FORTRA

WHITE PAPER (Titus)

ITAR Compliance

Strategies to Identify and Protect Technical Data

Introduction

The aerospace and defense industry continues to increase its global reach at a rapid rate. Aerospace agencies handle data that needs to be protected from competitors and foreign military and government organizations. Competitive sensitivities, disparate customer requirements and government regulations concerning the sharing of sensitive information are critical considerations in the aerospace and defense marketplace.

In an effort to protect national security and trade secrets, the U.S. government created the International Traffic in Arms Regulations (ITAR), governing the export and import of defense related material and technologies. U.S. companies can face multi-million dollar fines if they provide non-U.S. people with access to ITAR-protected products or information.

Managing and controlling ITAR-protected information is a critical step for organizations wishing to address ITAR compliance requirements. Titus has created a family of solutions that facilitates secure information sharing in today's global aerospace environment while helping organizations meet their compliance obligations.

Titus ITAR solutions enable organizations to manage and control sensitive information by labeling information and restricting access as part of an ITAR compliance program. Titus solutions are used worldwide in aerospace and defense organizations, including UTC, Pratt and Whitney, Xilinx, Dow Corning, DRS, BAE Systems, Lockheed Martin, and Northrop Grumman.

This whitepaper focuses on strategies to meet ITAR requirements and best practices surrounding implementation of an ITAR compliance program. Information about Titus' portfolio of solutions and how they can be deployed as part of an ITAR compliance program is also provided.

Building an Itar Compliance Program with Information Classification

ITAR legislation is a set of regulations that authorizes the government to control the export and import of defense-related articles and services. ITAR affects those involved in the manufacturing, distribution and regulation of aircraft, amphibious vehicles, cartridge and shell casings, chemical agents, firearms, naval equipment, missile control, and other military related equipment.

The U.S. Directorate of Defense Trade Controls (DDTC) strongly encourages organizations to create ITAR compliance programs for record keeping, including the identification, receipt and tracking of ITAR controlled items and technical data. Organizations that fail to control ITAR-related information are subject to fines and imprisonment. Titus ITAR solutions are built on the Microsoft Office and Microsoft SharePoint platforms. Because end-users are already generally familiar with the Microsoft environments, the ITAR solutions are easy to deploy and have a high level of acceptance among users.

For companies using SharePoint as a document management platform, Titus offers a metadata-based security solution to protect ITAR information. Information labeled in SharePoint as ITAR restricted will be secured for specific ITAR-cleared audiences.

Titus also offers desktop-based classification solutions for ITAR that allow organizations to identify, label and mark email and documents as part of an ITAR compliance program. ITAR-related information such as product plans, product specifications, financial information, manufacturing plans, instructions and product documentation can be protected with email and document classification labels.

ITAR Compliance in Microsoft SharePoint

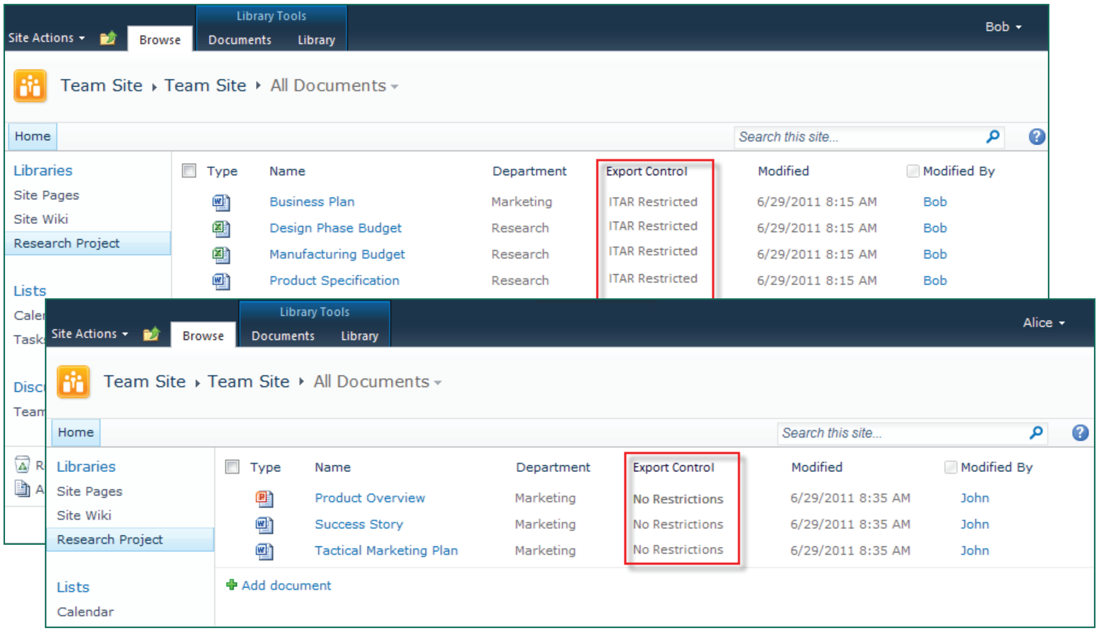
Many organizations working on sensitive ITAR projects want to promote collaboration and information sharing among the project staff, but also need to ensure that other employees who are not working on the project, or who hold citizenship in certain proscribed countries, do not gain access to the ITAR information.

