What is ITAR compliance?

Thank you for downloading this Box PDF. Carahsoft is the official government distributor for Box MultiCloud solutions available via NASA SEWP V, CMAS, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Box's solutions, please check out the following resources and information:

For additional resources:
carah.io/BoxResources

For upcoming events:
carah.io/BoxEvents

For additional Box solutions:
carah.io/BoxSolutions

For additional MultiCloud solutions:
carah.io/MultiCloud

To set up a meeting:
BoxInc@carahsoft.com
703-871-8548

To purchase, check out the contract vehicles available for procurement:
carah.io/BoxContracts

For more information, contact Carahsoft or our reseller partners:
BoxInc@carahsoft.com | 703-871-8548

box BLOGS

Home / Deep Dives

What is ITAR compliance?

FEBRUARY 23RD 2022 | **BOX COMMUNICATIONS**

Share

International Traffic in Arms Regulations (ITAR) is a set of American standards to ensure the security of defense articles in import and export. These articles can include munitions, defense services, or technical information about either. Companies in the United States that deal directly with these articles must meet ITAR requirements. These companies must also request ITAR compliance from those within their supply chain. Consequently, a variety of business types need to remain ITAR compliant.

ITAR guarantees the safety of the import and export of munitions, defense services, and more

What is ITAR compliance?

ITAR requirements restrict access to e
Munitions List (USML) to American citiz
with overseas operations cannot share technical information about
munitions covered on the USML with locally hired staff. They also cannot

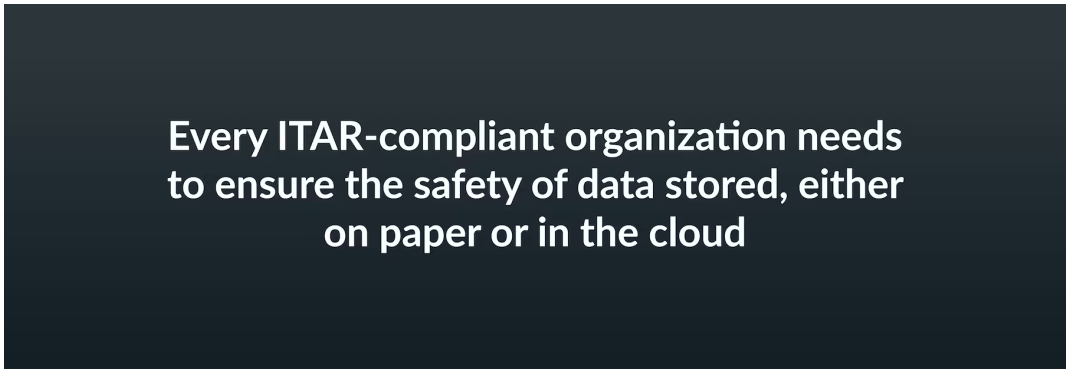
divulge this information with subcontractors who are not from the United States. Only non-American groups with approval from the State Department can access ITAR information.

Most non-American countries fall under the ITAR prohibitions for sharing or selling defense articles or data. Some nations have complete denial of receipt of these from Americans. Other countries have some very specific exceptions to ITAR. A handful of countries are exempt — those on the approved list include Australia, NATO members, Japan, and Sweden.

The specific countries and goods or services prohibited under ITAR stem from three main sources:

- Goods prohibited for export or sale under United Nations Security Council sanctions, regardless if they're on the existing USML
- Nations indicated by the Secretary of State as state sponsors of terrorism
- Countries under existing United States arms embargoes

Recordkeeping and compliance



Compliance with ITAR includes registering with the State Department Directorate of Defense Trade Controls (DDTC). Registration acknowledges the company fully understands ITAR requirements and fulfills them for any USML services or products. Once a business agrees to supply parts to a USML exporter, it accepts responsibility for following ITAR.

