titus
by HelpSystems

Protecting Sensitive ITAR Information: A Data-Centric Approach To Export Control Compliance

Including

- ITAR regulations
- Controlling export data
- User-driven data classification
- Safeguarding data
- Supporting data management

Indroduction

While the requirement to control the export of military goods is widely recognized, the challenge of complying with strict government regulations such as the International Traffic in Arms Regulations (ITAR), while keeping systems and processes usable, is less well known.

ITAR covers the transfer of technical data and information relating to goods, as well as the goods themselves. Technical documents, product plans and specifications, design drawings, manuals and financial details may all need to be shared across the supply chain if an ITAR-related project is to be delivered. However, authority needs to be granted and access by unauthorized persons prohibited or the organization and its employees are at risk.

Companies that fail to comply with these regulations – by sending ITAR-controlled information to the wrong recipient, for example – can be fined by the US government, required to make costly reparations, and even face criminal charges. With details of breaches and fines made public, violations are also likely to lead to loss of reputation and damage to the brand.

ITAR Violation

To avoid the types of penalties mentioned, the cost of post-event corrective actions and future governmental scruitny of their business, organizations must proactively introduce changes to their security procedures and processes.

Preventing sensitive technical documents from being leaked to unauthorized people requires a policy-based approach, which ensures disclosure and release of technical data is handled in the right way and provides the required audit trail so that organizations can demonstrate that they have complied. Having a policy is not enough, it has to be enforced regardless of the size or geographical dispersal of an organization or the complexity of their supply chain. This demands a data-centric approach to protection which involves users in classifying information.

While controlling user access and limiting the movement of data is important, taking a data-centric approach in addition to these measures will allow the safe flow of information between organizations to empower efficient, collaborative working.

Controlling Export Data

The Challenge

It's easy to understand why some organizations simply decide to take their chances and 'take the hit' for any violations that are discovered, rather than maintaining control of ITAR-related data. It can feel like a monumental task.

The traditional approach to protection for an organization has always focused on shoring up its perimeter or boundary against external threats, such as hackers attempting to access the network. However ITAR breaches are often a result of human error caused by employees working within the organization, and inside the perimeter. For example, only the members of staff dealing with a particular activity may have approval to use a piece of ITAR controlled data; it cannot be shared with non- approved members of staff.

In addition, firewalls, Cloud Access Security Brokers (CASB), insider threat and intrusion detection and prevention tools are not designed for the extremely complex business environment within which ITAR-related projects are run. With

ITAR In Detail

ITAR (International Traffic in Arms Regulations) protects and controls the import and export of defence-related products, technologies and services. It specifies that information and material concerning defence and military-related technology for items listed on the United States Munitions List (USML) may only be shared with US persons, unless authorisation is given by the US Department of State or a special exemption is granted. UK end-user and consignee companies can gain special project-by-project exemptions without prior approval, for transfers of unclassified technical data – but this is subject to satisfying requirements for screening and record-keeping, including the identification, receipt and tracking of ITAR-controlled data.

supply chains that involves multiple organizations and users in diverse geographical locations, handling many different types of data over a variety of devices, systems and networks, there really is no perimeter.

Project teams today also use collaboration sites and document management systems daily to share information with colleagues, partners, contractors and suppliers, potentially exposing it to accidental export or access by unauthorized users.

Access control – ensuring that authorized users have access to and can share documents appropriately – becomes almost impossible in such an environment. Standard tools such as application-based access and authentication controls, data loss prevention (DLP), Cloud Access Security Broker (CASB) and digital rights management are either not easily scalable, suffer from gaps in defense, or are limited in their coverage.

Low user awareness of compliance requirements around document handling is another problem. It's easy for users to make mistakes when they're used to the protocols in handling local classified material, but less familiar with the handling protocol for unclassified ITAR data, for instance.

It's also important that any controls applied enable safe international communications and trade, rather than introducing processes that will stifle the information flow and make business less productive.

A Data-Centric Approach

All organizations need an information policy to manage and control the handling, use and export of sensitive data both within the company and to external organizations – and this must be actively, consistently and accurately enforced.

A data-centric approach to security is the most effective way to do this. With data crossing the boundaries of organizations and nations, and no clear perimeter to defend, it's the data itself that has to be protected.

Enforcing Policy: User Driven Classification

Classification directs the controlled release of sensitive export data through the use of labelling – ensuring the correct information goes to the correct recipient based on their organization, role and clearance level.

The approach involves the user themselves identifying, labelling and marking ITAR-related emails and documents as part of a compliance program. They simply select the appropriate ITAR-related visual label – for example 'ITAR Controlled' number '8888222b'– from a pre-defined drop-down list before they can send, save or print information. These labels ensure export controlled information is only shared with or made accessible to ITAR-approved individuals.

Involving the user brings export control policies to life; making them deployable and translating them into actionable controls at all points in the project workflow at which sensitive data is being handled.

Users are reminded before they send an email or document that they need to comply with export policy, which dramatically reduces the risk of common, unintentional policy violations, and increases the effectiveness of a compliance program. Asking employees to make decisions about how data is stored and transmitted raises awareness of sensitive information and encourages proper handling across the organization.

Metadata: Safeguarding Against Inappropriate Disclosure

As well as attaching the label in a visual form that's clearly displayed to the user, classification tools also apply it as metadata, embedding a tag into document or file properties that stays with it wherever it goes. This means that protection travels with the data as its flows through or is stored on systems or networks that are administered by non-approved or unauthorized administrators, used for both defense and commercial applications, or have different controls.

