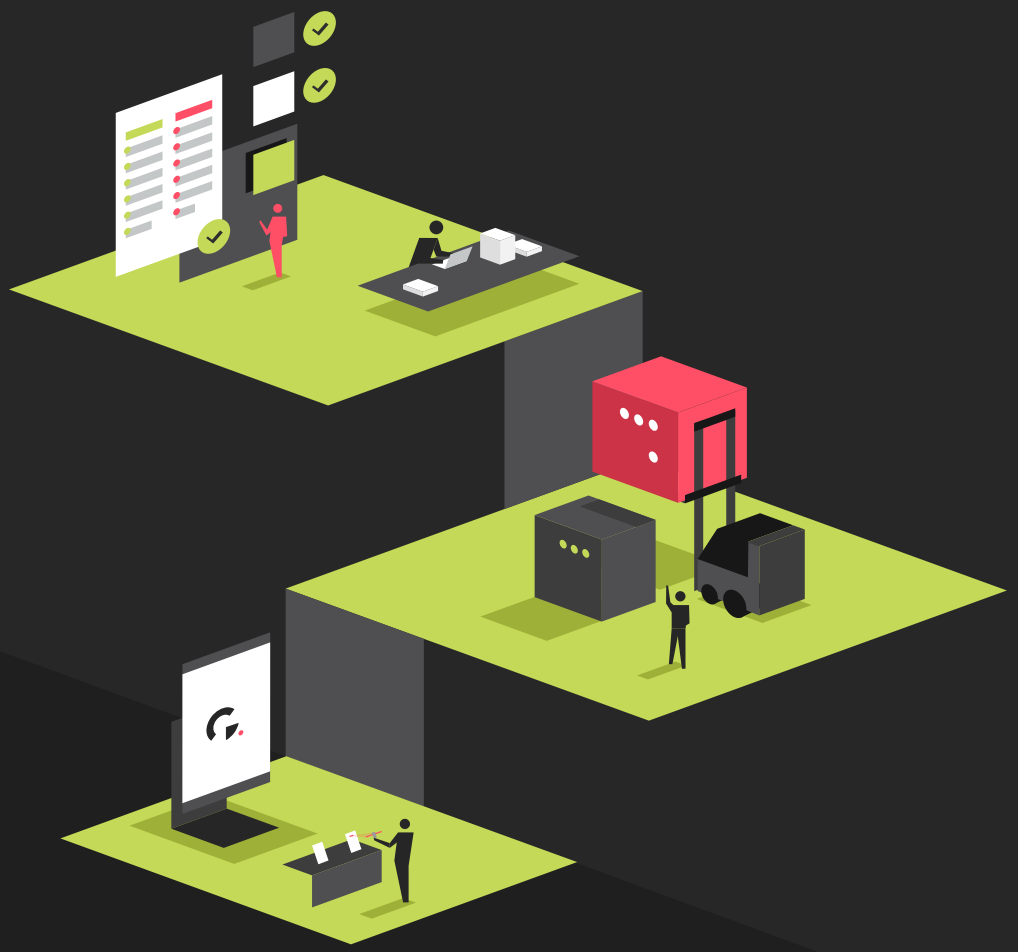
TRACTION Guest.



ITAR compliance for manufacturing organizations.

Complying with ITAR requirements in a manufacturing facility is a complex task with very strict standards. Many branches of the United States government have a stake in defining, monitoring, and auditing International Traffic in Arms Regulations (ITAR) compliance, which can impact manufacturers (including aerospace, food and beverage, automotive, pharmaceutical, and many others), exporters, brokers of defense articles and defense services.

Failure of manufacturers to comply with ITAR visitor requirements can result in severe penalties, ranging from civil and criminal prosecution, including a business fine up to $1 million for each violation, a civil penalty of $500,000 per violation, prison sentences, and disruption of business, not to mention the reputational damage that comes from being connected, or even suspected of being connected with arms trafficking.

In this eBook, we will explore what ITAR compliance means to manufacturing businesses, and what risks manufacturing organizations run if they are not following requirements.

