ITAR / EAR Data Controls

Export Administration Regulations (EAR) and International Traffic Arms Regulation (ITAR)

Export Administration Regulations (EAR) and International Traffic Arms Regulation (ITAR) are US government export controls that govern technical data at rest, in motion, and in use. EAR and ITAR are separate regulations that are compatible and consistent in their approach to controlling sensitive data.

Companies that work with controlled information must comply with both ITAR and EAR, however there are no certifications for ITAR or EAR compliance. Violations of these regulations may result in both criminal and civil prosecution.

ITAR

ITAR was created by the Directorate of Defense Trade Control (DDTC) to regulate two things, defense articles and defense services. A complete list of defense articles may be found on the US Munitions List (USML), but defense services are simply defined as any of the following.

- Assisting a foreign person with a defense article
- Providing technical data to a foreign person
- Providing military training to a foreign unit or force

ITAR restrictions are very tight, for example, showing technical data to a foreigner is considered an export even if the foreigner is in the USA. Releases of controlled technology to foreign persons in the USA is also deemed to be an export to the person's country or countries of nationality. ITAR regulations state that no non-US person may have physical or logical access to information stored in an ITAR environment.

ITAR sets criteria that allows for the use of cloud technology provided that the content is unclassified, secured using end-to-end encryption, secured using FIPS 140-2 encryption, and not intentionally sent to or from a person in or stored in a prohibited country. ITAR cloud compliance focuses on ensuring controlled technical data is not inadvertently exported. In 2016, DDCT provisioned that export controlled data must be end-to-end encrypted and the method for decrypting the data may not be shared with a third party before it reaches the intended recipient.

The standard encryption of data at rest by most cloud providers is not end-to-end encryption and fails to comply with ITAR. Providers who have access to your data and its encryption key are a violation of ITAR compliance.

> HighSide's **SecureDrive** meets and exceeds ITAR & EAR data encryption and access control requirements. With end-to-end encryption exceeding FIPS 140-2, geo based user access controls, and no access to private keys, HighSide is the complete ITAR & EAR solution.

EAR

Bureau of Industry and Security (BIS) administers Export Administration Regulations (EAR). EAR regulates items and their related technology that are designed for commercial use, but could have military applications. Similar to ITAR's USML, BIS maintains a Commerce Control List (CCL). BIS set rules that allow for the use of cloud technology under certain provisions:

- Content is unclassified
- Content is secured using end-to-end encryption
- Encryption is at least as effective as FIPS 140-2 standards
- Data is not stored in Russia or a military embargoed country (Country Group D:5)
- Means of decryption are not provided to any 3rd party

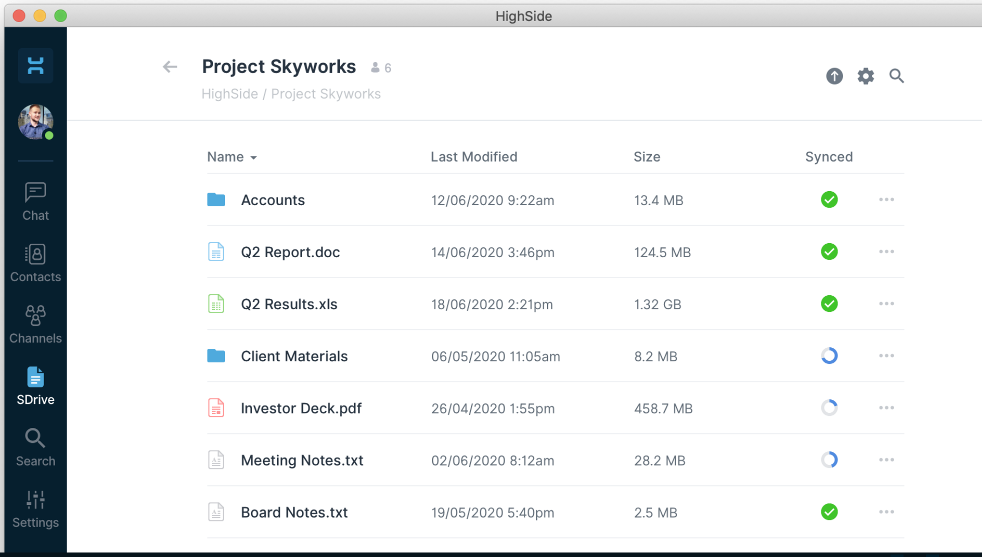
ITAR & EAR Compliance with HighSide's SecureDrive

ITAR and EAR compliance with cloud data is not an end result, but a continual journey protecting that data. There is no certificate of compliance or stamp of approval, as such organizations must implement the right technology, access controls and user programs.

HighSide's SecureDrive provides organizations the tools to govern how sensitive information is stored, where the information is accessed, and with whom it is shared. HighSide's end-to-end encryption meets and exceeds FIPS 140-2 standards and is persistent with no 3rd party (including HighSide) access. SecureDrive may be deployed in compliant environments up to Impact Level 6 and On-prem in order to satisfy the strictest security and compliance requirements. HighSide's SecureDrive provides organizations with modern capabilities to share data, store data in the cloud and collaborate on data while remaining secure and compliant.

SecureDrive Features

- End-to-End encryption that meets and exceeds FIPS 140-2 standards and offline document availability
- FedRAMP approved cloud hosting options including isolated computing environments up to IL 5. Support for On-Prem deployments.
- Access controls for data based on physical device location, LDAP integrated security groups and time based restrictions
- e-Discovery support for encrypted data with integrated compliance management platform
- Device management ensures only authorized devices can access data



Project Skyworks 6

HighSide / Project Skyworks

Name	Last Modified	Size	Synced
Accounts	12/06/2020 9:22am	13.4 MB	✓
Q2 Report.doc	14/06/2020 3:46pm	124.5 MB	✓
Q2 Results.xls	18/06/2020 2:21pm	1.32 GB	✓
Client Materials	06/05/2020 11:05am	8.2 MB	◌
Investor Deck.pdf	26/04/2020 1:55pm	458.7 MB	◌
Meeting Notes.txt	02/06/2020 8:12am	28.2 MB	◌
Board Notes.txt	19/05/2020 5:40pm	2.5 MB	✓

HighSide is the global leader in secure cloud sharing, collaboration & access management. Powered by a distributed cryptographic key management infrastructure, HighSide's suite of products enable businesses to engage securely in a remote first world. Through our zero-trust technology, teams have access to a modern unified communications and file sharing platform including voice, video, text and files, reducing risk of shadow IT and reliance on dated and insecure communications channels.

HighSide delivers applications that users actually want to use and that security leaders want to deploy. Founded in 2015, the company has offices in Columbia, MD, Esch-sur-Alzette, Luxembourg and New York, NY.

highside.io
sales@highside.io