Microsoft SharePoint is a popular platform for collaboration and document management. It can be used to share project related documents and information. Because of SharePoint's history of being used in decentralized environments, SharePoint's native security is generally not regarded as robust enough to handle ITAR-restricted information.

Titus Metadata Security for SharePoint solution adds an additional layer of security to the SharePoint platform which allows organizations to easily protect sensitive ITAR information. The administrator can easily create ITAR based security policy that will result in strong security for all project-related information.

For example, an organization may have a document library that contains a mix of documents, some of which are ITAR Restricted. The Titus administrator can define a security rule that will restrict access to all information labeled in SharePoint as "ITAR RESTRICTED" to a specific group of cleared employees working on that project. A user with ITAR clearance would see all documents in the folder, while a user without ITAR clearance would see only a sub-set of documents, as shown below.

In this way organizations can be confident that they are meeting the ITAR compliance requirements for export-controlled information.



□ Type	Name	Department	Export Control	Modified	□ Modified By
W	Business Plan	Marketing	ITAR Restricted	6/29/2011 8:15 AM	Bob
X	Design Phase Budget	Research	ITAR Restricted	6/29/2011 8:15 AM	Bob
X	Manufacturing Budget	Research	ITAR Restricted	6/29/2011 8:15 AM	Bob
W	Product Specification	Research	ITAR Restricted	6/29/2011 8:15 AM	Bob

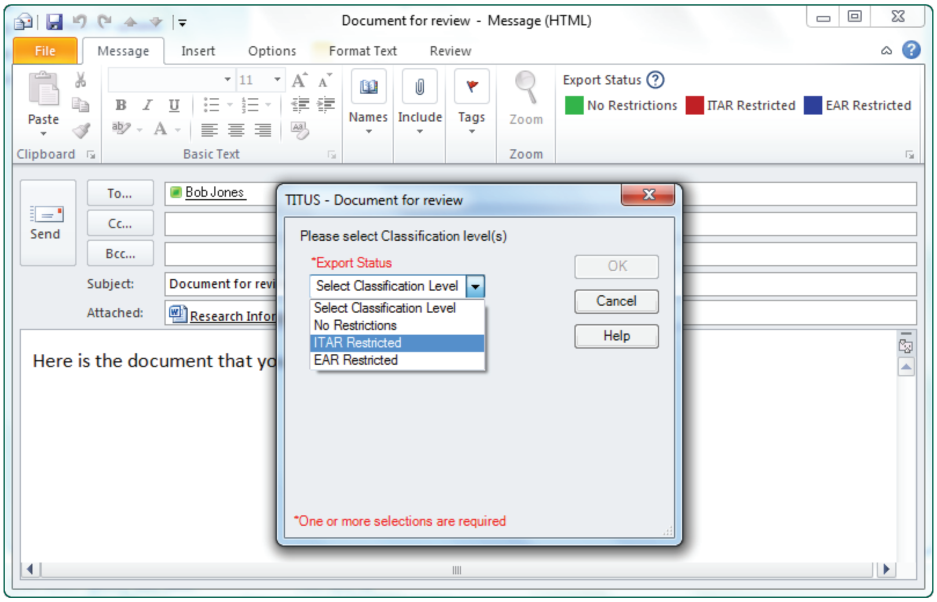
□ Type	Name	Department	Export Control	Modified	□ Modified By
P	Product Overview	Marketing	No Restrictions	6/29/2011 8:35 AM	John
W	Success Story	Marketing	No Restrictions	6/29/2011 8:35 AM	John
W	Tactical Marketing Plan	Marketing	No Restrictions	6/29/2011 8:35 AM	John

Figure 1 Using metadata to ensure the right people access the right information in SharePoint

ITAR Compliance Solutions for the Desktop

Organizations can also protect sensitive ITAR information by using Titus desktop solutions for ITAR. These solutions allow organizations to:

1. Prompt users to select pre-defined ITAR markings from a dropdown list in Microsoft Office and Outlook before they can send, save or print information.



