Helpful References:

- **SMTC ITAR/EAR Compliance Manual** - QP41100
- **Directorate of Defense Trade Controls:** https://www.pmddtc.state.gov/
- **ITAR Regulation**: https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M)
- **Bureau of Industry & Security**: https://www.bis.doc.gov
- **Export Admin Regulation:**
- https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C

Contact Info Here

EXPORT CONTROL HANDBOOK

Your guide to understanding and managing export-controlled information.

Exports Defined

The U.S. government defines an "export" as:

> "**Any** release of technology or source code subject to the EAR or ITAR to a foreign national, even in the United States."

This requires an export license or other official authorization for release. An export can occur in a number of ways. Here are some of the most common:

- **Overheard information** such as on a phone call, presentation, or meeting.
- **Visual inspection of products** on the production floor, drawings, presentations, trade show displays.
- **Email** explanations, information, attachments.
- **Posting information** on public-facing websites, or on networks accessible to a foreign entity.

Currently, SMTC is **not authorized** to release ANY ITAR/EAR information to a foreign national. Therefore if a release occurs, it is a reportable violation to the U.S. government.

Keep these key points in mind regarding export-controlled information and items:

- Keep all digital ITAR data stored on encrypted drives/servers.
- Know which countries are strictly prohibited from receiving ITAR information.
- Notify the FSO of any foreign national visitors ***in advance.***
- Notify Trade Compliance of any suspected ITAR violations ***immediately***!
- ***DO NOT*** Email ITAR information if it is not encrypted.
- If accessing ITAR outside the U.S. ensure you use the SMTC VPN, keep the session private, and ensure data is encrypted. Know what countries are on the "Denied" list.
- It is ***YOUR responsibility*** to verify the citizenship status of personnel with whom you share export-controlled information. You can request written confirmation from their organization.

Destruction

Never throw export-controlled material or documents into the regular trash or recycling. Instead, use of these approved shred bins for disposal of this material.

Locked shred bins are located near the printers/copiers. If you cannot locate a bin, contact the FSO.

Use these for other types of sensitive or proprietary company or customer information as well.

DO NOT put food waste or other similar garbage into these containers and remove all staples and other metal clips.

These bins are serviced monthly and shredded on-site. Notify the FSO if there are containers in need of more frequent servicing.

Identifying Export-Controlled Information

ITAR & EAR material must be marked so users understand it requires protection. Look for markings that look like these, although the wording my vary.

> “WARNING - This document contains information whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) [or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended]. Violations of these export laws are subject to severe criminal penalties.”

> "Export of this material is restricted by the Arms Export Control Act (Title 22, U.S.C. Sec. 2751 et seq.) [or the Export Administration Act of 1979, as amended Title 50 U.S.C., App 2401, et seq.]. Diversion contrary to U.S. law is prohibited and is subject to severe criminal penalties."

> "This equipment is subject to the Arms Export Control Act (Title 22, U.S.C. Sec. 2751 et seq.) [or the Export Administration Act of 1979, as amended Title 50 U.S.C., App 2401, et seq.]. Diversion contrary to U.S. law is prohibited and is subject to severe criminal penalties."

Clarify with the sender/originator if there are any doubts or concerns.

*Review **COMPANY POLICY** for additional information.*

Foreign National

A "foreign national" is a NON U.S. Person.

Foreign Nationals/Entities are barred from accessing or possessing ITAR/EAR information without explicit authorization via an export license or similar government approval.

A "**U.S. Person**" is one of the following:

- U.S. Citizen (native born or naturalized)
- Lawful Permanent Resident (also called a "Green Card Holder")

"**Foreign Entity**" can be :

- Foreign company not incorporated to do business in the United States
- International organizations
- Foreign governments
- Any agency or subdivision of foreign governments (e.g., diplomatic missions)

Storage of Export-Controlled Information

It is vital to store export-controlled information where is not accessible by unauthorized. Encryption of the data is the preferred solution.

