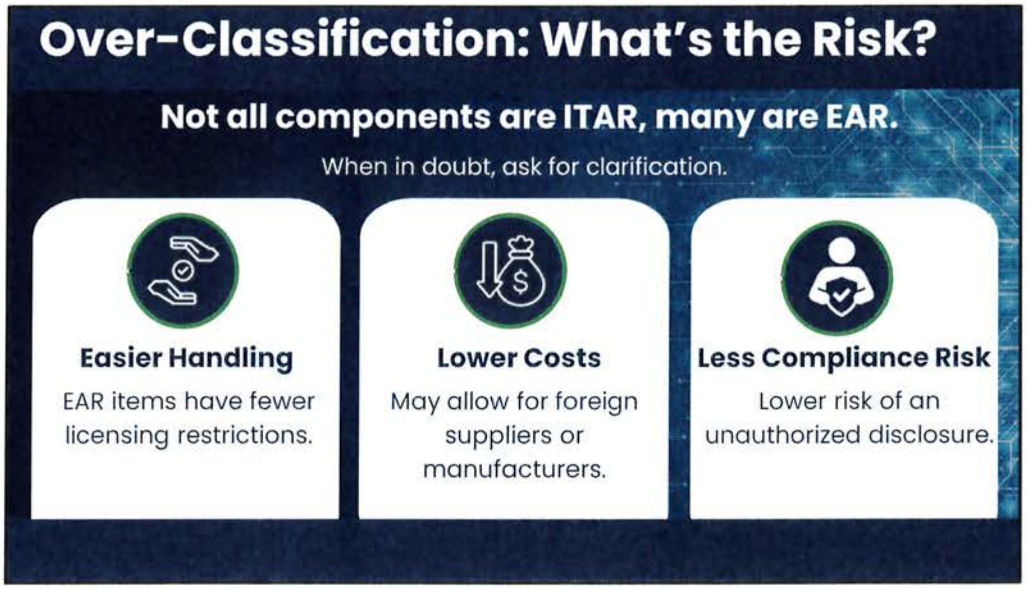


Export Control Markings

What is the problem with this marking?

data whose export is restricted by the Arms Export Control Act (AECA) (Title 22, U.S.C. 2751) or Export Administration Regulations (EAR) (15 CFR Parts 730-774). Export, re-export, or disclosure to foreign persons without prior U.S. Government authorization is prohibited. Violations may result in severe criminal and civil penalties."

The problem is it calls out BOTH the ITAR (ACEA) and the EAR. An item cannot be controlled by both regulations. It's one or the other.



Over-Classification: What's the Risk?

Not all components are ITAR, many are EAR.

When in doubt, ask for clarification.

Easier Handling

EAR items have fewer licensing restrictions.

Lower Costs

May allow for foreign suppliers or manufacturers.

Less Compliance Risk

Lower risk of an unauthorized disclosure.

One issue we encounter regularly is customers marking all their drawings and documents as "ITAR-Controlled."

While sometimes that's accurate, often it's just easier for customers to stamp everything with the ITAR label—even when not all the items actually require it. But over-classifying creates problems. As we discussed earlier, many ITAR-controlled end items are actually built from parts and components that fall under the EAR.

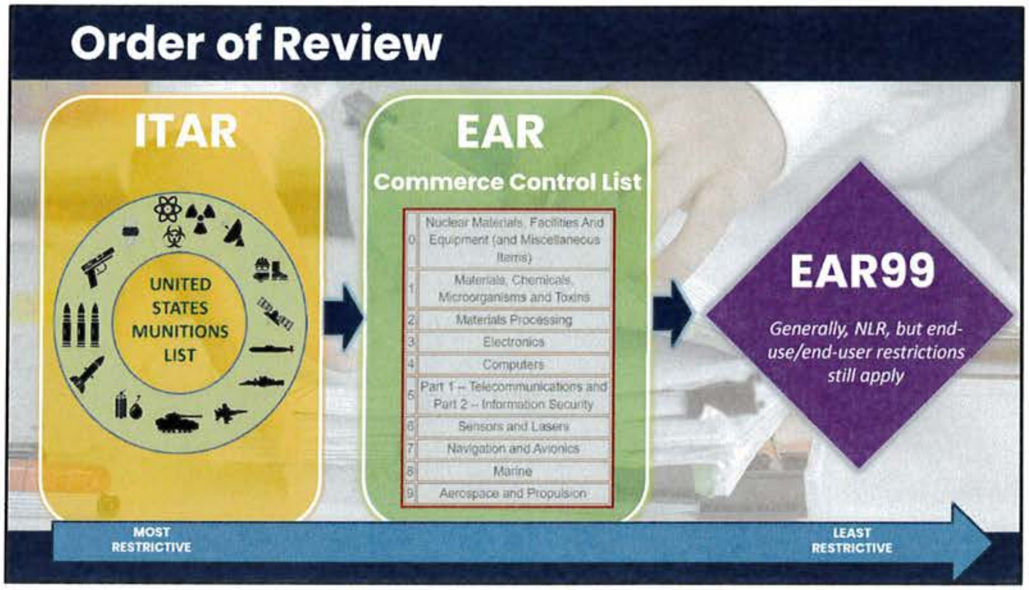
If customers made more accurate classification decisions, it could make things easier for everyone: [click]

EAR-controlled items are easier to handle and store because licensing is less strict.[click]

For EAR-controlled parts, SMTC may be able to use foreign suppliers or manufacturers, which can sometimes be less expensive than ITAR-registered U.S. sources. This can help reduce costs for both us and our customers. [click]

Finally, there's less compliance risk for SMTC when EAR items are handled under the correct rules.

That's why, whenever you have doubts about a marking or classification, it's important to diplomatically and respectfully ask the customer for clarification or more detailed information. In the end, proper classification benefits everyone—the customer, your company, and the integrity of our compliance program.



