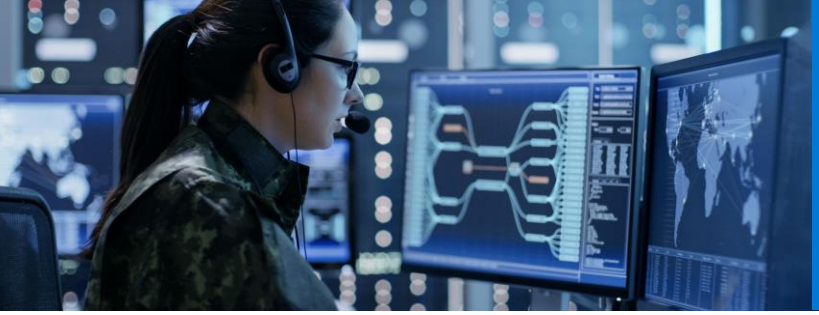

# Export Administration Regulations (EAR)

Microsoft cloud services help customers subject to the US Export Administration Regulations meet their compliance requirements and manage export control risk.

## Microsoft and the EAR

Microsoft technologies, products, and services are subject to the US Export Administration Regulations (EAR). While there is no compliance certification for the EAR, Microsoft Azure, Microsoft Azure Government, and Microsoft Office 365 Government (GCC-High and DoD environments) offer important features and tools to help eligible customers subject to the EAR manage export control risks and meet their compliance requirements.

The US Commerce Department, which enforces the EAR, has taken the position that customers, not cloud service providers such as Microsoft, are considered to be exporters of their own customer data. While most customer data is not considered "technology" or "technical data" subject to EAR export controls, Microsoft in-scope cloud services are structured to help customers manage and significantly mitigate the potential export control risks they face. Microsoft generally, but not exclusively, recommends the use of its government cloud services for eligible customers. With appropriate planning, customers can use the following tools and their own internal procedures to help ensure full compliance with US export controls.

- **Controls on data location**. Customers have visibility into where their data is stored and access to robust tools to restrict its storage. They may therefore ensure that their data is stored in the United States and minimize transfer of controlled technology or technical data outside the United States. Furthermore, customer data is not stored in a non-conforming location, consistent with EAR prohibitions on where data is "intentionally stored": no Azure datacenter is located in any of the 25 Group D:5 countries or the Russian Federation.
- **End-to-end encryption**. By taking advantage of the end-to-end encryption safe harbor for physical storage locations specified in the EAR, Microsoft in-scope cloud services deliver encryption features that can help protect against export control risks. They also offer customers a wide range of options for encrypting data in transit and at rest, as well as the flexibility to choose among encryption options.
- **Tools and protocols to prevent unauthorized deemed export**. The use of encryption also helps protect against a potential deemed export (or deemed re-export) under the EAR, because even if a non-US person has access to encrypted data, nothing is actually revealed if they cannot read or understand the data while it is encrypted; thus there is no "release" of controlled data.

## Microsoft in-scope cloud services

- Azure and Azure Government
  Learn more
- Intune
- Office 365 Government (GCC-High and DoD)
  Learn more

## How to implement

- **Microsoft and US export controls**
  Overview of US export controls and guidance for customers assessing their obligations under the EAR.
  - Azure
    Learn more
  - Office 365
    Learn more

## About the EAR

The US Department of Commerce enforces the Export Administration Regulations (EAR) through the Bureau of Industry and Security (BIS). The EAR broadly govern and impose controls on the export and re-export of most commercial goods, software, and technology, including "dual-use" items that can be used both for commercial and military purposes and certain defense items.

BIS guidance holds that, when data or software is uploaded to the cloud or transferred between user nodes, the customer, not the cloud provider, is the "exporter" who has the responsibility to ensure that transfers of, storage of, and access to that data or software complies with the EAR.

According to the BIS, *export* refers to the transfer of protected technology or technical data to a foreign destination or its release to a foreign person in the United States (also referred to as a *deemed export*). The EAR broadly govern:

- Exports from the United States.
- Re-exports or retransfers of US-origin items and certain foreign-origin items with more than a *de minimis* portion of US-origin content.
- Transfers or disclosures to persons from other countries.

Items subject to the EAR can be found on the Commerce Control List (CCL) where each item is assigned a unique Export Control Classification Number (ECCN). Items not listed on the CCL are designated as EAR99 and most EAR99 commercial products will not require a license to be exported. However, depending on the destination, end user, or end use of the item, even an EAR99 item may require a BIS export license.

The final rule, published in June 2016, clarified that EAR licensing requirements also would not apply to the transmission and storage of unclassified technical data and software if they were encrypted end-to-end using FIPS 140-2 validated cryptographic modules and were not intentionally stored in a military-embargoed country or in the Russian Federation.

## Frequently asked questions

**What should I do to comply with export controls when using Microsoft cloud services?**

Under the EAR, when data is uploaded to a cloud server such as the Microsoft cloud, the customer who owns the data—not the cloud services provider—is considered to be the exporter. For that reason, the owner of the data—that is, the Microsoft customer—must carefully assess how their use of the Microsoft cloud may implicate US export controls and determine whether any of the data they want to use or store there may be subject to EAR controls, and if so, what controls apply. Learn more about how Azure and Office 365 cloud services can help customers ensure their full compliance with US export controls.

**Are Microsoft technologies, products, and services subject to the EAR?**

Most Microsoft technologies, products, and services either:

- Are not subject to the EAR and thus are not on the Commerce Control List and have no ECCN;
- Or they are EAR99 or 5D992 Mass Market-eligible for self-classification by Microsoft and may be exported to non-embargoed countries without a license as No License Required (NLR).

That said, a few Microsoft products have been assigned an ECCN that may or may not require a license. Consult the EAR or legal counsel to determine the appropriate license type and eligible countries for export purposes.

**What's the difference between the EAR and International Traffic in Arms Regulations (ITAR)?**

The primary US export controls with the broadest application are the EAR, administered by the US Department of Commerce. The EAR are applicable to dual-use items that have both commercial and military applications, as well as to items with purely commercial applications.

The United States also has separate and more specialized export control regulations, such as the ITAR, that govern the most sensitive items and technology. Administered by the US Department of State, they impose controls on the export, temporary import, re-export, and transfer of many military, defense, and intelligence items (also known as "defense articles"), including related technical data.

## Additional resources

Exporting Microsoft Products: Overview

Exporting Microsoft Products: FAQ

Exporting Microsoft Products: Product Lookup

Export restrictions on cryptography

Microsoft and FIPS 140-2

Microsoft and ITAR