



Ten Tips for Managing Export Controlled Technology

Jennifer Saak, Ph.D.

The U.S. Department of Commerce's Export Administration Regulations (EAR)¹ regulates both the export of physical commodities (think goods and equipment) as well as the transfer of software and intangible technical information associated with those products. The EAR imposes requirements for transferring export controlled "technology"² outside of the U.S., as well to foreign nationals physically present in the U.S. The latter transfer is "deemed" to be an export, and thus the regulation is commonly referred to as the "deemed export rule"³. Research and advanced technology organizations that possess export controlled technology can face tough challenges to meet these U.S. government requirements. This is especially true in organizations with a mixed environment containing both controlled and uncontrolled ("EAR99") technology. The regulations impose legal requirements that affect all aspects of knowledge management including electronic data storage, intra-company transfer, and inter-company transfer of controlled technical data. The nature of the complexity changes depending on the size of the organization and the make-up of the personnel.

Below are ten questions for export compliance practitioners in industry and higher education to consider when designing practical solutions to handle EAR-controlled technology in their organization. The answers can guide compliance personnel and their key stakeholders to the best solution for their specific environment.

1. **What is the export control classification number (ECCN) of the data?** Determining the requirements to access controlled technology begins with identifying the ECCN of the data and associated goods or equipment. Properly classifying the items or associated technologies often involves understanding relevant scientific specifications. The more restrictive ECCNs will require a license before transferring to a broader range of citizenships.
2. **What are the government licensing requirements for the particular ECCNs?** Technology covered under less restrictive ECCNs may be eligible for certain license exceptions⁴, which can be easier to

manage. For more restrictive ECCNs, a U.S. government license is required before a non-U.S. citizen or legal U.S. permanent resident is permitted to access the data.

3. ***What portion of the organization's portfolio is export controlled?*** The most practical solution for an organization will vary if the portfolio is 100% export controlled versus partially export controlled. The blended business environment of non-EAR99 and EAR99 items is often more challenging. The export compliance management solution should be tailored to meet the legal requirements while maximizing operational efficiency.
4. ***How does the controlled technical data enter the company?*** Is it generated in-house by certain functions, such as researchers or manufacturing engineers? Is it brought into the organization via contractual technology licensing agreements? If so, export controls should be considered up front when managing those contracts and deals.
5. ***Who needs to access the controlled data?*** What are all the possible pathways for the data to move around once it is generated or introduced into the organization? One must consider all down-stream functions, departments, or teams that handle the data through normal operations at the institution or company.
6. ***What are the citizenships of the personnel?*** Global human resources databases can be one source of information. Currently, BIS references the most recently obtained citizenship or legal permanent residency when determining license requirements for a certain individual to access controlled technology⁵. However, dual-citizenship and permanent residency details are not always accounted for in personnel databases. Multi-national companies must also consider global privacy laws.
7. ***Where is the controlled technical data located?*** One should consider technical reports, presentations, laboratory notebooks, local and global IT systems (including email, instant messaging), shared drives, and other types of knowledge-sharing mechanisms.
8. ***How is export controlled technology accessed or disseminated?*** Consider the most common mode (e.g. via a corporate-wide IT system) as well as ad hoc methods such as group meetings, global newsletters, internal presentations, internal reports/memos, and on-site visits. Robust internal control plan solutions must meet all methods of transfer.
9. ***How will the company document internal procedures to manage the data transfers?*** A best practice is to develop and implement a written technology control plan (TCP) which captures comprehensive internal procedures for ensuring proper data security. This is also a required component of a U.S. government technology export or deemed export license application.
10. ***How will all relevant personnel be trained on their role in the organization's handling of export controlled information?*** Training programs are most effective when the contained information is directly relevant to the audience's role and daily work. Consider tailored modules designed for your organization and, furthermore, for each functional role. The content should bring forth clear actions and resources for the specific audience.

With these pointers in mind, export compliance officers in both industrial and academic environments can begin to establish the foundation for a strong export compliance program that effectively and efficiently handles export controlled technology.

¹ Export Administration Regulations: 15 CFR Parts 730-744

² Definition of “technology”: 15 CFR Part 772.1 and Part 774 Supplement 1 and 2

³ Deemed Export Rule: 15 CFR Part 734.2 (b)

⁴ License Exceptions: 15 CFR Part 740

⁵ Deemed Reexport Advisory Opinion (October 31, 2013)

Disclaimer: Traliance LLC is not a law firm and the information in this article is general in nature and is not intended to constitute legal advice.