BOOST YOUR INFORMATION SECURITY TO MEET ITAR COMPLIANCE

5 Essential Checkpoints and Strategies to Assist with ITAR Information Protection Obligations in Microsoft 365, Teams & SharePoint On-premises

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Complying with requirements of complex regulations such as the International Traffic in Arms Regulations (ITAR) can be a significant challenge, especially within today's global and complex supply chain, where business can blend and blur the traditional lines of geography and locality. We collaborate and share information daily with our partners, suppliers, subcontractors, and our clients, using numerous combinations of information systems.

When dealing with sensitive information that requires comprehensive controls, having information systems that enable and enforce access controls that adapt to the business need becomes an essential problem to solve for your business.

The good news is the Microsoft systems that you may already be using can become more secure by using comprehensive and validated security methodologies such as Attribute-based Access Control (ABAC), and extending dynamic policy enforcement to your information management and collaboration systems.

This white paper reviews the 5 essential checkpoints of ITAR and provides strategies, recommended security controls and tools to assist with information protection obligations in Microsoft 365, Teams and SharePoint on-premises.

WHAT'S AT STAKE?

Fines paid for unauthorized exports of technical data

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

UNDERSTANDING THE FIVE Ws OF ITAR:

To properly protect data and meet ITAR compliance you must be able to quickly determine the following factors when sharing any regulated content:

- What is ITAR?
- Who does it apply to?
- Where does it apply?
- Why is compliance important?
- What is at stake if you are non-compliant?

UNDERSTANDING THE FIVE Ws OF ITAR:

What are ITAR and EAR?

The International Traffic in Arms Regulations (ITAR), are issued by the United States government to control the export and import of defense-related articles and services on the United States Munitions List (USML), and cover items such as military hardware, guidance systems, submarines, armaments, military aircraft, IT, and defense specific software. In short, the U.S. Government requires all manufacturers, exporters, and brokers of defense articles, defense services or related technical data to be ITAR compliant.

The US Department of State has authority over export control of all articles, services, and related technologies under ITAR, which is managed by the DDTC (Directorate of Defense Trade Controls), with items under ITAR protection listed on the USML.

If you manufacture, export, sell, or support any items covered by the ITAR protections, you must be registered with the DDTC, understand and agree to comply with the regulations, and self-certify that you are in compliance with ITAR.

Export Administration Regulations (EAR) are issued and managed by the United States Department of Commerce to control the export of items which are designed for a commercial purpose which could have military applications (‘dual use items’), such as computer hardware and software (Commerce Control List).

Applying these regulations to your business and to those within the greater supply chain introduces additional costs, rigor, and complexity into your processes.

Who does it apply to?

These regulations apply to almost everyone conducting business with US Defense and Defense suppliers. The US based legislation aims to control access to specific types of technology and their associated data, to prevent the disclosure or transfer of sensitive information to an unauthorized or prohibited foreign national.

If your company falls under ITAR or EAR and you need to collaborate on product development plans, hardware specifications, source code, or other sensitive information, then you need to implement security controls over the applications being used to share and collaborate on regulated information to ensure compliance.

These ITAR controls and requirements are implemented with the intent of improving the security for the entire supply chain – including any subcontractors

Where does it apply?

These controls apply to any organization, including internal and external users or groups, that have access to ITAR regulated content in the USA and in countries as defined in the regulations.

Information and technical data requiring this protection and management can be referred to as Covered Defense Information (CDI), Controlled Technical Information (CTI), or as Controlled Unclassified Information (CUI).

ITAR compliance can pose challenges for companies, since data related to specific technologies may need to be transferred over the internet, via collaboration applications such as Microsoft 365 and SharePoint, or stored locally outside of the United States.

These requirements are not new - they have been mandatory since December 31, 2017.

A Defense Federal Acquisition Regulation Supplement DFARS 252.204-7012 aims to encourage all participants in the supply chain to be proactive in the protection of CDI. As a supplier you are required to demonstrate compliance for own business, as well as taking steps to ensure that your subcontractors comply, in order to help strengthen information security along the entire supply chain.

Your subcontractors are responsible for their systems, and for ensuring that their own practices also comply with the DFARS and NIST 800-171, however it is also your responsibility to ensure that secure information sharing practices and systems are in place, before you share CDI with that subcontractor and others in the supply chain.

Why is compliance important?

It is extremely important that you understand and comply with these regulations as ITAR and EAR violations can pose a huge risk for impacted companies and the surrounding industries – it is vital that we all have a common understanding of the requirements and what you are signing up for.