A major component of maintaining ITAR compliance is recordkeeping, with regulations including:

- Registered entities must retain information regarding brokering services, technical data, and political contributions
- They must hold data on the manufacture, acquisition, and disposal of defense articles
- Any data stored electronically must be reproducible on paper
- All information stored on paper or electronically must have protections against changes unless officially recorded
- Records must stay within the business's ownership for five years after its DDTC registration expires and be available for inspection by a DDTC representative

Any business required to be ITAR compliant must have a compliance program and ensure all storage of records meets the regulations. Both cloud storage and paper records need tight security to keep the data safe. For paper records, store them under lock and key and only permit authorized personnel access. Cloud storage requires encryption to ensure data stays secure. The type of information stored determines whether a business can share it with others, who it can go to, and how.

The federal government takes ITAR compliance seriously, and failure to meet these regulations results in severe penalties. Avoid violations by knowing ITAR requirements and following them exactly.

Who needs to follow ITAR compliance?

Businesses that follow ITAR compliance

- Distributors
- Manufacturers
- Wholesalers
- Contractors
- Foreign military sales (FMS) freight forwarders
- Third-party suppliers
- Vendors of computer hardware or software

Businesses that need to follow ITAR compliance include those directly and indirectly involved in exporting defense articles or data. These companies include those that manufacture, sell, design, distribute, or handle technical data, articles, or services listed on the USML. Businesses within the supply chain for these companies must also follow ITAR.

Examples of companies that need to be ITAR compliant are a producer of a part listed on the USML and the company that buys the part. If the second company that bought the part sold it to a prohibited nation, both businesses would face potential fines or other penalties for violating ITAR.

Companies do not have to specifically be within the defense industry to require ITAR compliance. They only need to be part of the supply chain for data, services, or goods that fall into the USML categories. Examples of types of businesses that need to become ITAR compliant include:

- Distributors
- Manufacturers
- Wholesalers
- Contractors
- Foreign military sales (FMS) freight forwarders
- Third-party suppliers
- Vendors of computer hardware or software

Those required to follow ITAR compliance must register with the DDTC first and create their in-house compliance programs. Supply chain members, such as manufacturers who do not export goods, must still register with DDTC and maintain ITAR compliance. The aim of requiring compliance from such broad categories is ensuring the security of USML goods, services, or data to only be accessed by Americans or those from other approved nations.

What are ITAR compliance requirements?

ITAR compliance has three steps. These steps ensure companies only provide goods or services that could be used for military reasons to people

in pre-approved countries. ITAR compliance helps the DDTC track the sales of arms and other USML products or services to ensure national security. Requirements for compliances include the following three stages:

1. Register with the DDTC

ITAR compliance requirements start with registration with the DDTC. Registration does not confer automatic authorization for exporting goods, but it does indicate a company now agrees to ITAR compliance.

Registration includes submitting a certified Statement of Registration. This registration also includes documents verifying that the company is based in, or authorized to do business in, the United States. Certification comes from a senior member of the company.

When submitting the registration, the senior officer needs to state whether anyone involved with the company has ever been convicted of certain criminal acts or if anyone connected to the organization is barred from contracting with the U.S. government.

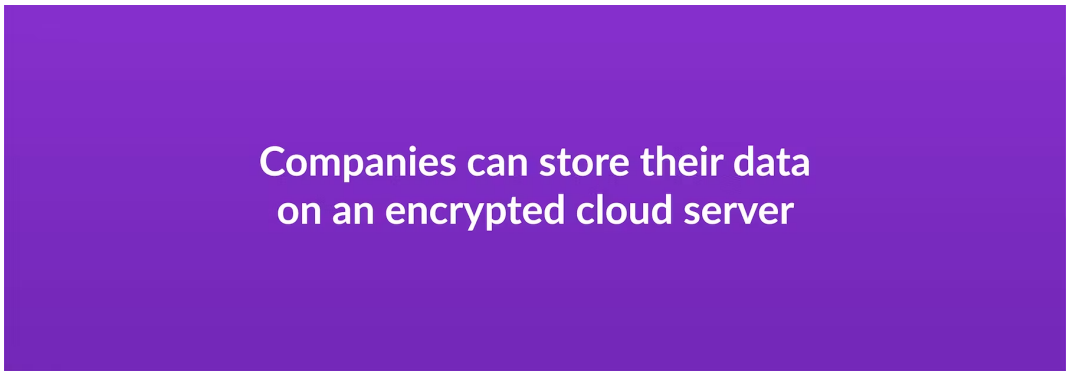
Companies must pay a registration fee and renew their registrations annually. They must also notify the DDTC within five days of any changes in their Statement of Registration or of charges against any of their corporate officers for breaking any U.S. criminal statutes.

