CODE42

TECH OVERVIEW | PRODUCT

HOW CODE42 HELPS ORGANIZATIONS MAINTAIN ITAR COMPLIANCE

Code42 endpoint data protection solutions (Incydr and CrashPlan) support customer compliance with International Traffic in Arms Regulation (ITAR) requirements, giving organizations the critical data risk detection and response capabilities as well as data preservation needed for handling defense-related information falling under the United States Munitions List (USML). In addition, Code42 provides a powerful data protection foundation that contributes to a long-term ITAR compliance strategy and prepares organizations to meet evolving regulations and complex compliance requirements.

What is ITAR?

ITAR regulates the security and control of sensitive information pertaining to the export and import of defense-related articles and services covered on the USML. In essence, ITAR aims to keep sensitive defense and military related information within the United States—moreover, to keep it out of the hands of foreign nationals.

ITAR was born in the midst of the Cold War. Today's business world looks much different. Rather than control movement of physical documents, companies that fall under ITAR now must secure electronic data that can (and does) easily move around the globe in an instant.

Maintaining ITAR compliance in the cloud

As organizations increasingly pursue cloud-first strategies, there is a growing misconception that ITAR-regulated companies cannot use cloud technologies. In fact, there are only a few additional requirements for maintaining ITAR compliance with cloud-based solutions for storing protected defense articles and controlled unclassified information (CUI):

- **Verify data is secured using end-to-end encryption.**
- **Ensure cloud data remains within the U.S.**
- **Allow only U.S. Persons to access cloud data.**

Leading cloud technology providers like Code42 specifically design their cloud solutions to support these ITAR compliance requirements.

Debunking the myth of "ITAR Certification"

One of the most common approaches to an ITAR compliance audit is to simply send letters to all technology partners requesting that they confirm they are "ITAR Certified." Unfortunately, there is no such thing as ITAR certification. There is ITAR registration, but this step is typically reserved for the organization that directly falls under ITAR—not the technology partner.

In other words, the most technology partners aren't themselves covered by ITAR. Though they could choose to maintain ITAR registration, this generally falls outside the scope of their business. Instead, leading technology partners like Code42 focus their effots on delivering solutions that enable their customers to maintain ITAR compliance.

How Code42 supports ITAR compliance

Code42's endpoint data protection solutions deliver several key functionalities that play a vital role in supporting ITAR compliance:

1. **Secure and control your endpoint data.** Your employees and end users create and move an incredible amount of data on a daily basis. More than half of this data now lives exclusively on endpoint devices—laptops and desktops. In today's world, these devices (and the data that resides on them) can sit outside the traditional perimeter and beyond the visibility of traditional data security tools. Code42 solves this challenge, by automatically encrypting all endpoint data no matter where it lives or moves. Code42 Incydr gives you visibility to data exfiltration across a variety of vectors and provides protection against insider risk. This is the starting point of a comprehensive data security and data control strategy that supports ITAR compliance.
2. **Maintain U.S.-based data storage.** Code42 gives you the ability to control where your data lives, no matter where your endpoints reside, including on or off network. Our cloud offering includes a robust U.S. presence, enabling organizations to keep ITAR-regulated data within the U.S. while still gaining the advantages and efficiencies of the cloud.
3. **Ensure end-to-end encryption** Unlike other technology providers, Code42 doesn't have to deploy a specialized solution for customers that fall under ITAR. That's because we protect all customer data with end-to-end encryption that meets the highest U.S. government standards: 256-bit AES encryption to secure data at rest and 256-bit Transport Layer Security (TLS 1.2) encryption to secure all data in transit, utilizing FIPS 140-2 validated modules.
4. **Gain visibility, monitor data movement and spot risk sooner** At Code42, we believe ITAR compliance is about more than checking boxes; it's about choosing solutions that enable your organization to mitigate the risk of sensitive USML data falling into the wrong hands. With Incydr you have the ability to detect, mitigate and respond to data exfiltration and insider risks. See how your employees move data across vectors— including web browser uploads, cloud sync activity, cloud file sharing, email, and use of removable media. Know if and when users move ITAR-covered data outside the U.S., so you can take action quickly to mitigate risk non-compliance and avoid potentially associated penalties and other impacts, including reputational damage.

   Leverage this powerful data visibility to enable a proactive and intelligent approach to data security and protection. Establish baselines of normal individual user behavior and detect deviations or unusual activity. In short, spot anomalies sooner. Take action faster.

Code42 answers the big ITAR questions

Will our ITAR-covered information be encrypted?

Yes. Code42 uses 256-bit AES encryption to secure all data at rest and 256-bit Transport Layer Security (TLS) 1.2 encryption to secure all data in transit

Are Code42 employees with data access U.S. Persons?

Yes. All Code42 staff who work with customers' data are U.S. Persons, as defined by ITAR.

Will our data reside in the U.S. —even in cloud deployments?

Yes. Code42 offers the flexibility to choose from specific data centers globally. With the agile Code42 cloud platform, customers can elect to keep all data at cloud storage locations within the U.S.

CODE42

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242
code42.com

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com, read Code42's blog or follow the company on Twitter. (WP2010210)