To... Bob Jones

Subject: Document for revi

Attached: Research Infor

Here is the document that yo

TITUS - Document for review

Please select Classification level(s)

*Export Status

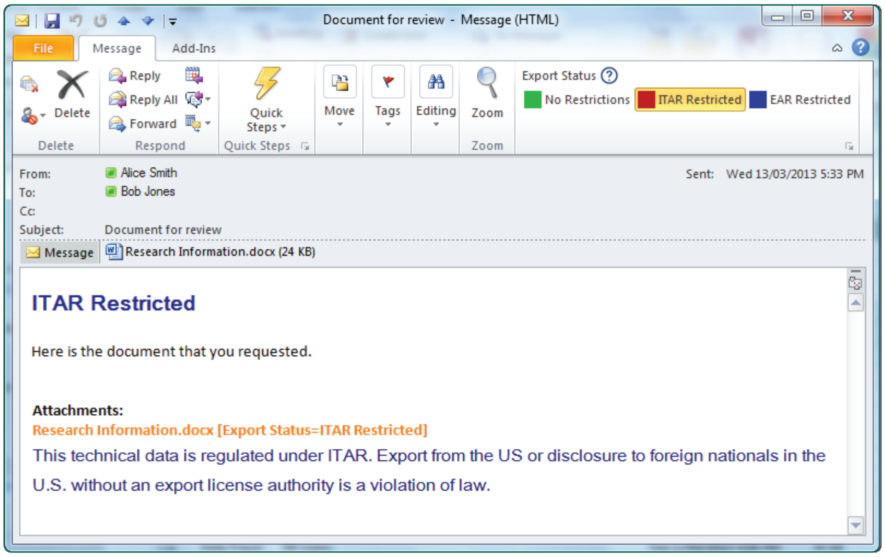
Select Classification Level

- Select Classification Level
- No Restrictions
- ITAR Restricted
- EAR Restricted

*One or more selections are required

Figure 2 Prompting user to select ITAR labels on send in Microsoft Outlook

2. Apply visual markings (headers, footers, watermarks) to increase awareness of sensitive information and encourage proper handling.



From: Alice Smith

To: Bob Jones

Cc:

Subject: Document for review

Sent: Wed 13/03/2013 5:33 PM

Message Research Information.docx (24 KB)

ITAR Restricted

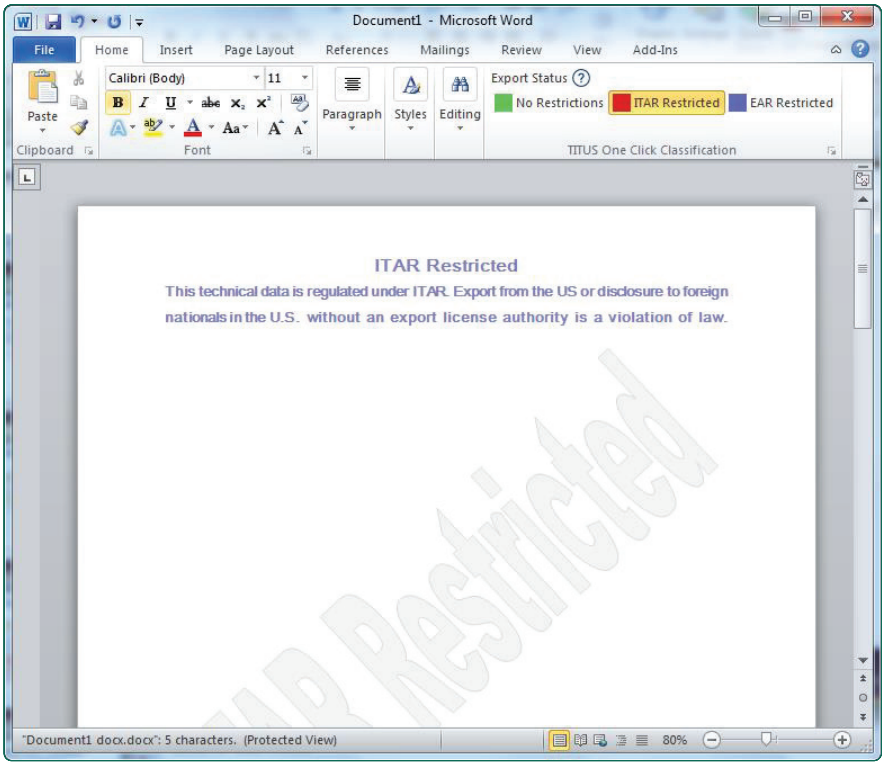
Here is the document that you requested.

Attachments:

Research Information.docx [Export Status=ITAR Restricted]

This technical data is regulated under ITAR. Export from the US or disclosure to foreign nationals in the U.S. without an export license authority is a violation of law.