What is at stake if you are non-compliant?

ITAR violations carry a civil penalty of US $1 million+ per violation. Defense contractors have been fined tens of millions of dollars for breaches for failing to control access to EAR and ITAR regulated data.

Violators can also be 'debarred' or lose the ability to export goods.

Notably, violations can impact more than just the company's bottom line – criminal penalties of up to 20 years in prison are also possible.

BEGINNING THE ITAR COMPLIANCE JOURNEY

Complying with ITAR can be complex and challenging, irrespective of the size of your organization.

This compliance requires registration with the DDTC, implementing a Compliance program, as well as meeting a number of controls to ensure that your ICT systems are suitable for protecting relevant information.

The requirements for data protection are complex, with numerous different contexts in play.

It's critically important to understand and consider the data that is likely to be relevant to your contract!

This includes data created throughout the contract lifespan, as well as protecting that data, and costs associated with the protection requirements.

Warning signs of ITAR and EAR non-compliance

To properly protect data and meet ITAR compliance you must be able to quickly determine the following factors when sharing any regulated content:

- User clearance level and caveats
- User citizenship
- Document/item clearance level (i.e. Top Secret, Protected, classified, sensitive, etc.)
- Device (i.e. browser or OS such as iPad, Android, tablet or other mobile device)
- Geography and access locations

If you are not able to address the points above easily when users access and share information, then you are potentially in violation of ITAR.

FIVE KEY ITAR FACTORS:

To properly protect data and meet ITAR compliance you must be able to quickly determine the following factors when sharing any regulated content:

- User clearance level and caveats
- User citizenship
- Document/item clearance level (i.e. Top Secret, Protected, classified, sensitive, etc.)
- Device (i.e. browser or OS such as iPad, Android, tablet or other mobile device)
- Geography and access locations

FIVE CONTROLS RELEVANT TO TECHNICAL DATA PROTECTION

1. Encryption
2. Granular access control
3. Persistent access control
4. Detection and Prevention
5. Comprehensive audit capabilities

HOW CAN I ENSURE DATA COLLABORATION IS SECURE AND COMPLIANT?

It is important to understand how to secure your ITAR-controlled data in your collaboration and information sharing applications: including but not limited to Microsoft 365 applications, SharePoint, other file share providers, Teams/Slack, and even email.

Here are some best practices to guide you on how you can properly secure ITAR and EAR controlled data:

- Establish and maintain an information security policy.
- Implement zero trust network access methodologies.
- Regularly test networks, security systems and processes.
- Implement attribute-based access control (ABAC).
- Protect sensitive data with encryption and usage restrictions (e.g. restrict printing, copy/paste functions, downloads, etc.).
- Watermark documents to track chain of custody and remind users of a document's sensitivity.
- Track and monitor all access to network resources and sensitive data.
- Implement measures to prevent the loss of ITAR and EAR controlled data through data misuse, accidental sharing, or theft.

Requirements will vary from company to company; however, this list provides a strong starting point for securing sensitive data to meet ITAR and EAR compliance. You should consult an expert if you are unsure of what is required.

WHAT TECHNICAL CONTROLS ARE NEEDED FOR MY IT SYSTEMS?

The NIST Special Publication (SP) 800-17 details Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

DFARS 252.204-7012 includes terminology and definitions of what information and controls are needed.

With these updates and publications in effect, organizations can now store, share, and collaborate on this data in cloud environments, as long as it has appropriate controls in place.

Controls relevant to Technical Data protection to meet these include:

1. **Encryption:** The mechanism by which data is encrypted at every stage from storage, transit, until it gets to the recipient, such that intermediaries do not decrypt the information.
2. **Granular access control:** The ability (on a per-object basis) to both measure and enforce access based on a set of specified criteria or rules - This can include a user's attributes, such as their nationality, clearance, or organization.
3. **Persistent access control:** The means by which access controls are enforced wherever the data goes, whether by email, chat, or other form.
4. **Detection and Prevention:** Includes scanning for relevant information at relevant points and automatically enforcing the relevant access controls and encryption to prevent the information controls from being accidentally missed by users.
5. **Comprehensive audit capabilities:** Detect and log all activities and attempts related to the information, maintaining context and control throughout collaboration and sharing.

REDUCING COMPLEXITY AND COST

The complexity of designing, building, and assessing an environment to satisfy these requirements is a significant challenge, requiring specialists with deep experience, along with careful planning and comprehensive technical expertise. There is a need to maintain the environment in line with the security expectations, as well as the risk management expectations that come with handling sensitive information.

