ITAR COMPLIANCE CHECKLIST

Guide to compliance and information security requirements and best practices for ITAR compliance

archTIS

TABLE OF CONTENTS

COST OF ITAR VIOLATIONS

FLIR fined $30 million for exports and re-exports by FLIR to FLIR AB of ITAR-controlled Defense Articles and Technical Data to Foreign Person employees.

Honeywell fined $13 million for unauthorized exports and retransfers of ITAR-controlled technical data in the form of engineering files to several countries across three continents.

Bright Lights USA fined $400,000 for transfer unauthorized defense components and technical data to foreign persons in the People's Republic of China.

VTA Telecom Corporation (VTA) fined $1,869,372 fine under EAR and placed under a three-year administrative debarment under ITAR for six unauthorized exports made or attempted to Vietnam that are controlled on the U.S. Munitions List (USML).

EXECUTIVE SUMMARY

The United States government has established strict regulations to safeguard its intellectual property and military superiority. Compliance with the International Traffic in Arms Regulations (ITAR) is imperative for companies that are involved with U.S. defense technologies and data. Failure to comply can lead to severe legal and financial repercussions, as well as reputational damage. To avoid these risks, organizations must establish robust ITAR compliance programs and provide training to employees on the requirements.

WHAT IS ITAR?

The International Traffic in Arms Regulations or 'ITAR' are issued by the U.S. State Department to control the export and import of defense-related articles and services on the United States Munitions List (USML), such as military hardware, guidance systems, submarines, armaments, military aircraft, IT and software. The purpose of ITAR is to control access to specific types of technology and their associated data to prevent the disclosure or transfer of sensitive information to a foreign national.

WHO MUST COMPLY WITH ITAR?

If your organization is doing business with U.S. Defense, ITAR likely applies to you. Any organization that handles, designs, sells, or distributes items on the USML, must be ITAR compliant.

All U.S. companies, research labs, and universities involved in the manufacturing, exporting, and brokering of defense articles, services, or technical data must register with the Directorate of Defense Trade Controls (DDTC) and comply with ITAR regulations. Additionally, product development plans, hardware specifications, source code, and other sensitive technical data must be adequately secured in accordance with ITAR guidelines.

WHAT IS TECHNICAL DATA UNDER ITAR?

ITAR § 120.33[1] defines technical data as any of the following:

1. Information that is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles on the USML and the 600-series items on the Commerce Control List (CCL), including blueprints, drawings, photographs, plans, instructions or documentation.
2. Classified information relating to defense articles and defense services.
3. Information covered by an invention secrecy order.
4. Software directly related to defense articles.

WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE WITH ITAR?

The consequences of failing to comply with export regulations are severe, with the possibility of facing fines of hundreds of thousands of dollars for each civil violation of ITAR regulations. With penalties of $1 million+ per violation, non-adherence to export laws can easily cost an organization millions of dollars. Organizations can also be 'debarred' or lose the ability to export defense articles. The penalties for willful misconduct are even more severe, with criminal consequences. In such instances, apart from major multi-million dollar fines, the violators can also face imprisonment of up to 20 years.

[1] https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120#120.33 ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

ITAR COMPLIANCE CHECKLIST

Unlike CMMC, there is no ITAR certification program, just a responsibility to register with DDTC and comply with the terms of the regulation. Organizations must develop, implement, and maintain their own compliance programs.

Use this checklist to assist with best practices for implementing an ITAR compliance program. If you're unsure of what's required, seek expert advice.

1. Determine If ITAR applies to your organization

Start by reviewing the USML list to understand which defense articles, services, or data are applicable to your organization and covered by ITAR. Assess any associated threats or vulnerabilities and formulate risk-based compliance plans for physical and information security to assist with mitigation and compliance.

2. Register your company with the Directorate of Defense Trade Controls (DDTC)

U.S. companies must register with DDTC as quickly as possible if any ITAR-controlled activities or defense articles apply to your organization. Typically, registration is a precondition to the DDTC issuing any import/export license or other approval, unless you are granted an exception by the DDTC. Registration must be renewed annually, so be aware of expiration and renewal dates and processes.