ITAR information must be stored on the
"info appropriate for your company"

Use this folder for sharing ITAR information between authorized SMTC employees.

DO NOT store ITAR on the C: drive of your computer or other network location unless the drive is properly encrypted.

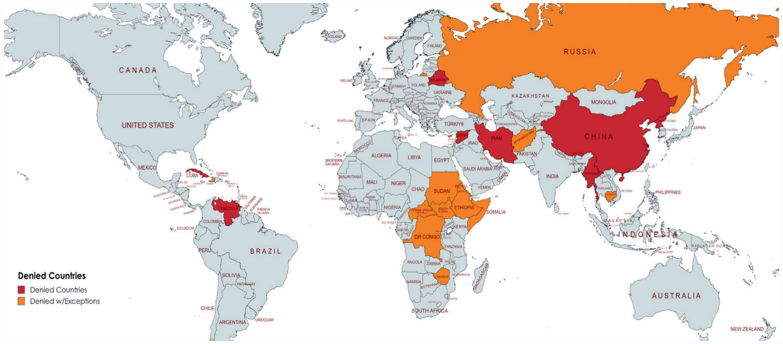
Contact the IT team to confirm encryption status before saving to a location OTHER than the share drives.

Trade Shows

Any information to be distributed or displayed should be limited to **general system descriptions/basic marketing information**, or other information that is already properly in the public domain.

If foreign nationals are attending the show, take particular care to safeguard any export-controlled or company proprietary information.

Foreign Travel



Transporting ITAR information to **any** of the highlighted countries is strictly prohibited by U.S. law. Follow the QR code to review 22 CFR 126.1 and a current list of restricted countries.

Contact the Trade Compliance and Facility Security Officer for more information on traveling overseas with proprietary or sensitive information.

Foreign Visitors

Inviting foreign nationals to visit our ITAR-restricted facilities is possible with **PRIOR coordination with the FSO.**

Here are few things to remember about visits from foreign nationals:

1. Notify FSO of pending visit.
2. Conduct pre-visit screening. Use iLobby's pre-registration feature.
3. Identify escort(s). Visitors MUST be under escort 100% of the time.
4. Install obscuration screening (if needed).
5. Pre-walk routes to ensure all ITAR info is hidden from view.

Follow the Foreign Visitor Checklist (FSO can provide a copy)

NOTE: The Visit Host must ensure visitor citizenship by obtaining written confirmation from the visitor's company/organization, preferably through official channels like Human Resources, not from the visitor directly.

Electronic Transmission of Export-Controlled Data

Government regulations require that export-controlled data be encrypted "end-to-end" while in transit. When it is necessary to transmit (or receive) export-controlled information outside SMTC, follow one of the two approved methods outlined below:

1 Use an approved encryption token (see example below). However, due to the cost of these tokens, not everyone can be issued one.

2 The **preferred** method of transmission is via Secure File Transfer Protocol (SFTP). Pre-vetted customers/vendors/suppliers can also use the SFTP to send and receive export-controlled and other sensitive data.

1. Open SMTC SFTP
2. Upload EAR/ITAR files
3. Notify recipient
4. Recipient opens SFTP and downloads files

Email & ITAR

Emailing ITAR/EAR information is **strictly prohibited** without the approval of the Facility Security Officer. Emails containing ITAR/EAR data MUST be properly encrypted using an approved encryption token.

"Password protecting" a document is insufficient; it lacks encryption and is unauthorized. This rule aims to prevent potential export control violations, safeguarding both our company and individuals.

Penalties for breaches are severe. Sharing ITAR/EAR information via Teams is also banned for these reasons.

Proper electronic transmission of ITAR/EAR mandates the use of approved encryption tokens, the Secure File Transfer Protocol (SFTP), or the internal drive where applicable. External organizations with adequately encrypted SFTP sites, approved for transmitting export-controlled data, are also permitted.

Contact the Trade Compliance and Facility Security Officer for guidance: