



GE Aerospace

— Stress-Testing Your TCP: From Compliance Binder to Living System

— The 14th Joint Industry Outreach Seminar on Strategic Trade Management

Lino Arboleda

08 Sep 2026

“Are Technology Control Plans
(TCPs) becoming a  exercise
rather than a living risk-
mitigation ?”

Technical Data Transfer Violations: Major DDTC Enforcement Actions

\$258M+
TOTAL PENALTIES



\$200M

2024

DDTC

Resolved alleged AECA/ITAR violations stemming from misclassification of technical data and defense articles in acquired companies, resulting in **unauthorized exports and retransfers of controlled technical data** across defense platforms.



\$30M

2018

DDTC

Unauthorized deemed exports of ITAR-controlled technical data to dual-national and third-country national employees — **foreign nationals accessed controlled technical data without authorization**. Also failed to properly manage export licenses for technical data transfers.



\$13M

2021

DDTC

Unauthorized export and retransfer of **ITAR-controlled technical drawings and engineering prints** related to military aircraft engines and defense platform components. Technical data shared with foreign persons without proper authorization.



\$6.6M

2022

DDTC

Unauthorized exports of ITAR-controlled technical data and defense articles related to defense electronic test and measurement equipment. Failed to obtain authorization before **transferring controlled technical data**.



\$5.5M

2020

DDTC

Unauthorized export of ITAR-controlled technical data and defense services related to military satellite and space systems. Failed to obtain proper authorizations for **technical data transfers in defense transactions**.



\$2.77M

2023

DDTC

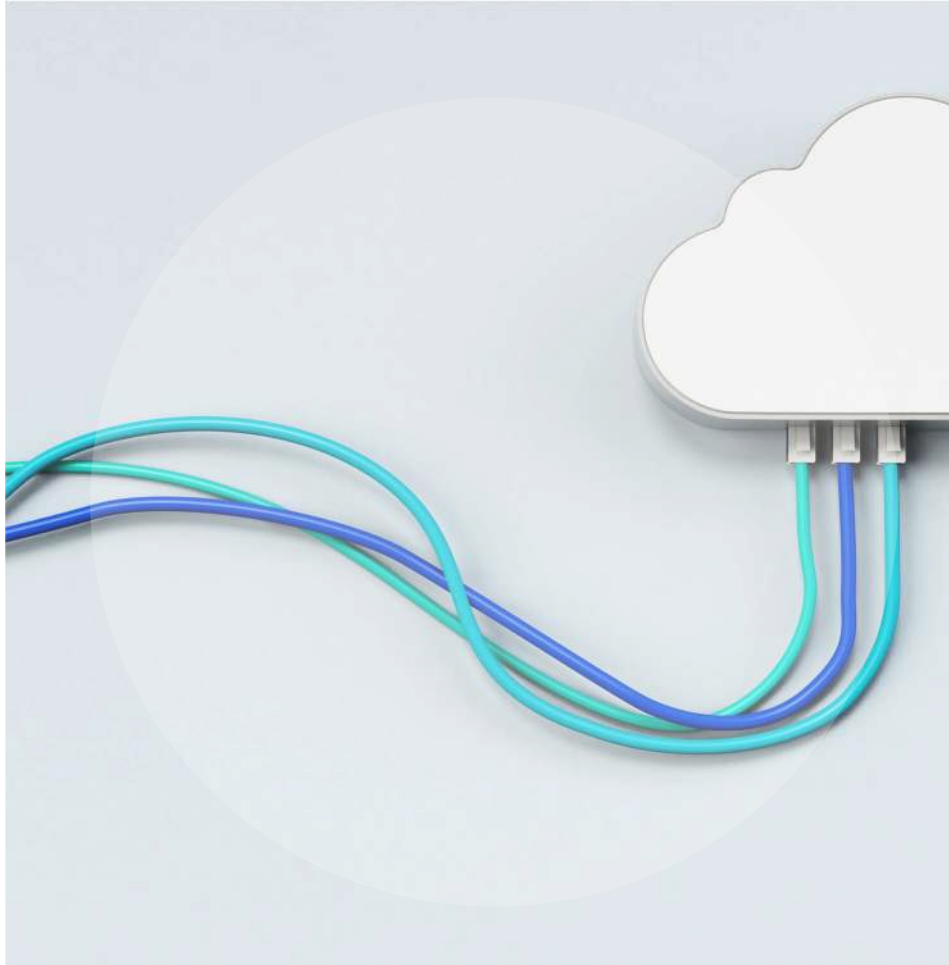
Emailed ITAR-controlled technical data — **design drawings, blueprints, and specifications for aerospace and military electronics** — to its foreign subsidiary. Constituted unauthorized export of controlled technical data.

● >\$100M

● \$10M–\$50M

● <\$10M

Source: U.S. Department of State, Directorate of Defense Trade Controls (DDTC), Consent Agreements & Enforcement Records | Violations of 22 CFR Part 125 & § 127.1



Regulatory Expectations Are Sharpening — Are TCPs Keeping Up?