3. Obtain necessary export/import licenses and exemptions

Before U.S. companies export or temporarily import defense-related articles, including technical data, they must first obtain proper approval and licensing from the DDTC unless the temporary import qualifies for an exemption. If an exemption applies, you must follow the documented procedures and file any required documents. Permanent import of defense articles is regulated by the Department of the Justice's Bureau of Alcohol, Tobacco, Firearms and Explosives.

4. Train all employees in ITAR policies

Implement employee training programs to ensure all employees and contractors are educated on ITAR handling and sharing policies for physical items and technical data, and any internal processes for identifying and safeguarding ITAR-related materials on company networks and mobile devices.

5. Ensure only U.S. Citizens in the U.S. can access ITAR data

Access to ITAR-controlled data is restricted to employees who are U.S. citizens located in the U.S. Any U.S. companies operating abroad must obtain State Department authorization before sharing ITAR data with their local staff. Third parties who are involved in ITAR work must also comply with this requirement. However, there are specific exemptions for allied countries.

To properly safeguard ITAR-controlled information, implementing technology such as attribute-based access control (ABAC) policies can restrict access and limit sharing based on various factors such as the user's citizenship, clearance level, exemptions, and other attributes. This helps ensure that only authorized individuals have access to ITAR information and that it is shared only with those who are allowed to see it.

6. Implement record-keeping and auditing protocols

Ensure that all activities related to ITAR are documented, including but not limited to registration, manufacturing, acquisition, and disposition, as well as any minutes, notes, drawings, etc. Organizations are also required to maintain ITAR-related transaction records for five years and furnish them to DDTC upon

request. It is recommended to create an audit team that regularly reviews ITAR policies and record-keeping procedures.

7. Verify that your supply chain partners are ITAR compliant

As an organization dealing with ITAR-regulated data, it is crucial to ensure that all third parties and subcontractors with whom you share such data comply with the regulations and have their own access controls in place. To help ensure compliance, notify them when materials are ITAR-controlled and secure end-user statements to attest that they understand what is required of them under ITAR.

8. Do not share data with individuals outside the U.S. or from prohibited countries

It is strictly prohibited to share any ITAR data with foreign individuals without the proper licensure. Under no circumstances should you share ITAR data with anyone residing in a country on the prohibited countries list. You should employ technology that can proactively prevent the sharing of ITAR data with unauthorized individuals to prevent human error.

9. Control data access on all systems and devices

Currently, there are no established regulations or certification programs for cybersecurity under ITAR. DDTC expects organizations to ensure that processes are in place for securing access to, handling and sharing of ITAR data to protect against cyberattacks and other threats. They do, however, make some security recommendations, including:

- Having clear policies, procedures, and training programs in place.
- Controlling access to ITAR-controlled data on file sharing, cloud storage, and collaboration applications to ensure only authorized personnel can access data.
- Ensuring foreign employees do not have access to ITAR data.
- Using end-to-end encryption for data in transit or stored on mobile devices, such as phones and laptops, that is FIPS 140-2 compliant or by other cryptographic means is comparable to the Advanced Encryption Standard (AES-128).
- Employing intrusion detection systems.
- Logging and controlling access to networks and applications that contain ITAR-controlled technical data.

10. Implement FIPS 140-2 compliant encryption

While encryption is recommended as a best practice by ITAR, actual encryption requirements were added in ITAR § 120.54(a)(5). They apply to “activities that are not exports, reexports, retransfers, or temporary imports” regarding the sending, taking, or storing of unclassified technical data without an export/import license, including:

- Allowing the transfer of unclassified technical data without the need for licenses, provided it is secured with end-to-end encryption that is FIPS 140-2 compliant or an alternative that meets AES-128 criteria.
- Ensuring technical data is not backed up to servers in foreign locations unless it meets ITAR § 120.54(a)(5) criteria for end-to-end encryption.

11. Report ITAR violations immediately

Despite having all the proper precautions, mistakes and malicious activities can occur. In the event of an accidental or deliberate ITAR violation, you must immediately report it to the DDTC. Not doing so can result in fines, criminal penalties, and debarment.