Learn more about

- What does ITAR compliance mean for manufacturers
- Common ITAR violations
- Consequences of non-compliance
- <svg id="ff4b8bc0-a131-49da-955a-215ae6afa52e" data-name="Layer 1" xmlns="http://

Table of contents.

What is ITAR compliance for manufacturing and supply chain organizations?

International Traffic Control Regulations (ITAR) control the export of goods, services, and data listed on the United States Munitions List (USML). Manufacturers are required to adhere to a wide-range of regulations to ensure ITAR compliance is met in their operation. Any manufacturer with a connection to items on the USML, in any way, must address ITAR compliance across the entire organization including functions such as:

- Research and development
- Manufacturing
- Importing
- Exporting

Further, any technical data listed in the USML is also required to meet ITAR compliance standards. This is commonly referred to as technician data, which includes:

- Blueprints
- Documentation
- Repair and maintenance
- Assembly instructions
- Operations manuals

At the core of ITAR is ensuring that this sensitive data, with connections to defence technology and operation of the military, is restricted to US citizens. And with US operations stationed worldwide, that data can not be accessed without restrictions in place to ensure only those who have authorization to see it are able to.

Navigating ITAR compliance guidelines.

The requirements that make up the ITAR legislation have been structured and designed to allow the government flexibility and control over military articles and services. This can be challenging for those trying to interpret ITAR compliance, however, a basic checklist of best practices to follow will help when building an ITAR compliance program. They include:

- Screening all parties and verifying citizenship
- Ensuring names are accurate and complete
- Tailoring compliance programs to specific business type
- Keeping complete, detailed visitor records for at least five years
- Records must be organized and easily accessible
- Securing all physical and digital access points
- Monitoring and regularly reviewing compliance programs

ITAR requires that any person or company who engages in the business of manufacturing defense articles or repairing, maintaining or providing defense services is required to register with the current United States Department of State.

Registering is only the first step, and it's expected the employees are educated and trained on ITAR regulations in order to ensure compliance. Manufacturers also need to **demonstrate a proactive implementation** of ITAR best practices in all their facilities, including **audit readiness** and **training protocols**.

Common ITAR violations.

There is a long list of actions that could cause a manufacturing concern to fail at complying to ITAR policies. ITAR goes under significant changes each year, so compliance teams need to continuously review their best practices, redefine their compliance policy and educate their entire organization on those new regulations.

The U.S. Department of State lists all violations, penalties and oversight agreements reached with companies who have failed to meet ITAR compliance. Since 2011, there have been 18 violations where the State Department has reached a consent agreement.

Typical infractions or non-compliance incidents tends to fall in the following categories:

Willfully failing to comply.

Some of the most serious consequences, including civil and criminal penalties, go to manufacturers that purposefully fail to comply with ITAR regulations. This includes companies who do not want to invest in the proper technologies, data security measures or compliance teams due to costs or a perceived lack of a risk of getting caught. However, willfully failing to comply increases the risk of violating ITAR standards, and puts the organization at a higher-risk for the largest fines and penalties.

Accidentally failing to comply.

While some manufacturers will actively not comply with ITAR, others make accidental violations. ITAR is updated yearly, and regulations can change, resulting in missing a critical new compliance standard, security requirement or data collection opportunity. It's possible that security standards will lapse as ITAR evolves, leading to an accidental failure to comply. These types of failures, where it is a result of an accidental oversight do lead to penalties. However, they generally result in lower fines, which can be waived if the organization follows an alternative disclosure program.

18
violations
since 2011

Not verifying exporting data.

The State Department limits which countries technical data that falls under ITAR can be transmitted to, including China, Cuba, and Venezuela. Manufacturers cannot send data to customers in those countries, and there is even a responsibility for them to know who their customer's customers are, to ensure that data being sent to them is not going to a company located in one of these restricted locations. This is a common mistake, as manufacturers can fail to investigate the entire chain of people who will have access to the goods or information to ensure that even a customer's customers meets ITAR compliance.

Inaccurate recording keeping.

