

Customers subject to the export control requirements of US DoE 10 CFR Part 810 can use Azure Government.

Microsoft and DoE 10 CFR Part 810

Microsoft Azure Government can help support customers subject to the export control requirements of US Department of Energy (DoE) 10 CFR Part 810 through two authorizations:

- The FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the Joint Authorization Board (JAB)
- The Level 4 and 5 Provisional Authorizations from the Department of Defense (DoD) Defense Information Systems Agency

FedRAMP offers an appropriate baseline to provide assurances that Azure Government delivers core infrastructure and virtualization technologies and services such as compute, storage, and networking that are designed with stringent NIST controls. These help meet customer data separation requirements and help enable secure connections to customers' on-premises environments.

Furthermore, Azure Government is a US government community cloud that is physically separated from the Azure cloud. It provides additional assurances regarding specific background screening requirements by the US government, including specific controls that restrict access to information and systems to screened US citizens among Azure operations personnel.

Microsoft in-scope cloud services

- Azure Government
[Learn more](#)
- Intune

How to implement

- **NERC CIP Standards & Cloud Computing**
Guidance for electric utilities and Registered Entities deploying workloads on Azure or Azure Government.
[Learn more](#)

About DoE 10 CFR Part 810

The US Department of Energy (DoE) export control regulation [10 CFR Part 810](#) governs the export of unclassified nuclear technology and assistance. It helps ensure that nuclear technologies exported from the United States will be used only for peaceful purposes. The revised Part 810 (Final Rule) took effect in March 2015 and is administered by the [National Nuclear Security Administration](#). Section 810.6 states that specific DoE authorization is required for both provisions of assistance and transfers of sensitive nuclear technology that are "generally authorized," as well as those requiring specific authorization (such as for assistance involving sensitive nuclear technologies like enrichment and heavy water production).

Frequently asked questions

Do the 10 CFR Part 110 regulations of the US Nuclear Regulatory Commission apply to Azure Government?

No. The [US Nuclear Regulatory Commission](#) (NRC) regulates the [export and import](#) of nuclear facilities and related equipment and materials under [10 CFR Part 110](#). The NRC does not regulate nuclear technology and assistance related to these items that fall under DoE jurisdiction. Consequently, NRC 10 CFR Part 110 regulations would not apply to Azure Government.

How can I supply evidence that I am complying with DoE 10 CFR Part 810?

If your organization is deploying data to Azure Government, you can rely on the Azure Government FedRAMP High P-ATO as evidence that you are handling data in an appropriately restricted manner. However, you are responsible for getting DoE authorization of your own systems, including the use of cloud services.

What are my responsibilities for classifying data deployed to Azure Government?

Customers deploying data to Azure Government are responsible for their own security classification process. For customer data subject to DoE export controls, the classification system is augmented by the Unclassified Controlled Nuclear Information (UCNI) controls established by Section 148 of the [US Atomic Energy Act](#).

Additional resources

[Azure Cloud Services and US Export Controls](#)

[Microsoft and FedRAMP](#)

[Microsoft and DoD](#)

[Microsoft Government Cloud](#)