USML CATEGORIES

The US Munitions List (USML) is a comprehensive list of defense articles, services and related technical data that spans 21 categories:[2]

Category I: Firearms and Related Articles

Category II: Guns and Armament

Category III: Ammunition and Ordinance

Category IV: Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines

Category V: Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents

Category VI: Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents

Category VII: Ground Vehicles

Category VIII: Aircraft and Related Articles

Category IX: Military Training Equipment and Training

Category X: Protective Personnel Equipment

Category XI: Military Electronics

Category XII: Fire Control, Laser, Imaging, and Guidance Equipment

Category XIII: Materials and Miscellaneous Articles

Category XIV: Toxicological aAgents, including Chemical Agents, Biological Agents, and associated equipment

Category XV: Spacecraft Systems and Related Articles

Category XVI: Nuclear Weapons Related Articles

Category XVII: Classified Articles, Technical Data and Defense Services not otherwise enumerated

Category XVIII: Directed Energy Weapons

Category XIX: Gas Turbine Engines and Associated Equipment

Category XX: Submersible Vessels and Related Articles

Category XXI: Articles, Technical Data, and Defense Services not otherwise enumerated

[2] https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121

SECURING ITAR-CONTROLLED DATA AND ACCESS

When it comes to cyber security and encryption, the guidance from DDTC for ITAR is fairly standard. You must implement robust access control and data protection mechanisms to safeguard ITAR-controlled data.

There are multiple factors you must evaluate when determining access and handling policies for ITAR-controlled data, including:

- User citizenship
- User clearance level and caveats
- Exemptions
- Document categorization (e.g., ITAR, EAR, etc.)
- Document classification (e.g., Controlled Unclassified, Public Trust Position, Confidential, Secret, Top Secret, Compartmented)
- Device, Browser or Operating System (e.g., iPad, Android, tablet or another mobile device)
- Geography/location of the user requesting access
- Other regulations that may apply, including EAR, DFARS, CMMC, etc.

To ensure compliance with the ITAR, it is important to use classificational tools that can accurately identify and tag ITAR data. These tags can then be utilized by your data security and access management tools to restrict access to authorized individuals and control the conditions under which the data can be accessed and shared with others (e.g., applying end-to-end encryption). This way, you can avoid any potential violations by maintaining strict control over who has access to ITAR data and who it can be shared with.

archTIS has deep experience helping companies implement solutions for data-centric access control and protection of ITAR-controlled data. We offer a range of products, from secure document management platforms with built-in ITAR data controls to solutions for managing ITAR-controlled data in your Microsoft file sharing and collaboration applications.

Our products use policy-enforced attribute-based access control (ABAC) and data protection to dynamically secure data in real time. With archTIS, it's easy to manage ITAR access controls and data security with precision and efficiency.

Kojensi Secure Document Management and Collaboration Platform

Kojensi is a document management and collaboration platform designed from the ground up to meet the specific needs of the Government, Defence, and Defence Industry, including ITAR. Kojensi is designed with ITAR controls to assist organizations with meeting their compliance obligations. Kojensi's ITAR compartments enforce ITAR dissemination controls and visually alert users that they are working on export-controlled materials to reduce human error. With Kojensi, securely share any number of files that may have different export controls internally, with partners and with Defense.

NC Protect for M365, GCC & GCC High and SharePoint

Microsoft Partner

Member of Microsoft Intelligent Security Association

Microsoft

NC Protect simplifies the management of ITAR-controlled information in Microsoft 365, GCC, GCC High, SharePoint Server, and file shares. ABAC policies dynamically secure ITAR data access based on user nationality, location, device and file classification. Policies can also apply data protection, including encryption, visual markings and other security controls automatically based on a document's classification/ sensitivity to ensure ITAR data remains secure while auditing file access and actions.

Contact archTIS today to learn more about our information security solutions, specifically designed to meet the unique security and compliance needs of the Defense industry.

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, SharePoint Server, NetApp ONTAP, Nutanix Files and Windows file shares.

For more information visit archtis.com. Follow us on twitter @arch_tis.

archTIS

archtis.com | info@archtis.com

Australia | United States | United Kingdom