Order of Review

ITAR

UNITED STATES MUNITIONS LIST

EAR

Commerce Control List

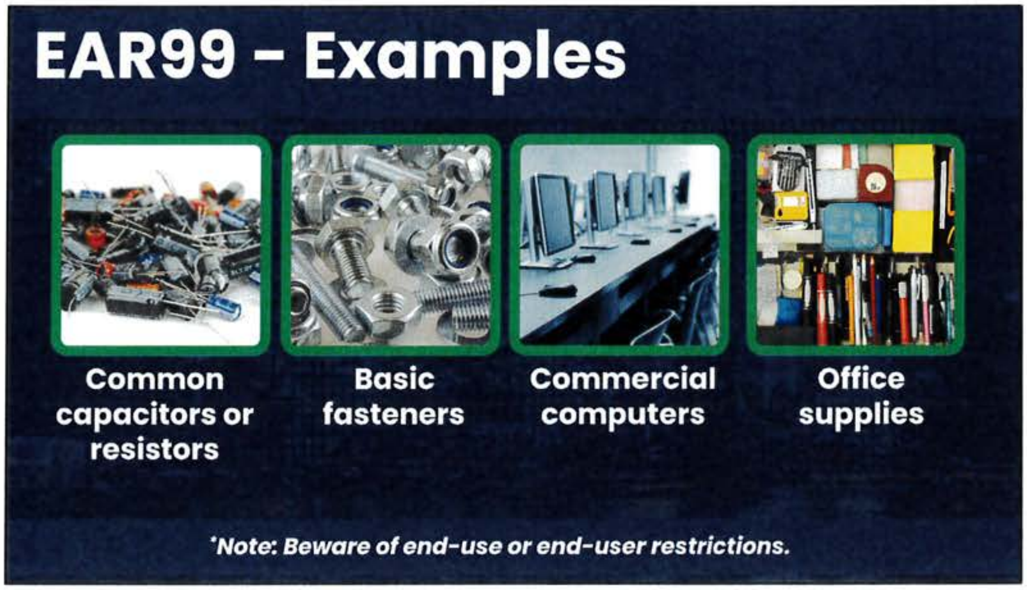
0	Nuclear Materials, Facilities And Equipment (and Miscellaneous Items)
1	Materials, Chemicals, Microorganisms and Toxins
2	Materials Processing
3	Electronics
4	Computers
5	Part 1 -- Telecommunications and Part 2 -- Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

EAR99

Generally, NLR, but end-use/end-user restrictions still apply

MOST RESTRICTIVE

LEAST RESTRICTIVE



EAR99 - Examples

Common capacitors or resistors

Basic fasteners

Commercial computers

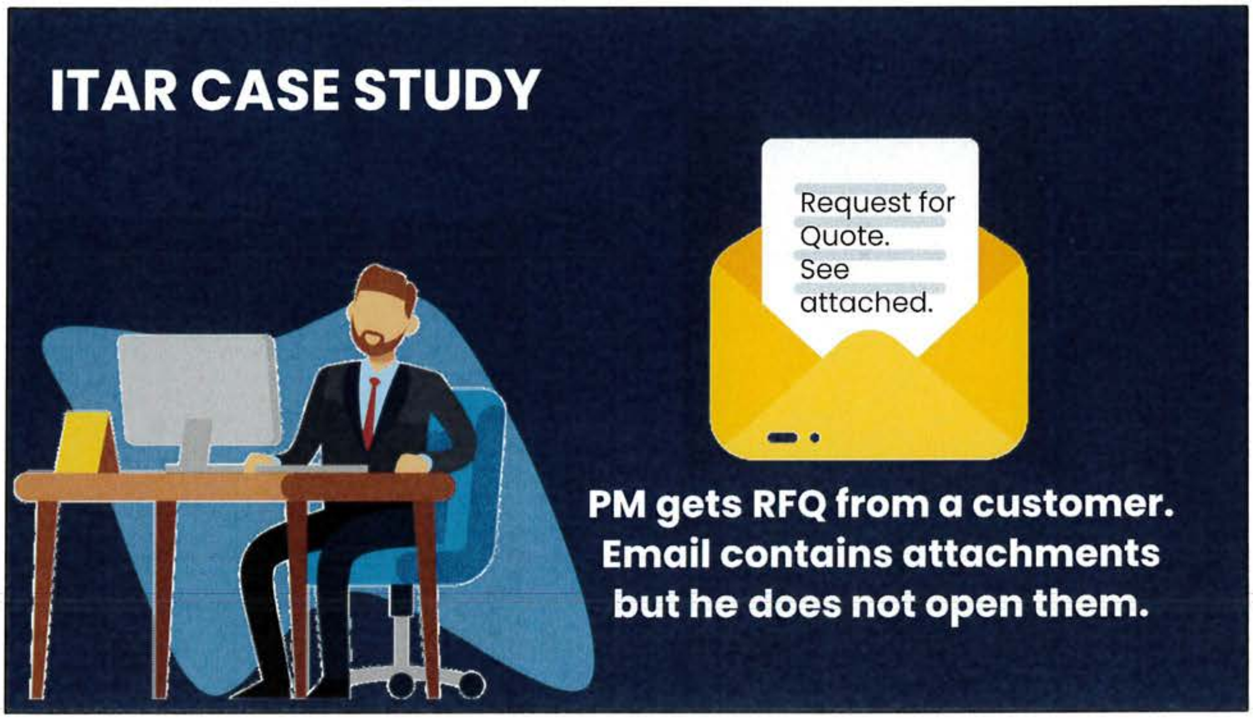
Office supplies

**Note: Beware of end-use or end-user restrictions.*

Here are some examples of common EAR99 products you might see at your company.
This isn't a complete list, but it gives you a sense of the kinds of items that typically fall under EAR99.

These products are much easier to source and work with because they have fewer restrictions.

But remember: "fewer restrictions" doesn't mean no restrictions.
Let's talk about situations where an EAR99 item may still require a license.