2. Create a compliance program

Registered businesses must form a customized ITAR compliance program for their companies. This program indicates an understanding of ITAR

requirements and how the business will meet them. Information in the compliance program may include data on unclassified and classified records or data storage. It will also cover any USML goods the company handles.

3. Maintain secure records



Keeping secure records is most important to the DDTC for ITAR compliance. The organization requires that a company keep records on all disposal, acquisition, and manufacture of USML goods, data, or services. The company must also retain data about exemptions to exports, applications, licenses, and other documents for exports. Companies must keep these records for five years after the license expiration of the approval date.

A representative from DDTC may access a registered company's ITAR records at any time. Companies must have paper records of classified technical information because this data does not qualify for the Encryption Rule. Most companies will have some information stored on-site and other unclassified technical data kept in an encrypted cloud server.

How do I achieve ITAR compliance?

Your company-specific achievement of ITAR compliance starts with a Statement of Registration. The DDTC will inform your company if you have any information missing from the registration. Registration with

DDTC does not immediately mean your business can export. Verify that your company has any required export licenses for sending goods outside the United States.

You must also create a specific documented ITAR compliance program within your operation. This includes information on what records you will keep and how. Distinguish classified and unclassified data to know what you can store in a content cloud management (CCM) service and what must remain in hard-copy format in a secure location on-premises.

Unclassified data stored in a CCM must have secure access and full encryption. Verify your data storage service meets the requirements for ITAR before using it to keep sensitive information.

Consult with an expert in ITAR and other regulatory compliance requirements to ensure your company is fully compliant. Failure to meet ITAR can be costly.

Penalties of ITAR compliance violations

Civil penalties cost up to $500K per violation, while criminal charges incur fines up to $1M

ITAR compliance violations include:

- Omitting or misrepresenting facts for any temporary import or export document
- Falsifying registration information
- Exporting defense articles without DDTC registration
- Sharing or selling USML goods, services, or data to prohibited entities

Penalties for these violations can include criminal or civil fines. Civil penalties may not exceed $500K per offense, depending on the infraction, according to § 127.10. Criminal charges could result in fines up to $1 million, imprisonment for up to 20 years, or both.

One example of a violation of ITAR and the penalties for it is Airbus's fine of $3.9 billion for bribery charges. The company was charged in January 2020 with paying bribes to officials in China and other countries to obtain contracts for selling aircraft. The charges under the Arms Export Control Act (AECA) also indicated that Airbus failed to disclose political contributions, as required under ITAR. This steep penalty indicates the seriousness of the charges and the years-long violation from Airbus.

Another incident involved ITT Corporation, which marked the first case of a major defense contractor charged under the AECA. In 2007, the company pleaded guilty to sending night-vision systems to China and other nations with restrictions to receiving exports of defense articles. The company paid a total of $100 million in fines.

The penalty included $2 million in criminal fines, $28 million forfeited profits to the United States, a $20 million penalty to the Department of State, and a $50 million deferred prosecution penalty. ITT Corporation had the opportunity to reduce the $50 million deferred prosecution penalty by investing the same amount in furthering night vision research to ensure the United States keeps its technological advantage.