-  Regulators increasingly want to see **evidence of effectiveness**, not just documented procedures
-  Growing convergence (and divergence) of TCP expectations across jurisdictions
-  Multinational engineering, computing, and R&D operations must satisfy multiple regulatory regimes simultaneously

Implementation Gaps: Where TCPs Break Down

Access control vs. access reality

Many TCPs set access boundaries on paper but overlook real-world technology flows

Personnel screening decay

Initial screening is common, but ongoing monitoring for changes in nationality status, or foreign affiliations is often weak or absent

Scope creep and classification drift

TCPs are often drafted for a specific technology but not updated as it matures or is reclassified

Third-party and vendor blind spots

Subcontractors, visiting researchers, and JV partners often fall outside TCP scope despite accessing controlled technology



Practitioner insight: Most common audit finding is not the *absence* of a TCP but the *staleness* of one — the plan that was current two years ago and has not been revisited since.

TCPs Without Borders: The Multi-Jurisdictional Challenge

**01 ITT Definition & Scope
of Control**

02 Foreign Person Definition

03 Deemed Export

04 Offshore Re-Transfer

**05 Encryption as a Safe
Harbor**

06 Server Location

**07 Cloud Computing: IaaS,
PaaS, SaaS**

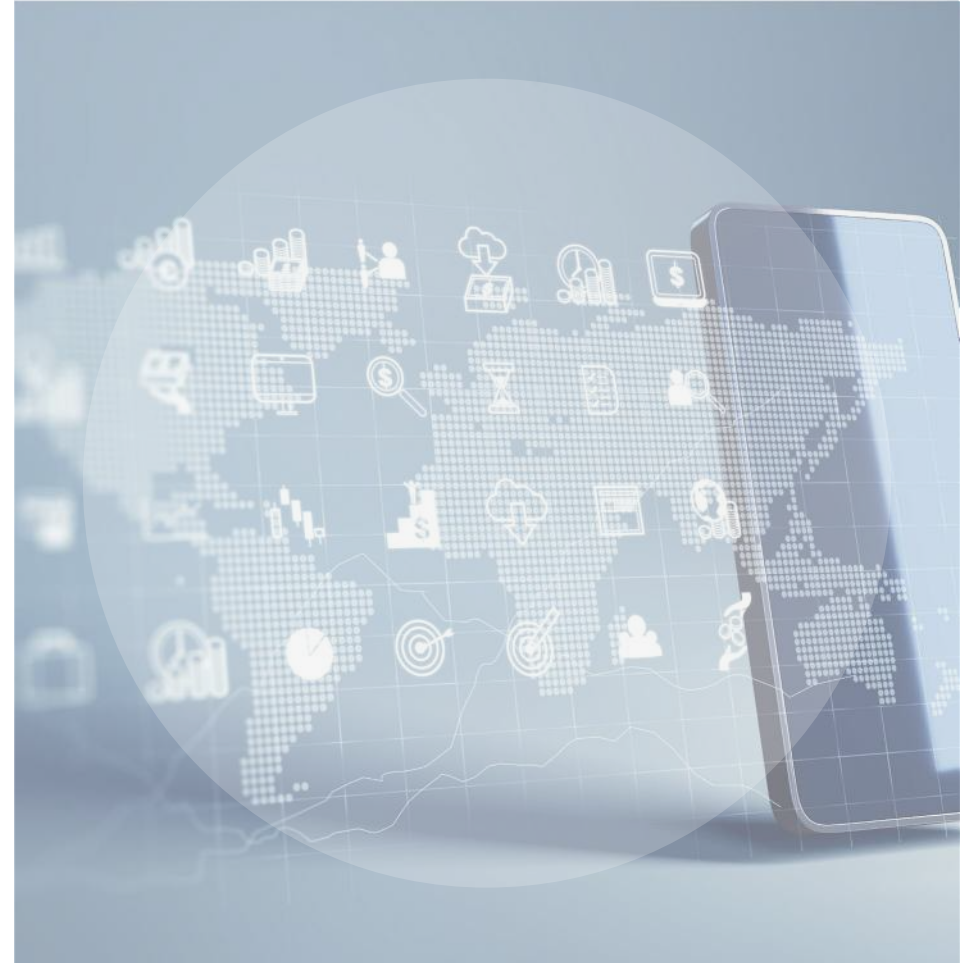
08 Data Hosting: HPC

09 Global Mobility

10 Remote Work Access

Toward Operationally Resilient TCPs

- 1 Integrate TCP reviews into technology development milestones**, not just annual compliance calendars
- 2 Invest in digital access-control infrastructure** that mirrors TCP boundaries in real time
- 3 Conduct red-team exercises** — simulate a deemed export scenario or a diversion attempt and test whether the TCP actually prevents it





GE Aerospace