ITAR CASE STUDY

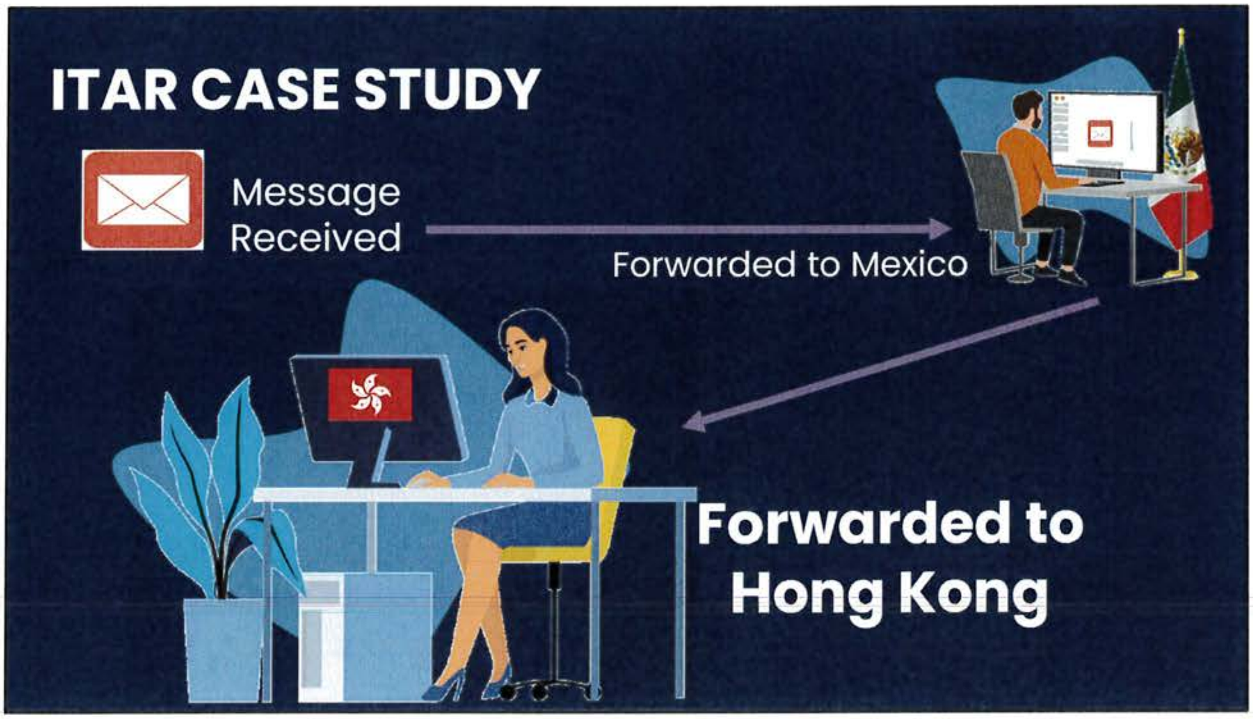
PM gets RFQ from a customer. Email contains attachments but he does not open them.

In this case, we had a complete lack of awareness of how to properly handle ITAR-controlled training. One of our program managers received a request for a quote from a customer and rather than reviewing the attachments first, he forwarded them on to our commercial quoting team in Mexico. That team started to work on the quote and additionally forwarded it to Hong Kong for assistance. The next workday the PM realized the documents were marked as Export Controlled and immediately called the FSO. While we did our best to recall the messages and mitigate the damage, because foreign nationals had already been exposed to the information, we had an obligation to report this to the government. It just proves how quickly a simple lack of awareness can escalate.

