

Technical-data recipient and access map

Engineering security, export-control and legal teams

[Read the complete guide on aona.ai](#)

Classify the information and map who can access it before sending engineering material to AI. ITAR can concern transmissions abroad and releases to foreign persons within the United States. US hosting or ordinary TLS alone does not establish an exception, and a worksheet cannot authorise an export.

A fictional engineering team maps a proposed AI service before considering a separate record that may be controlled. The controlled record is not included.

Synthetic system and recipient roles only. No controlled engineering content, real export classification, licence or authorisation is represented.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ Establish data classification

Record the export-control determination and supporting basis for the actual information.

☐ Trace readable access and keys

Include model processing, support, logs, connections and intermediaries, not just hosting country.

☐ Resolve the authorisation or exception

Have the accountable export-control owner apply current requirements to the exact recipients and use.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: _____

Evidence to collect: _____

Owner and next review date: _____

Review matrix

Map point	Fictional proposed route	Question before a real decision
Source record	Engineering document with classification unresolved.	What is the actual jurisdiction/classification and supporting determination?
Employee device	Input assembled on a managed device in the United States.	Which local users and services can access the material?

Map point	Fictional proposed route	Question before a real decision
Application operator	External AI interface sends content for model processing.	Who is the legal recipient and what content can it read?
Model and hosting service	Processing location and authorised personnel are not established.	Where is processing, and who can obtain plaintext or access information?
Support, logs and connected tools	Potential additional recipients and retained copies.	What onward access exists, in which roles and locations, under which authority?
Encryption and keys	Transport encryption is proposed; end-to-end conditions are unverified.	Do actual key/recipient arrangements satisfy any relied-upon exception?
Review outcome	Material facts remain unresolved in this exercise.	Do not treat the map as permission to transmit controlled material.

Follow the content and access

- **Source:** Classification and intended purpose
- **Processing:** Application and model recipients
- **Additional access:** Support, logs, connections and intermediaries
- **Review:** Locations, plaintext, keys and legal authority

Unrestricted teaching input

“Rewrite a generic engineering-team meeting reminder.” No technical specifications, defence design or controlled information are provided.

Fictional assessment record

Record: TECH-EX-29, not included.

Classification: unresolved in the teaching scenario.

Potential recipients: AI interface, model service, support/logging services and a security intermediary.

US hosting: a proposed fact, not an export conclusion.

Encryption exception: not established by a TLS label.

Authorisation: none represented.

Source-currency note

FR Doc 2026-17660, published 28 August 2026 and effective 13 October 2026, changes aircraft-related paragraphs of 120.54. It does not amend the paragraph (a)(5) encryption conditions discussed in this exercise.

Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information, not professional approval or a completed control test. It does not classify ITAR data, grant export authorisations or establish that a provider or processing route is permitted.

[22 CFR 120.33: Technical data](#). ITAR technical-data definition and stated exclusions; a document label alone does not classify a real dataset.

[22 CFR 120.50: Export](#). Export includes specified transmissions outside the United States and releases to foreign persons within the United States, subject to the stated exceptions.

[22 CFR 120.56: Release](#). Technical-data release through the specified inspection, exchange and access-information circumstances.

[22 CFR 120.54: Activities that are not exports](#). Conditional treatment of unclassified technical data secured with qualifying end-to-end encryption; third-party decryption and other conditions matter.

[State Department: Aircraft survivability equipment amendment](#). The source page flags an amendment published at 91 FR 55460. The official rule, FR Doc 2026-17660, concerns civil aircraft incorporating survivability equipment and is effective 13 October 2026. Its changes to 120.54 concern aircraft-related paragraphs (a)(6) through (a)(9), not the paragraph (a)(5) encryption conditions discussed here. That dated check resolves the specific amendment flag; it does not replace a complete export analysis. Keep the applicable classification, authorisation, recipient and current legal review with any real decision, particularly if the use or law changes.