The metadata makes it easier to enforce policy downstream, by directing other security technologies such as email gateways, encryption and information rights management (IRM). The marking enables them to apply more accurate security decisions to data by triggering rules so that, for example, any documents or files marked 'ITAR Restricted' might be blocked from being emailed to a high-risk destination or hidden in a shared folder from users who are not working on the project.

Cleaner, Better-Organised Data Across The Boundaries

Data classification can also support data and information management tools, processes and activities, including:

- **Search and retrieval -** making it easier to maintain an audit trail and quickly find documents that are needed for investigations, to prove ITAR-compliance, or to meet information requests from regulators

- **Discovery -** enabling employees to rapidly locate information and understand instantly how it can be used, or whether it can be released
- **Data retention and archiving -** retention rules can also be set for different classifications – for instance, 'keep ITAR restricted files for 10 years'.
  Data security becomes more manageable and realistic when data volumes are reduced, and disposing of data that's no longer needed mitigates legal risks.
  If a document isn't there, it can't be leaked or lost.
  Streamlining data will also cut the costs of both storing and protecting it.
- **Data governance and auditing -** using the data classification label, data governance tools can effectively audit who is accessing sensitive information, and who might be violating policy, and therefore prompt any correcting action. As the amount of data being created and processed by organizations grows exponentially, the demands on reporting will increase
- **Event monitoring and alert -** picking up the metadata labels being applied by users, Security Incident and Event Monitoring (SIEM) tools can ensure that any unusual user behaviour is identified early and the relevant people are notified. For classified data, this could be identifying changes in patterns around the classification of data, for example a user consistently downgrading files from 'ITAR Controlled' to 'Public'
- **Access control -** by connecting with other access control or collaboration tools, labels can be used to dictate who can access a file in a shared area, for example within Microsoft SharePoint

Data classification tools allow security controls, rules and policies to be more consistently enforced, and guide users' decisions on the release of info. The user attaches an appropriate electronic marking to a message, document, drawing or file, which establishes that it requires special handling and allows it to be saved or sent only in accordance with the rules that correspond to that marking. This type of tool seamlessly plugs into standard applications such as Microsoft Office, Outlook, Lotus Notes and CAD applications, which makes classifying messages, documents, drawings and files simple and unobtrusive.

The Cost Of An ITAR Violation:

FLIR Systems

- $30m for alleged unauthorized exports of defense articles, including techncial data and other violations

ITT

- $100m fine for illegal exports of military night vision to China, Singapore and the UK

Boeing

- $10m civilian fine, $2.5m mandated compliance program, corporate restructuring

Lockheed Martin

- $13m fine and mandated compliance program

Loral

- $20m fine, $6m compliance program, corporate executives also fined $100,000 for their role in the violations

IBM East Europe/Asia Ltd

- $8.5m for computer exports

Raytheon

- $8m fine, required to appoint external Special Compliance Officer (SCO) and conduct an extensive classification review

Meggit-USA

- $25m fine for 67 violations ranging from unauthorised export of defence articles to failing to maintain records involving ITAR-controlled transactions

Facilitating An Agile Organization

Data classification supports secure sharing of export-controlled information among project teams, and between an organization and its partners and suppliers, enabling data mobility across global business environments without exposing it to risks.
Embedding classification in the metadata ensures that, for example, any files or documents held in a file store that are labelled 'ITAR-restricted' will be protected on upload to Microsoft SharePoint, and secured for specific ITAR-cleared individuals only.

Export controlled data can also be secured in the mobile environment, with content classification and rules that prevent users working in locations that are subject to ITAR restrictions from accessing sensitive files on the network.

Building A Culture Of Protection And Compliance

Getting users to 'stop and think' about the sensitivity of information before they take action educates them upfront – improving awareness of the value and risks associated with export data, and their duty of care in relation to it. This helps

to build a culture of accountability and ITAR compliance across the supply chain.

The monitoring and reporting capability of data classification tools also enables ongoing auditing of compliance. The visibility they provide of any potential areas of concern – for instance, a number of users who repeatedly label documents incorrectly – allows concerns to be addressed through training or disciplinary procedures.

ITAR: Don't Fall Victim To The Next Data Breach

Organizations that handle ITAR-related material have a duty to control it appropriately; to protect national security, the confidentiality of customers and partners, and also their own employees, business and reputation.

Taking a proactive approach to managing and controlling ITAR-protected information through user-driven data classification reduces the risk of inappropriate disclosure and export control violations. This, in turn, will safeguard against the fines, remediation costs and criminal penalties, including jail sentences for those held accountable, that can follow.

Importantly, this approach also educates users on procedures and their responsibilities, ensuring that they follow best practice. Meanwhile, the business is not forced to restrict information sharing to meet its compliance obligations, compromising its productivity, efficiency and agility.

In the event of an investigation or contravention of ITAR regulations, user-driven data classification allows an organization to quickly demonstrate its compliance position, with a clear audit trail and accurate reporting that proves information is being appropriately controlled and documented.

"Because we elected to use a very obvious and mandatory marking system, the ITAR consideration is front and centre for our staff every day. ITAR is now part of our minute-to-minute considerations and decision making, significantly reducing the opportunity for inadvertent or unconsidered non-compliance."

Lachlan Burg, Director - Human Resources & Shared Services for QinetiQ

Global brands trust us to protect their sensitive data:

More Information

For more information about how you can implement a data classification solution as part of your data protection strategy, please **contact us**

titus
by HelpSystems
www.titus.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.