ITAR CASE STUDY

Message Received

Forwarded to Mexico

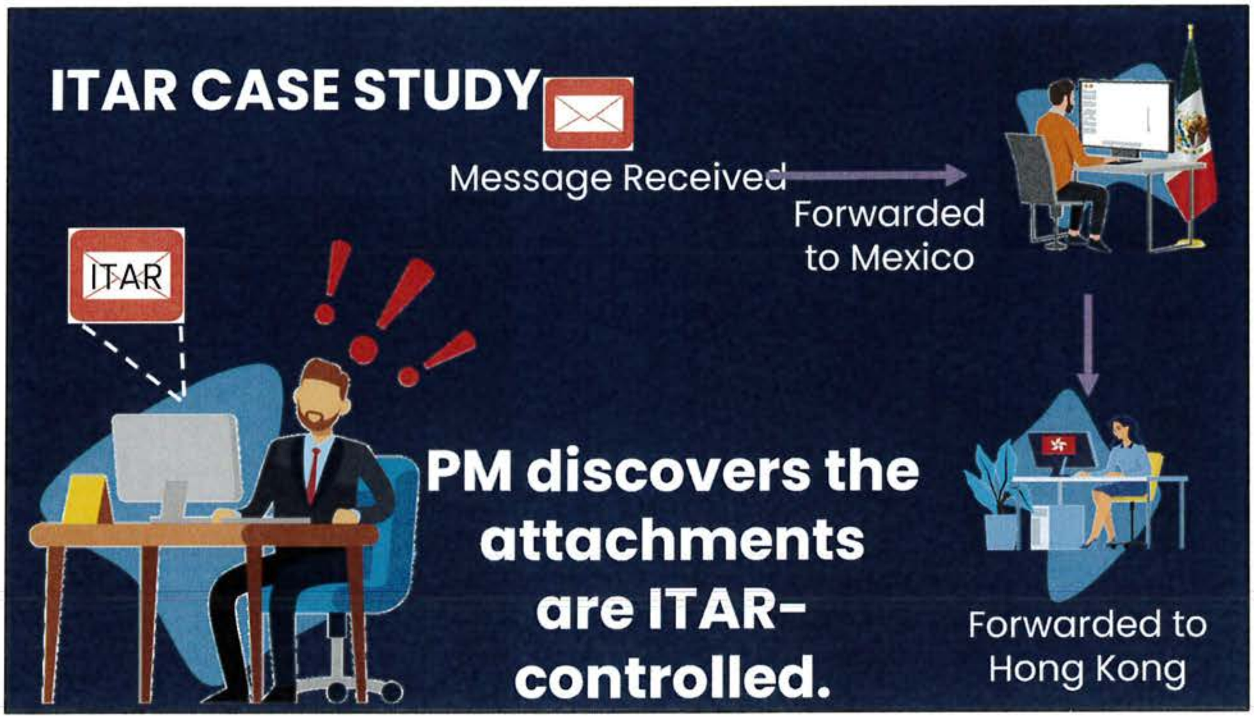


ITAR CASE STUDY

Message Received

Forwarded to Mexico

Forwarded to Hong Kong



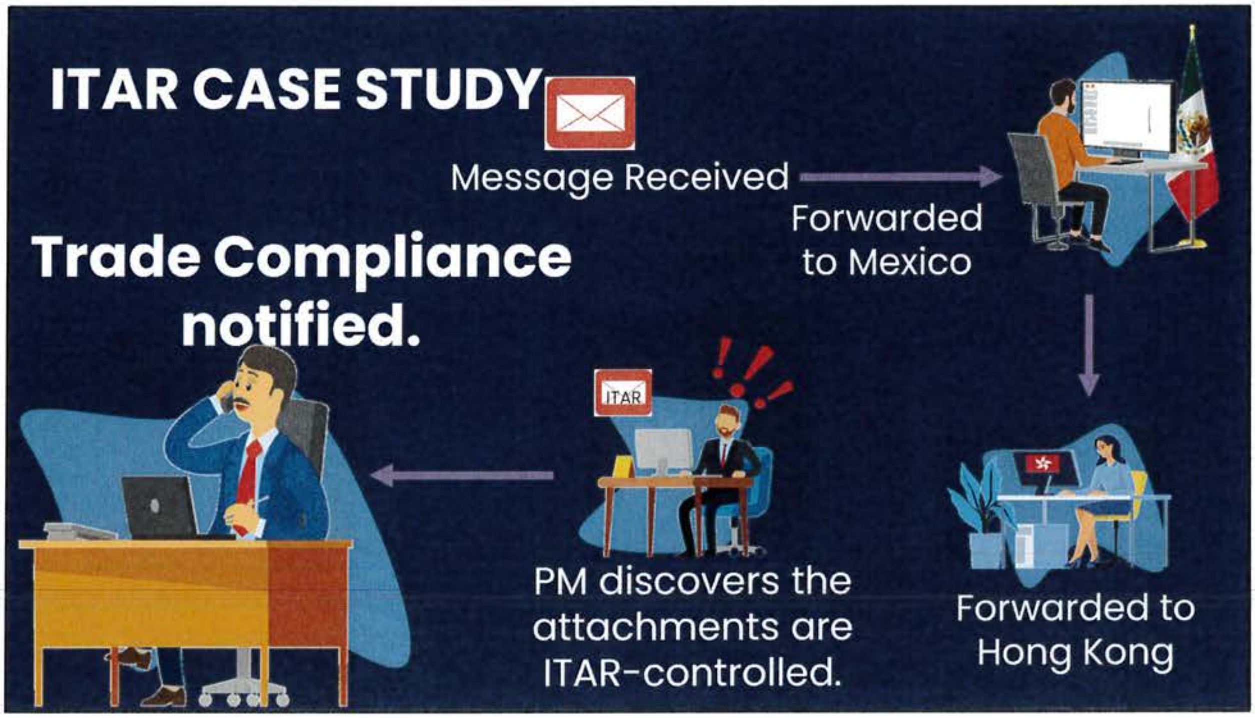
ITAR CASE STUDY

Message Received

Forwarded to Mexico

Forwarded to Hong Kong

PM discovers the attachments are ITAR-controlled.



ITAR CASE STUDY

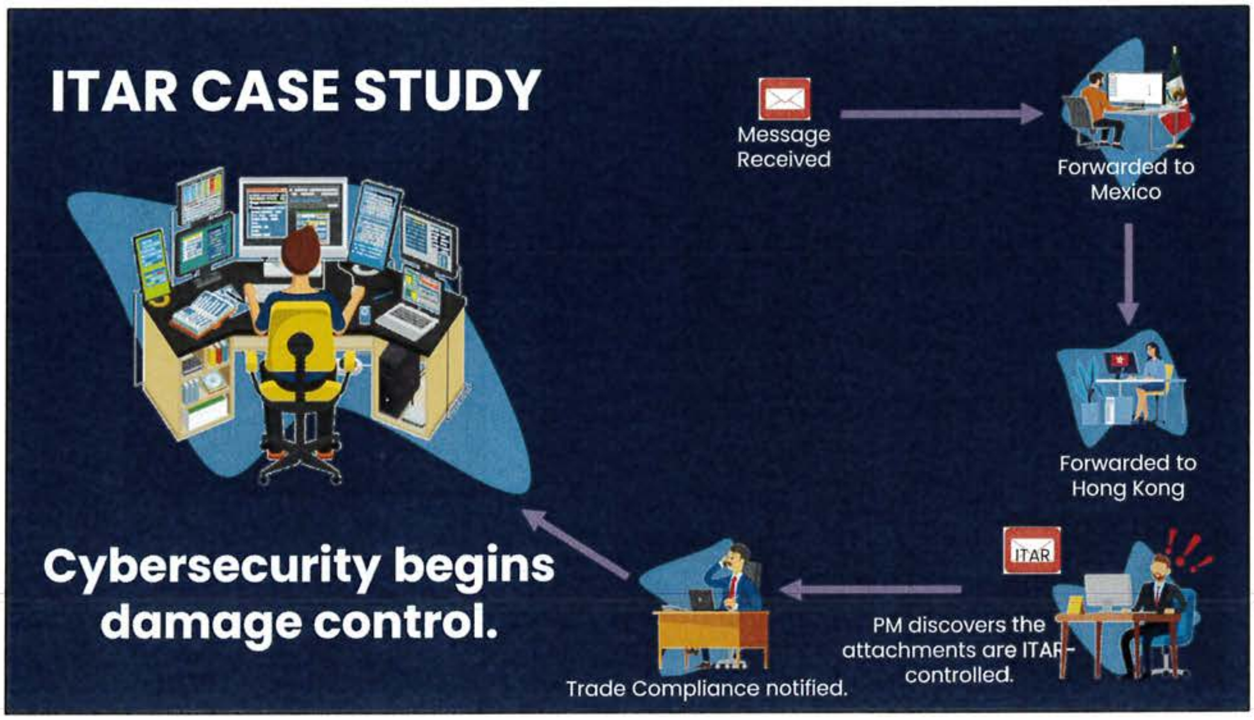
Message Received

Forwarded to Mexico

Forwarded to Hong Kong

PM discovers the attachments are ITAR-controlled.

Trade Compliance notified.



ITAR CASE STUDY

Message Received

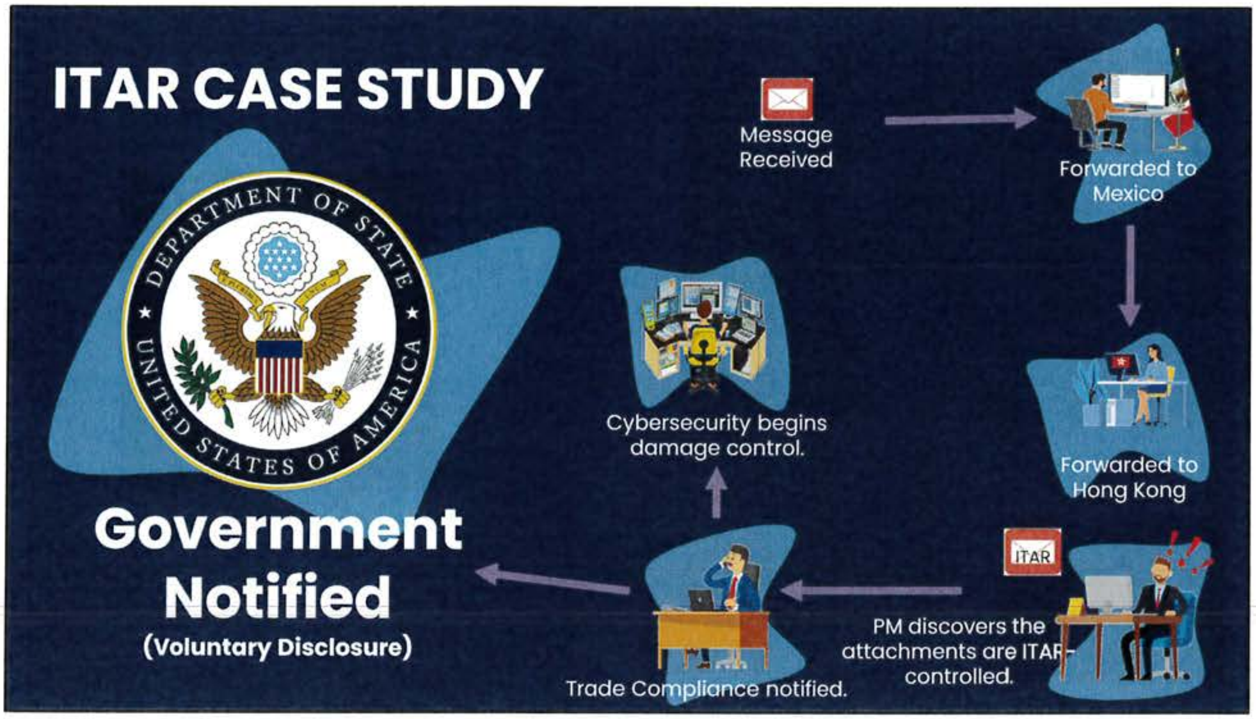
Forwarded to Mexico

Forwarded to Hong Kong

PM discovers the attachments are ITAR-controlled.

Trade Compliance notified.

Cybersecurity begins damage control.



ITAR CASE STUDY

Message Received

Forwarded to Mexico

Forwarded to Hong Kong

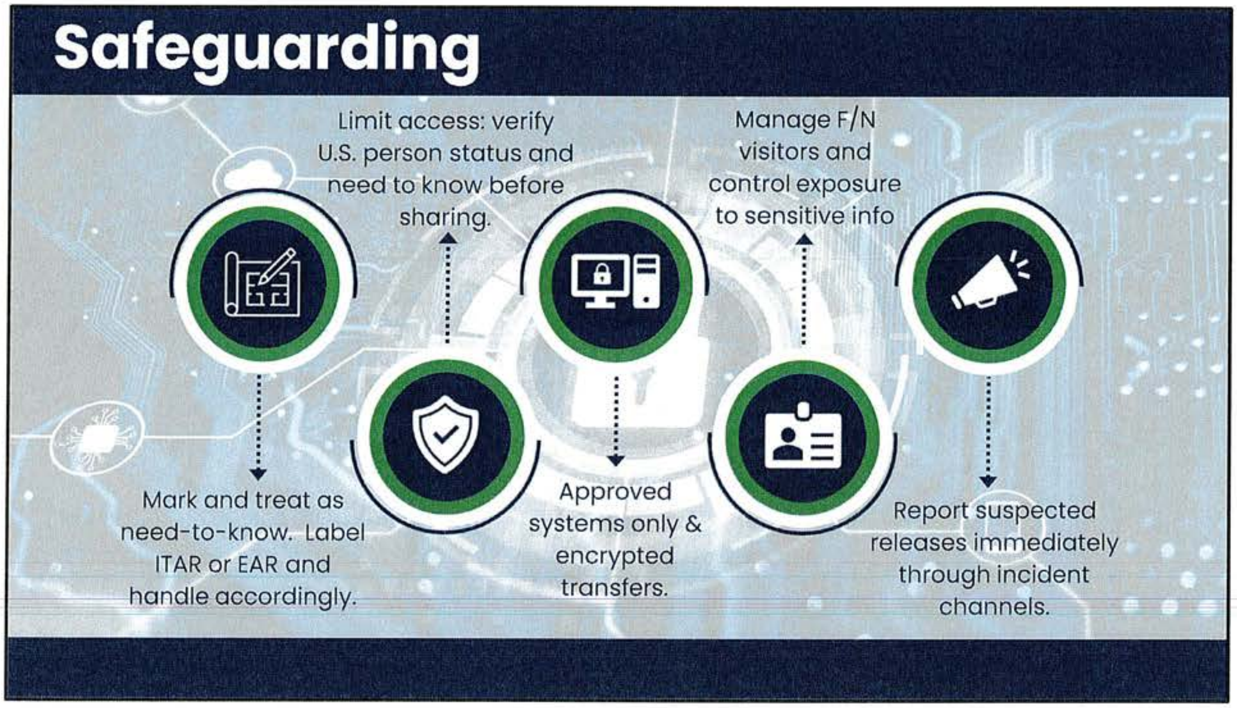
PM discovers the attachments are ITAR-controlled.

Trade Compliance notified.

Cybersecurity begins damage control.

Government Notified

(Voluntary Disclosure)



Safeguarding

Mark and treat as need-to-know. Label ITAR or EAR and handle accordingly.

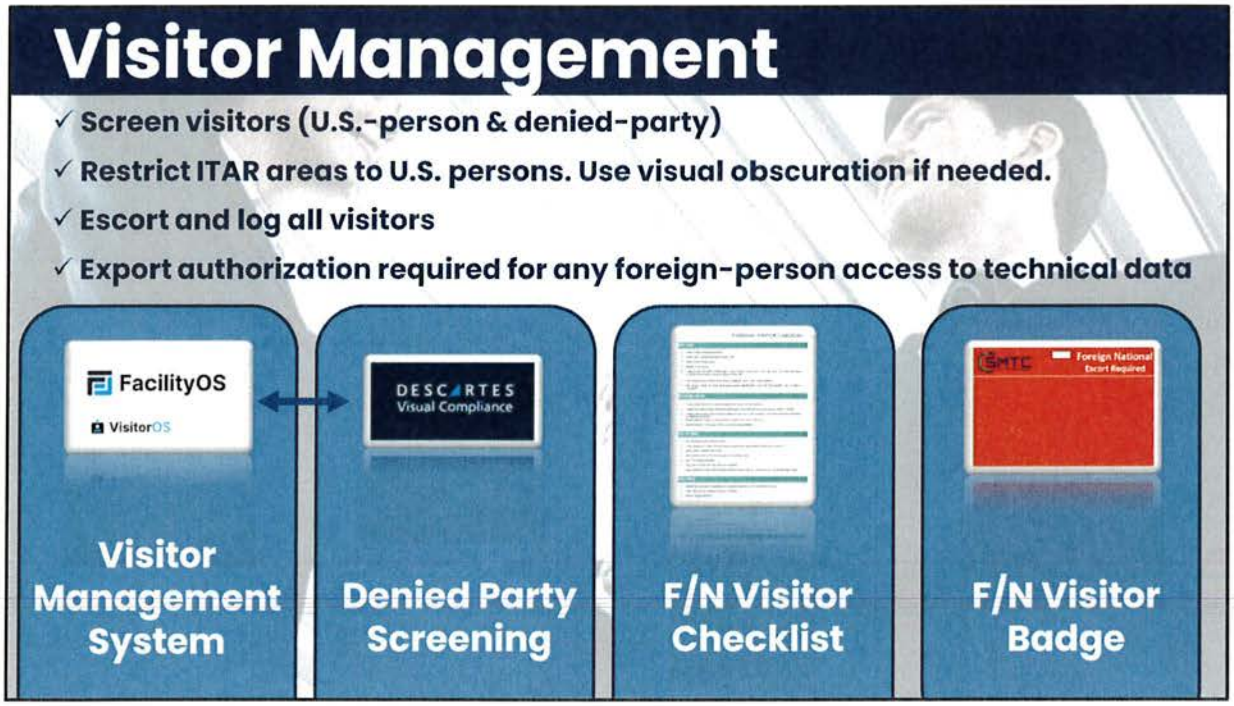
Limit access: verify U.S. person status and need to know before sharing.

Approved systems only & encrypted transfers.

Manage F/N visitors and control exposure to sensitive info

Report suspected releases immediately through incident channels.

Just like with CUI and classified information, export-controlled data and products must also be properly safeguarded against unauthorized disclosure. Primarily this means restricting access to non-U.S. Persons but other rules also govern where and how export-controlled data can be stored, transmitted, etc.



Visitor Management

- ✓ Screen visitors (U.S.-person & denied-party)
- ✓ Restrict ITAR areas to U.S. persons. Use visual obscuration if needed.
- ✓ Escort and log all visitors
- ✓ Export authorization required for any foreign-person access to technical data

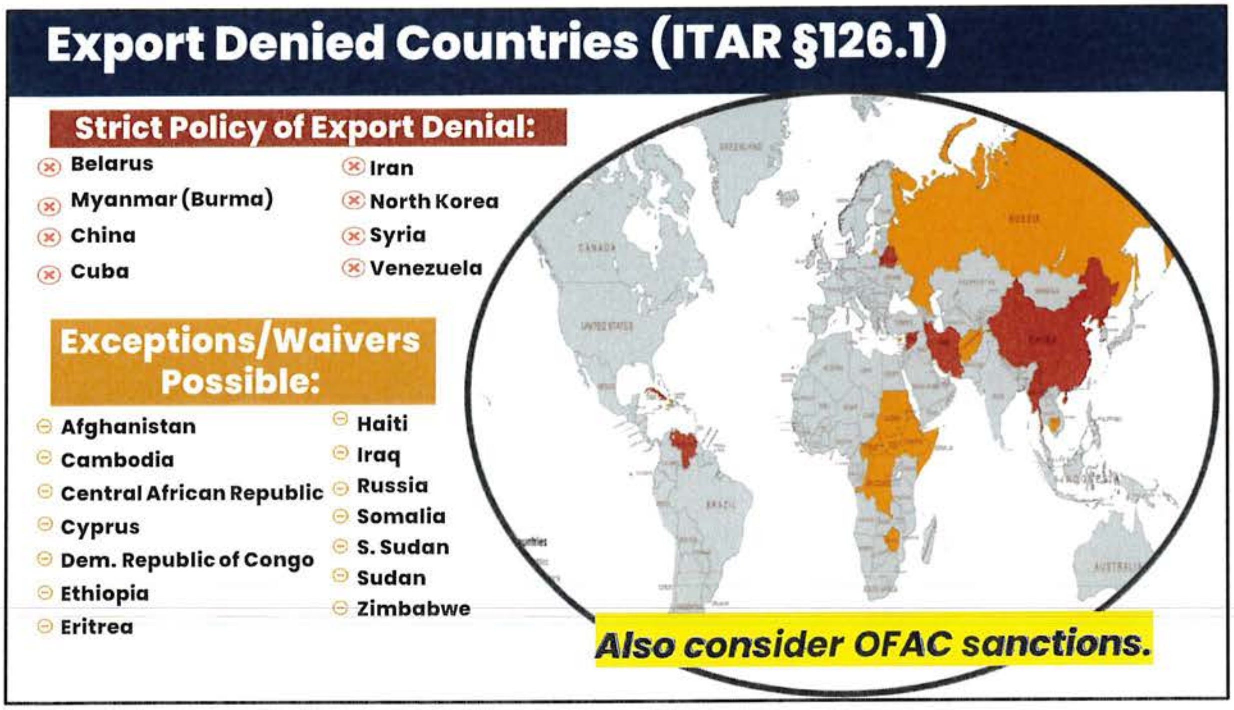
Visitor Management System

Denied Party Screening

F/N Visitor Checklist

F/N Visitor Badge

Controlling visitors—especially foreign nationals—is a core trade-compliance control. We use a visitor management process paired with **automated denied-party screening** so every visitor is checked against U.S. government lists (you can also use the free Consolidated Screening List if you screen manually). Before the visit, run a simple **F/N checklist**: pre-notify hosts, confirm U.S.-person status or escort requirement, pre-walk the route, and **sanitize/obscure** conference rooms and production areas as needed. Day of, **badge and log** all visitors, clearly identify foreign-national badges, and ensure **continuous escort**. Remember: **export authorization is required** for any foreign-person access to **technical data**—screening and escorting do not substitute for authorization.



Export Denied Countries (ITAR §126.1)

Strict Policy of Export Denial:

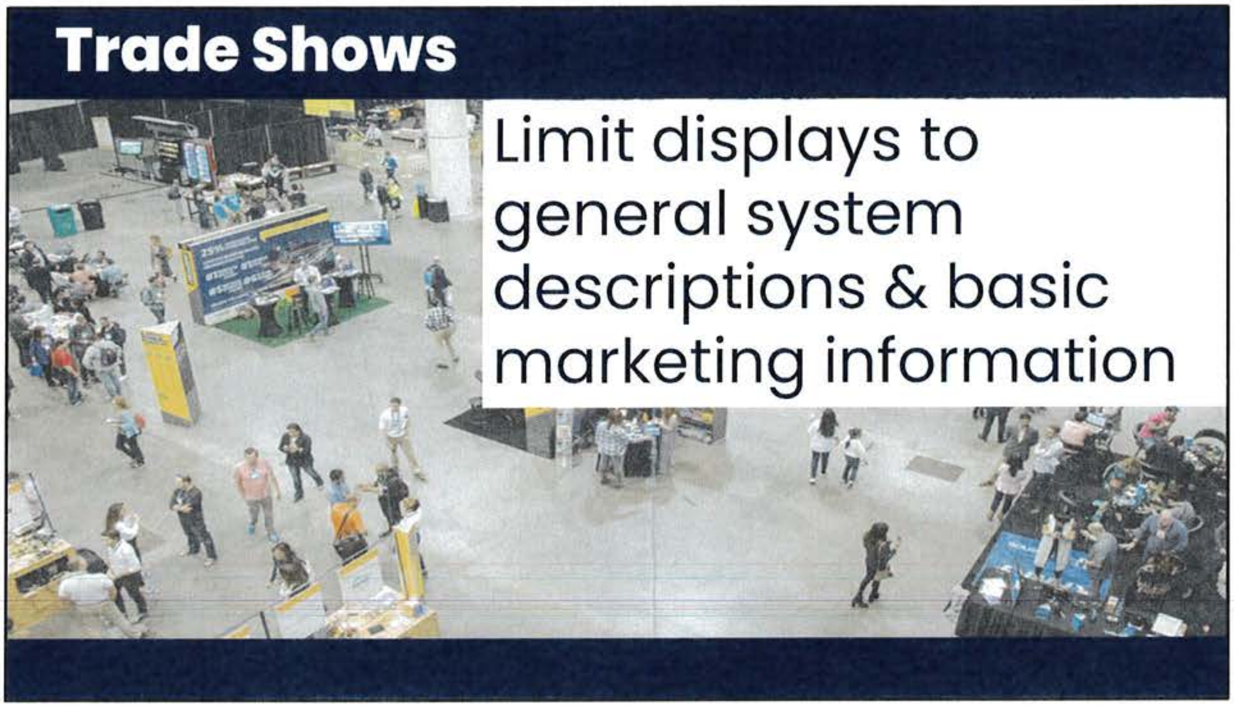
- ⊗ Belarus
- ⊗ Myanmar (Burma)
- ⊗ China
- ⊗ Cuba
- ⊗ Iran
- ⊗ North Korea
- ⊗ Syria
- ⊗ Venezuela

Exceptions/Waivers Possible:

- ⊖ Afghanistan
- ⊖ Cambodia
- ⊖ Central African Republic
- ⊖ Cyprus
- ⊖ Dem. Republic of Congo
- ⊖ Ethiopia
- ⊖ Eritrea
- ⊖ Haiti
- ⊖ Iraq
- ⊖ Russia
- ⊖ Somalia
- ⊖ S. Sudan
- ⊖ Sudan
- ⊖ Zimbabwe

Also consider OFAC sanctions.

ITAR §126.1 lists countries subject to a **policy of denial**—the default answer is **no** for exports, reexports, retransfers, temporary imports, brokering, and releases of **technical data** to their nationals. A small set is absolute denial; others may allow **rare, case-by-case waivers** or specific exemptions, but those require State approval—don't assume they apply. Two practical takeaways: first, **screen every transaction and visitor** against §126.1 and **also check OFAC sanctions**, which can be broader. Second, treat nationality exposure as an export: **no access to controlled hardware or data by §126.1 nationals**—on site or in meetings, calls, portals, or labs—without a State-authorized path. If you think there's a legitimate government purpose or humanitarian carve-out, **pause and escalate** to Trade/Legal for a formal review; do not improvise.



Trade Shows

Limit displays to general system descriptions & basic marketing information

Treat trade shows as public, uncontrolled release environments. Unless it's a U.S.-only, government-controlled venue with written authorization, assume every booth visitor may be a foreign person. Keep content at marketing level only—high-level capabilities and use cases. Do not share drawings, specs or tolerances, performance data, subassembly photos, repair manuals, source code, or anything tied to an ITAR/EAR classification. Pre-clear all slides, brochures, and demos through compliance; no ad-hoc technical deep dives. Train booth staff to deflect: 'We'd need an NDA and export review to discuss that.' Control handouts/USBs, prohibit unvetted samples, and if a visitor is from a §126.1/OFAC country or appears on a screening hit, end the conversation and notify compliance.

