End-to-End DATA Protection for ITAR Compliance

SECURING CRITICAL **DATA** along its entire journey

The Challenge

The International Traffic in Arms Regulations (ITAR) 1976 is a set of policy requirements that restrict and control the export and import of defence-related articles, services and technology listed on the U.S. Munitions List (USML).

Basically any company that supplies the US State Department or sits in its supply chain needs to comply with ITAR. The Directorate of Defence Trade Controls required companies to have an export license to export technical/classified and unclassified data within the ITAR definition.

- ☑ Pre- 2020: Export Licenses required to transmit ITAR data outside the US including Cloud
- ☑ Post 2020: Act Amended such that as long as the data was protected using "End to End Encryption and FIPS 140-2 validated algorithms" with no access to the keys by a third party including the service provider no Export license was required.
- ☒ Technologies such as VPN / SDWAN / Encrypted MPLS / Encrypted Cloud onramps are not sufficient as they only protect part of the data journey , may not be FIPS 140-2 certified and do not separate the key ownership from the key management.

The term "end-to-end encryption" is defined in the amendment as: (i) the provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and (ii) the means of decryption are not provided to any third party.

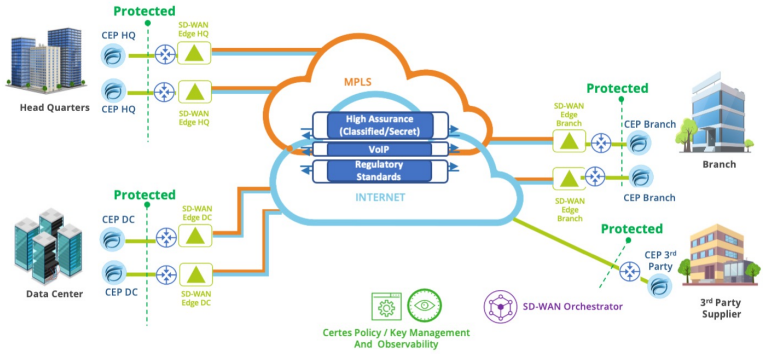
Penalties for Non-compliance?

- Seizure and Forfeiture: government confiscation of any items or technical data involved in the violation
- Administrative or Statutory Debarment: inability to apply for contracts
- Civil Fines: fines up to $500,000
- Criminal Penalties: of up to $1 million and/or 10 years imprisonment per violation

The Solution:

High Assurance Data Protection from Certes Networks:

- ☑ FIPS-140-2 Compliant
- ☑ Network Agnostic Transparent Overlay
- ☑ Public / Private Cloud
- ☑ NIST Compliant Separation of Duties for Key Management
- ☑ End-to-End Encryption



Certes – Patented technology placed at the Data origin and Intended recipient protect the entire Data Journey

Contact Certes Networks

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

www.certesnetworks.com

CERTES NETWORKS

Tel: 1 (888) 833-1142
Fax: 1 (412) 262-2574

sales@certesnetworks.com
info@certesnetworks.com