Improper keeping of records commonly leads to violations of ITAR compliance. This includes the omission of data and facts that are relevant to ITAR compliance when submitting ITAR reports, or failing to report a violation. Record keeping and data collection are core aspects of ITAR, which can include citizenship information, nondisclosure agreements and licenses for people who will have or need access to information that falls under ITAR.

Consequences of ITAR non-compliance.

Failing to comply with the strict ITAR requirements, as described in the previous section, has severe consequences. While it's most common to think of consequences in terms of fines, which can be as high as $1 million per violation, other damaging consequences can come from being non-compliant. The United States government takes ITAR very seriously, which is why they continue to update the compliance regulations annually.

Consequences are based on:

- **Severity**
- **Type**
- **Scope**

Those who willingly choose to ignore compliance rules will face harsh penalties, while low-risk, and accidental compliance violations typically receive smaller fines and a chance to mitigate the situation. But there are other consequences to the manufacturing business itself that can derive from an ITAR violation.

Financial penalties.

The severity of fines can range from $20,000 up to $1 million based on the potential risk, type of security breach and whether a manufacturer knowingly circumvented ITAR compliance. This fine is based on per violation, so multiple violations can be financially devastating to an organization who isn't keeping ITAR compliance. The State Department can also apply up to $500,000 to an individual in a civil penalty for each violation.

Loss of exporting license.

Fines are monetary losses that are paid directly to the State Department, but these are only the start of financial losses that could occur. For example, Government contracts could be canceled, due to the organization losing their license to export the goods and services in those contracts. For some organizations, this can result in a complete shutdown of their business if they work significantly or solely with ITAR-controlled goods and services.

Increase staffing mandate.

An organization may also be required under their agreement to hire a compliance officer to overhaul their compliance policy. This new officer will monitor the company's progress in building a proper ITAR compliance program. Some organizations are already adding compliance staff to their security teams and organizational structure. But for some, this is a mandatory position that needs to be created with long-term effects to the business, especially for those who willfully decided to ignore ITAR rules and regulations.

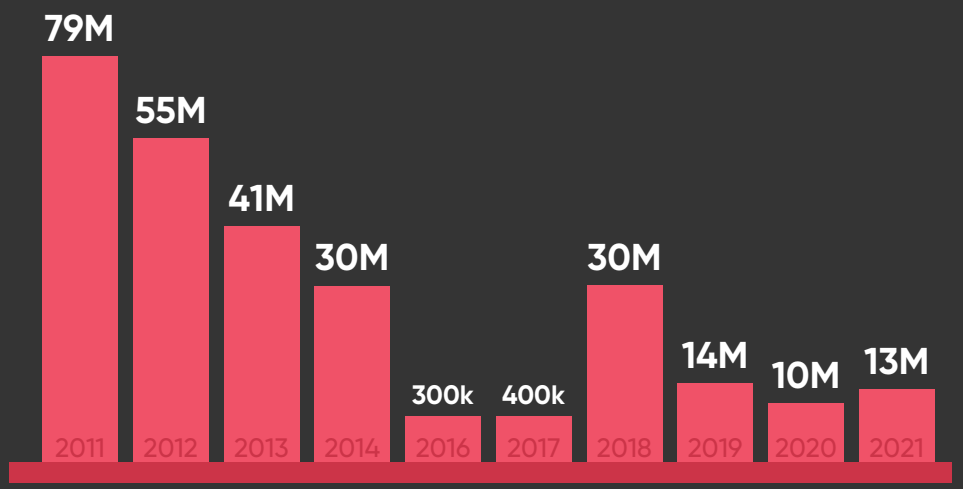
Increased audit frequency.

Those found in violation of ITAR compliance will be subjected to an increase in external audits which must occur at least once each year. These audits will examine ITAR policies, identify gaps and risks with the program, and possibly find additional ITAR violations that result in more fines and penalties. Such additional scrutiny can have a severe impact on resources required to prepare for/support audit demands.

Loss of business reputation.

When an ITAR violation occurs, a company's name is placed on a list published by the State Department (after signing a consent agreement). That list is available publicly, and can result in a loss of business reputation. Customers, prospective customers, government agencies, as well as partners, and employees, can all view this list, read the violations, and see how they occurred.