Summary

✓ Trade controls protect technology.

✓ Understand Jurisdiction & Classification.

✓ Safeguard export-controlled information.

✓ When in doubt, seek guidance.

1) Trade controls protect technology

"Bottom line: we're protecting controlled *technology and technical data*—on paper, in parts, and in people's heads—from unauthorized foreign-person access or transfers."

2) Understand Jurisdiction & Classification

"Every decision starts here: is it ITAR or EAR, and what's the USML entry or ECCN/EAR99? If we don't know the lane and the label, we can't choose the right authorization or controls."

3) Safeguard export-controlled information

"Apply controls where risk lives—people, places, and packets. Mark clearly, verify U.S.-person status and need-to-know, use approved repositories with encrypted transfers, and control the environment during visits."

4) When in doubt, seek guidance

"Pause and escalate early—classification and access calls are a team sport. Screening and escorting don't replace authorization, and §126.1/OFAC rules can change."

Helpful Resources

The Good, the Bad, and the ITAR. Written in layman's language by a trade-compliance expert. Helpful and easy-to-understand reference. Available via Amazon ~$16

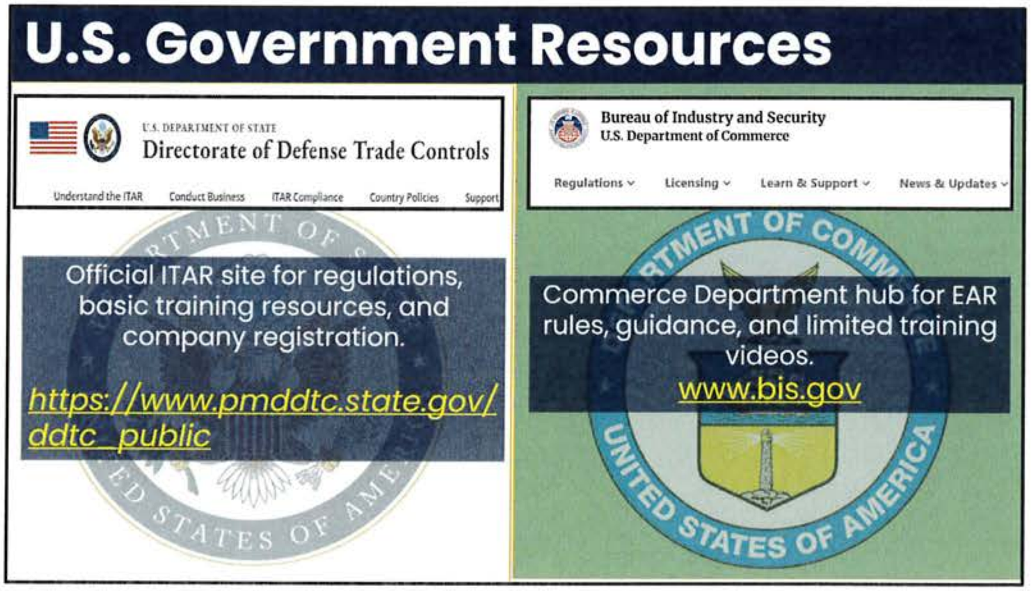
Export Compliance Training Institute (ECTI). Conduct virtual and in-person training seminars. In-depth, comprehensive, and they also offer certifications. www.learnexportcompliance.com

Society for International Affairs (SIA). Helpful resources and publications. Conduct several seminars each year to include "Back-to-Basics" and "Advanced". www.SIAED.org

Partnering for Compliance. Headquartered here in Brevard County, they sponsor seminars and other resources "dedicated to assisting businesses overcome hurdles to trading successfully in the global marketplace." www.partneringforcompliance.org

The Daily Bugle. A daily newsletter from Full Circle Trade Law PLLC emailed to subscribers worldwide to stay informed about the latest amendments of high-tech trade laws, regulations, advice, and world-wide news. https://bartlettpublications.com

U.S. Government Resources

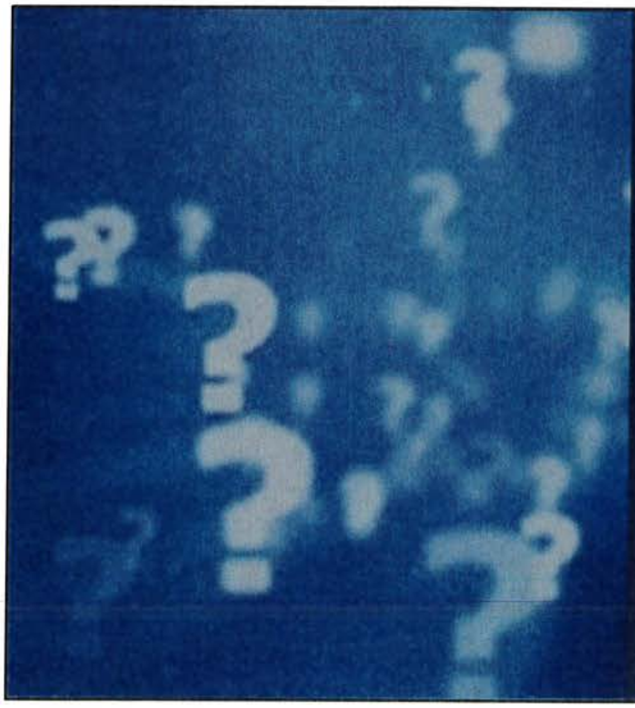


Official ITAR site for regulations, basic training resources, and company registration.

https://www.pmddtc.state.gov/ddtc_public

Commerce Department hub for EAR rules, guidance, and limited training videos.

www.bis.gov



BRAVE AND INTERESTING QUESTIONS?

Charles "Chip" Seifert, CPP®, PSP®
Trade Compliance & Facility Security Officer
(321) 409-4739 (Desk)
(321) 272-7665 (Mobile)
charles.seifert@smtc.com