Appropriately securing physical premises, information systems, and the personnel needed represents significant cost and complexity to organizations. This results in environments of this nature being prohibitively expensive, both to build and maintain - Expertise in ICT and security is expensive, as is the cost of purchasing and maintaining ICT equipment.

With expensive specialist resources and equipment, the cost of a dedicated secure ICT environment for a small number of users can be costly to build (and even more expensive when considering larger organizations with more complex needs), plus the ongoing costs of sustainment and support.

SECURITY MEASURES

To address technical information protection requirements for ITAR sharing and collaboration requirements and controls you need to employ these security measures:

Encryption

Data needs to have protections in place wherever it is, including where it is located (storage, at rest) whether on-premises or in the cloud, and while being transferred or moved across networks or boundaries (in-transit).

Encryption provides a means to ensure only authorized users can see the content, through locking up information in a provable and enforced (encryption algorithms) manner that is readable only when the right keys to the lock are provided.

It is important to have data encrypted at every stage from storage, transit, until it gets to the recipient, such that intermediaries do not decrypt the information.

Granular Access Control

In order to meet ITAR considerations for protecting information, you have to be able to control who has access to the information, and under what conditions. The granularity required may mean different rules for different files, with only specific people or those of a given nationality being able to access the information. Enforcing access based on these criteria or rules means being able to define and act based on a user's attributes such as their nationality, clearance, or organization.

This ability to assess, decide, and enforce security based on a set of rules is referred to as Attribute-based Access Control (ABAC), which is described by NIST in their Special Publication SP 800-162, as well as being identified as a key building block of security (https://www.nccoe.nist.gov/projects/building-blocks/attribute-based-access-control).

Persistent Access Control

Strongly enforced access control needs to consider the context in which the information is stored, accessed, transferred, or shared. Limitations of some systems means that once the information leaves the "walled garden", these controls can become unenforceable. This is critical when dealing with information that has to have protections in place across different security boundaries, through multiple systems, and across multiple environments.

In scenarios requiring higher assurance, such as the handling of classified information, as well as other considerations such as jurisdiction and location of storage - persistent access control within each context is important.

You need to ensure that classified/controlled information has those controls applied and enforced, as the data is moved or accessed by email, chat, or by another form.

Detection and Prevention

The saying "an ounce of prevention is worth a pound of cure" definitely applies to security of ITAR information, as once information is exposed or compromised, it is very difficult to control or recover.

An in-depth security approach should be applied, ensuring that logical control points are configured to detect and enforce rules, as well as providing means to define, describe, detect, and inform controls.

This can include scanning for relevant information at relevant points, and automatically enforcing the relevant access controls and encryption to prevent the information controls being accidentally missed by users, whether stored on a file system, within an email, in an online repository, or sent by chat.

Comprehensive Audit Capabilities

In any security context, the ability to identify who has done what, when, and where becomes critical in ensuring that both information security is being upheld, as well as whether compliance obligations are being met.

Systems that store, process, or handle information that is sensitive in nature should detect and log activities and attempts related to the information. This helps both in maintaining context, as well as enabling and enforcing control throughout collaboration and sharing in a complex supply chain.

ITAR and EAR compliance is one of the most complex access management issues to solve.

archTIS helps tackle compliance and control information access and sharing in compliance with requirements across Microsoft Content Management and Collaboration tools.

ITAR AND EAR COMPLIANCE MADE EASY

ITAR and EAR compliance is one of the most complex access management issues to solve.

Trying to define access applications that utilize item or role-based permissions generally requires the creation of thousands of security groups, and if using inheritance thousands of sites or libraries and folders. You also run the risk of exceeding the limit of allowed security scopes on a list. The complexity and ongoing management of these security schemes greatly expand the likelihood of multiple single point defects in individual user or document permissions – any of which constitute an export breach.