Types of defense articles

Defense articles include items listed in the USML and are classified across 21 categories

ITAR defines defense articles in the Code of Federal Regulation (CFR) in § 120.6 as any item or technical data enumerated on the USML that is

outlined in § 121.1. Defense articles, services, and data fall into 21 categories on the United States Munitions List. These categories are the following:

1. Firearms, such as fully automatic weapons up to 50 calibers and those using caseless ammunition
2. Guns and armament greater than 50 calibers, including flamethrowers with ranges greater than 20 meters
3. Ammunition and ordnance and related handling equipment
4. Missiles, bombs, mines, torpedoes, and launch vehicles
5. Explosives, incendiary agents, propellants, and related equipment
6. Naval equipment and surface vessels, such as combat vessels and warships
7. Armored combat ground vehicles
8. Aircraft and related equipment
9. Military training and related training equipment
10. Personal protective equipment, such as body armor
11. Military electronics, including electronic warfare equipment
12. Fire control systems, laser, guidance, and imaging equipment
13. Miscellaneous articles and materials, including cryptographic systems and classified articles
14. Chemical, biological, or other toxicological agents and any associated equipment
15. Spacecraft, including satellites and vehicles, and related articles
16. Nuclear weapons and related articles, including simulation tools and technical data
17. Any other classified technical data, defense services, or articles not elsewhere mentioned
18. Directed energy weapons, such as those that cause lethal effects or disrupt electronic circuitry
19. Gas turbine engines, such as turbojet and turbofan, and associated equipment
20. Submersibles and related articles, including military submarines and antisubmarine warfare vehicles

21. Technical data, articles, and defense services not otherwise enumerated, including data and services relating to the above categories or future additions to the USML

Defense technical data in the above categories also include models, mockups, physical forms, or other means of gleaning plans for articles. Incomplete parts, such as moldings, castings, machined components, extrusions, and other unfinished parts that could allow someone to determine the properties, materials, function, or geometry are also part of the articles prohibited for sharing. ITAR doesn't prohibit marketing function information or providing general descriptions.

An amendment to ITAR in 2020 further specified the types of articles included in the first three categories on the USML. It also indicated that goods not under ITAR compliance still needed to meet Export Administration Regulations (EAR).

This change also included an Encryption Rule. This rule outlines how companies share and store technical data. Cloud-based information would not be exported data subject to ITAR as long as it was:

- Unclassified
- Fully encrypted from end to end
- Not deliberately sent or received from a country on the list of nations under restrictions and outlined in § 126.1 or the Russian Federation

The information cannot be stored in servers in nations listed in § 126.1 or the Russian Federation. Those changes increase the potential cloud server locations from beyond the United States.

How to secure your ITAR data

box BLOGS

Your company's ITAR data will depend on what your operation does. You must first identify and separate classified information for physical storage at your facility in a highly secure location.

You can store unclassified information in a CCM of your choice. Check with your cloud content management service to verify that they use appropriate encryption methods as indicated by the Encryption Rule. You must maintain documentation of the encryption methods used by the storage system before you upload any data to the system.

A system must use a minimum of Federal Information Processing Standards (FIPS) 140-2 standard or another encryption method equal to or stronger than Advanced Encryption Standard (AES) 128 bits security. CCM companies cannot obtain certification for having this level of ITAR-required security. Individual companies must research their storage providers to verify the security methods used meet the required standards.