According to the State Department Consent Agreements list, since 2011 there have been 18 violations of ITAR compliance.



Total of 260M in fines since 2011

What does ITAR mean for workforce security professionals?

Each visitor coming to a manufacturing facility poses an ITAR compliance risk. This includes employees, contractors, and essential visitors, all of whom have to be regarded as a risk when coming into a facility that deals with ITAR-related goods and services.

To protect these facilities, and the technical data related to ITAR compliance, screening is imperative to stay within the regulations, while also promoting a more secure facility. However, the system has to scale with the requirements, and there is risk relying on manual techniques, such as log-books and sign-in sheets to meet compliance. Human error is one of the main sources of accidental ITAR violation.

Under ITAR, it's required to submit audit reports on the visitors coming into a facility. Missing information can result in a compliance violation, and granting access to a foreign national without State Department clearance will result in penalties.

Manufacturers need tools, such as enterprise visitor management to support compliance. Automated systems that gather information and record it for an audit of each visitor that comes into the facility are a critical part of ITAR preparedness. Those tools include:

Electronic logbooks

A system to remove the paper-based and manual logging of visitor information. These are available for auditing purposes.

Entry screening

Facilities with multiple entry points can deploy a system that helps to screen consistently at each gate. This acts as a filter to ensure that only the right people are allowed into the right place to reduce information-access and ensure sensitive information is only viewed by following proper procedures. Through registration, visitors can enter their country of origin and attach a passport or ID to support and verify citizenship.

Automated escalations.

Security teams can be alerted when a visitor responds to questions that would require action. Once a possible risk is identified, security is notified to escort the visitor throughout the facility or deny them entry.

Watchlists.

ID scanning and connections to watchlist databases, including local, national and international databases, screens visitors for possible risks. This includes criminal or violent history, to get a full profile of the visitors entering a facility. Internal watchlists can also ensure those denied access to one facility cannot access another facility.

Visitor management systems provide transparency and accountability when dealing with ITAR compliance, while also adding another level of enhanced security. These systems act as the administrative, documentation and communication tools required to meet ITAR standards, which avoids major penalties and violations.

Summary.

Violating ITAR can have long-lasting effects on manufacturers disrupting current and future business outcomes. Leading organizations are looking to enhance their compliance teams and systems to ensure consistent compliance with ITAR requirements and reduce the risk of non-compliance and penalties.

By taking a proactive approach to managing these compliance practices and policies, manufacturers can avoid millions of dollars in fines and penalties as well as the resulting reputational damage. These policies and procedures will be required if an ITAR violation occurs, so manufacturers can avoid costly consequences by putting them in before a compliance issue happens and avoid consequences altogether.

Over the past decade there have been a number of technological advances and so managing ITAR compliance need not be a daunting task. Leveraging best-practice lessons from other manufacturers, tools such as enterprise visitor management, watchlists, workflow automations, audit automation etc. are becoming commonplace amongst manufacturers seeking to reduce their risk exposure and take proactive steps to ensure ITAR compliance -- to protect the safety of their staff, their partners, and the world at large.

About Traction Guest.

Traction Guest ensures safety and security for employees, contractors, and essential visitors – wherever they work - through our Workforce Security Platform. The platform provides the most advanced enterprise visitor management system (VMS), health and safety controls, critical outreach and alerting, as well as analytics and auditing functionality.

Traction Guest facilitates multi-layered screening and approvals so that security processes can be finely tuned for unlimited locations, types of workplaces, and roles. It's a robust solution to support duty of care requirements and keep people safe in a rapidly changing environment.

- Centrally manage multi-location customizations
- Support employees and non-employees in a hybrid environment
- Standardize and codify compliance requirements
- Solve complex security and safety problems

Global brands across five continents and dozens of industries trust Traction Guest's highly customizable platform to mitigate risk and deliver unparalleled security through an intuitive, touchless, highly branded experience that supports compliance, employee engagement, and duty of care requirements.

TRACTION Guest.

tractionguest.com >

info@tractionguest.com >