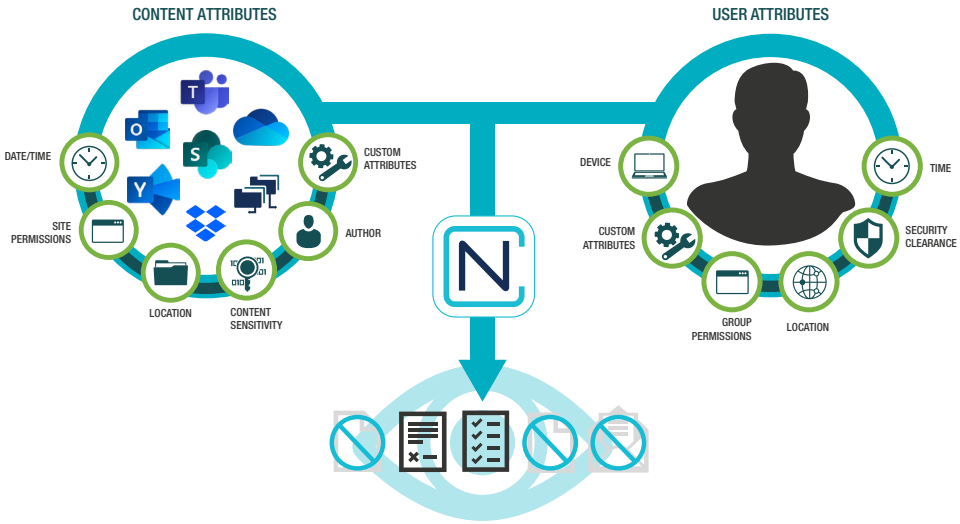
Fortunately, archTIS provides organizations with multiple solutions to help tackle ITAR and EAR compliance and controlled information sharing needs. archTIS solutions are built on a zero trust methodology that use fine-grain attribute-based access control (ABAC) to determine access, usage and sharing permissions at the item level.

Advanced Information Protection and Compliance for Microsoft 365, Teams & SharePoint On-premises

If you currently use Microsoft content management and collaboration tools, or have sensitive data stored within file shares, NC Protect provides advanced information protection capabilities, leveraging existing Microsoft technology investments (MPIP, RMS, E3 and E5) to provide a simpler, faster and dynamic solution to automatically identify and secure business-critical information against insider threats.

NC Protect product enhances information protection using granular ABAC-based policies to control file access and sharing, messaging, and emailing of sensitive and classified content across Microsoft 365 apps (SharePoint Online, Teams, and Exchange), SharePoint on-premises, Nutanix Files and Windows file shares to meet ITAR and EAR compliance.

NC PROTECT PROVIDES REAL TIME, ATTRIBUTE-BASED ACCESS, USAGE AND SHARING CONTROL



GET UNIQUE CAPABILITIES FOR DYNAMIC, FINE-GRAIN ACCESS CONTROL AND DATA PROTECTION IN MICROSOFT APPLICATIONS

NC Protect secures your data at rest or in motion to protect it as users and partners collaborate and share it across different communication channels (file sharing tools, chat and email) to:

Discover & Classify

- Locate and classify all sensitive and confidential data (ITAR, CUI, FCI, CMMC, PII, IP, etc.).
- Single rule set for one or multiple on-premises, cloud or hybrid environments.
- Automatically encrypt or quarantine files when required.

Prevent Data Loss, Misuse & Human Error

- Control what users can see, how they can use and share information and with whom at the file, message and chat level.
- Uses fine-grain attribute-based access, usage and sharing (ABAC) policies.
- Dynamically adjusts in-transit file access, security and encryption.
- Real-time comparison of user and file attributes to approve or restrict access.
- Enforce access and security policies across all devices and locations to ensure secure information access for BYOD and work from home.
- Restrict what users can do with files: download, copy/paste, email, etc.
- Remove/redact sensitive or confidential information, such as keywords or phrases.
- Hide sensitive files from unauthorized users.
- Add dynamic security watermarks.

Enforce Regulatory Compliance

- Restrict access to and flow of information between individual or groups of individuals for SEC, GDPR, ITAR, CMMC, etc.
- Embeds CUI Designation Indicator markings (Owner Name, Controlled By, Category, Distribution/Limited Dissemination Control, POC) into documents as a persistent watermark for CMMC 2.0 compliance.
- Flexible Information Barriers allow users to chat and collaborate on permitted projects/topics, but block restricted ones.
- Enforce global data privacy and handling regulations.

Control Guest / Third Party Access

- Control what content guests can see based on their user profile.
- Automatically restrict guest data access and limit file usage / actions.
- Limit guests to read-only access via a secure viewer.

Audit Activity & Permissions

- Logs file access and user actions, and changes to NC Protect policies.
- Find and fix incorrect app level at-rest permissions.
- Identity and associated permissions are no longer a single point of failure.
- Integrate user activity and protection logs with Microsoft Sentinel and Splunk for further analysis and downstream actions.

Need fine grain access and security to meet ITAR, EAR or other Export Control compliance requirements?

CONTACT US

www.archtis.com/contact

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, Dropbox, 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