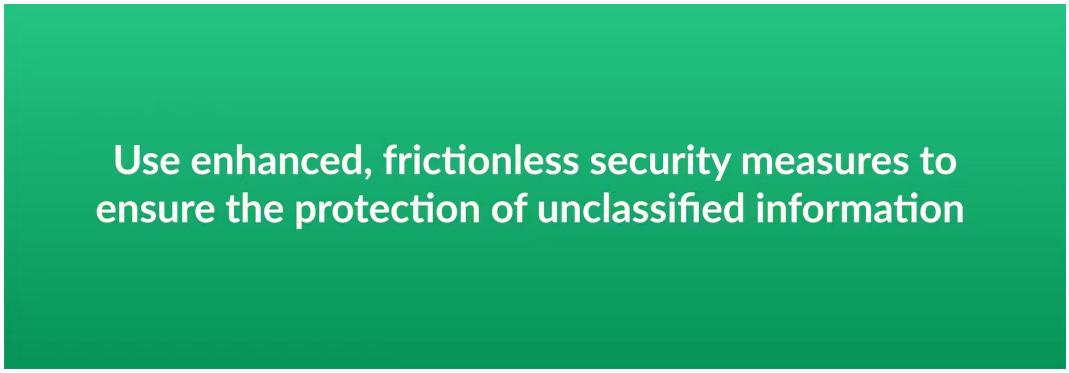
To secure your ITAR data, you should also:

- Determine who has permission to access unclassified, secured ITAR information and which pieces of information they can access
- Keep regular tabs on these individuals and deactivate any who move away from the company — or who change positions and no longer require access to the secure data
- Eliminate any files with global access
- Create groups for files that will require several people to access them
- Avoid letting everyone in the company have free access to any folder in secure storage.

box BLOGS

Monitor the system and keep logs of all who access securely stored folders or files in the cloud. This audit trail becomes part of your proof of security.

Secure sharing of ITAR data with end-to-end encryption



Secure sharing of ITAR data requires end-to-end encryption. This type of encryption keeps information in a coded format that someone without the decryption key cannot view. Only authorized individuals will have the decryption key when they receive the information.

Basic security features for protecting remote data help secure ITAR information, too. Using enhanced, frictionless security measures such as two-factor authentication (2FA), multilayer watermarking, and secure data lifecycle governance can protect unclassified information on CCM while maintaining ITAR compliance.

Box's approach to ITAR compliance

We created the Content Cloud to protect user information via FIPS 140-2 certification and AES 256-bit encryption. Our customers have the option of choosing their own managed encryption keys, too.

Security features we provide to ensure data stays protected include:

- 2FA
- Native verification of ownership for devices
- Classification-based access controls
- Encryption in transit and at rest
- In-depth audit logs

Organizations at the highest levels of government trust Box with keeping their data secure. We have received Department of Defense (DoD) Level 4 authorization. This authorization allows for the DoD to store Controlled Unclassified Information (CUI) and securely share it to facilitate logistics, plan acquisitions, protect health information, and provide mobility support for those within the services. Part of this Impact Level 4 authorization includes Export Control data.

Ourf security also has backing from authorization through the Federal Risk and Authorization Management Program (FedRAMP). Authorization from FedRAMP verifies that CCM companies have the elevated security system for data storage and compliance required to manage non-classified information handled by civilian agencies of the federal government.

Government agencies trust Box to provide a full suite of solutions for their operations. That's because we securely store unclassified ITAR data in a fully encrypted format during storage and transit.

Learn more about Box

Box serves government agencies, manufacturers, warehouses, distributors, third-party suppliers, and other entities under ITAR requirements. Our cloud platform delivers frictionless security and compliance with end-to-end data encryption, 2FA, and complete lifecycle data governance. With comprehensive capabilities to build scalable retention, the Content Cloud empowers businesses to maintain ITAR compliance and protect confidential data, including their munitions plans .

Government, manufacturing, tech, healthcare, defense, and other industries rely on the Content Cloud for secure collaboration, information sharing, file storage, and seamless integrations. Our customizable security options help ensure compliance across regulations, while our security

box BLOGS

provides dynamic, multilayer watermarking; seven sharing roles; organization-wide sharing controls; link expiration; and SSO support with all major providers.

Get started with Box today or contact us to find information on custom solutions.

**While we maintain our steadfast commitment to offering products and services with best-in-class privacy, security, and compliance, the information provided in this blogpost is not intended to constitute legal advice. We strongly encourage prospective and current customers to perform their own due diligence when assessing compliance with applicable laws.