ITAR COMPLIANCE IN THE CLOUD

WHAT IS ITAR?

ITAR (International Traffic in Arms Regulations) is a list of defense-related articles on the U.S. Munitions List (USML) that require a license to export. As a cloud infrastructure provider, AWS does not have visibility into how customers use its services, including whether customer data is subject to ITAR, for this reason. AWS also applies a strong security control over ITAR-compliant workloads in the region, regardless of whether the data is subject to ITAR or other export control requirements.

AWS GovCloud (US) provides customers with the ability to achieve ITAR compliance in the US.

AWS Shared Responsibility Models

A physical and logically isolated region, separate from all other AWS data centers.

Region accessible to the customer, organizations, and users.

Managed by AWS personnel who are US citizens located on US soil.

Supports FIPS 140-2 ready environments.

Examples of Controlled Unclassified Information (CUI) in AWS GovCloud (US)

Examples of ITAR Data

Achieve and Maintain Compliance

CONTROL ACCESS TO ACHIEVE COMPLIANCE

Audit access and use of sensitive data with your work in Amazon GovCloud using AWS Key Management Service (KMS).

IMPROVE VISIBILITY

View and share the graphic Amazon GovCloud (US) video at: www.aws.amazon.com/govcloud-us/

SAFEGUARD SENSITIVE DATA

Protect data with sensitive access permissions in Amazon S3 and metadata management with AWS GovCloud (US) over users' data with AWS Key Management Service (KMS).

STRENGTHEN IDENTITIY MANAGEMENT

Limit access to sensitive data by individual users, teams, and organizations. AWS GovCloud data centers are able to meet identity federation, proxy key rotation, and other requirements across contributing bodies.