Figure 3 Visual markings in email, including ITAR disclaimer



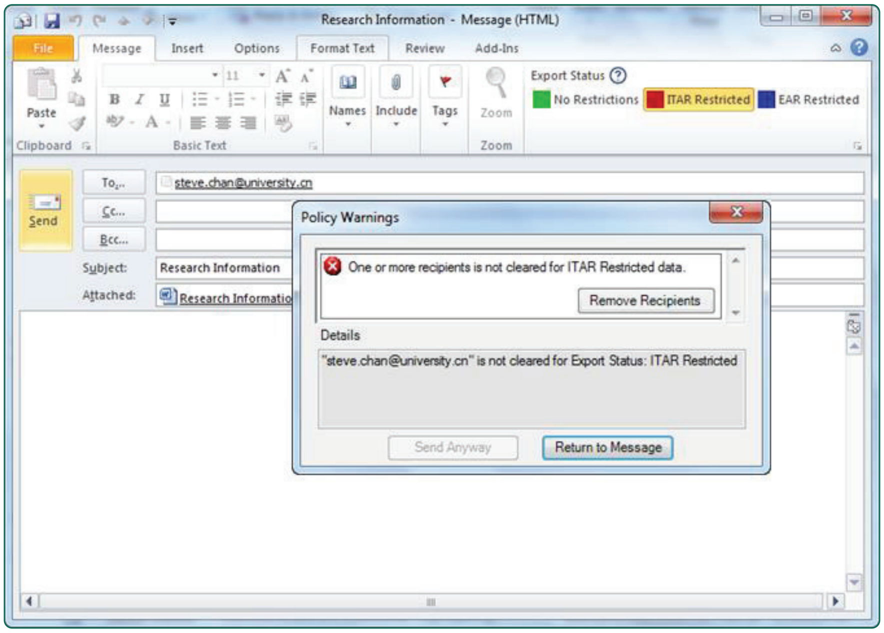
ITAR Restricted

This technical data is regulated under ITAR. Export from the US or disclosure to foreign nationals in the U.S. without an export license authority is a violation of law.

"Document1 docx.docx": 5 characters. (Protected View)

Figure 4 Visual markings in Microsoft Office (header/footer, disclaimer, watermark)

3. Ensure ITAR emails and documents are only sent to ITAR-approved individuals.



To... steve.chan@university.cn

Cc...

Bcc...

Subject: Research Information

Attached: Research Informatio

Policy Warnings

One or more recipients is not cleared for ITAR Restricted data.

Details

"steve.chan@university.cn" is not cleared for Export Status: ITAR Restricted

Figure 5 Sender is prevented from sending ITAR information to unauthorized recipients

Titus desktop solutions have several security features that can help organizations to apply and enforce security policy in an ITAR-controlled environment. Key features include:

- **Safe Recipient Lists** — Safe recipient checking ensures that only authorized or intended recipients receive ITAR related email, even in cases where different people with different privileges have the same name. Titus checks both internal and external recipients, and can prevent common export violations such as inadvertently sending ITAR information to an unauthorized user hidden in a distribution list.
- **Automatic Content Scanning** – Titus solutions can scan content and warn users if an email or document appear to contain ITAR-restricted information. Titus can also prevent users from discussing potential ITAR violations through email, and instead, direct them to report the potential violation through proper channels.
- **Automatic Email and Document Protection** — Titus solutions can automatically apply encryption or Microsoft AD Rights Management Services (RMS) based on the email or document label. This feature is transparent to the user; they simply select a label from the dropdown list, and the protection is applied automatically, with no encryption or RMS training required.
- **Customized Email and Document Disclaimers** — Titus solutions can automatically insert a customized disclaimer based on a selected export control label. For example, if a user selects an ITAR Restricted label, Titus can automatically add a disclaimer such as: "This technical data is regulated under ITAR. Export from the US or disclosure to foreign nationals in the U.S. without an export license authority is a violation of law." By clearly identifying that the information is export controlled, the organization puts accountability and responsibility on the recipient.
- **Auditing and Retention** – Through the use of audit files, Titus solutions can help to identify users who are willfully breaking ITAR rules for email and documents, and prove that the organization took steps to prevent it. Titus can also help with archiving and e-Discovery by automatically sending a copy of all ITAR-related email to an ITAR retention mailbox.

Titus Solutions for ITAR Compliance

Titus ITAR solutions provide many key features and capabilities that an organization needs for a successful ITAR compliance program. Titus products can be used as stand-alone solutions or together as a powerful integrated solution. This section highlights just some of the features included in the Titus family of ITAR solutions.

Titus Security Suite for SharePoint

The Titus Security Suite for SharePoint enhances SharePoint security and ensures that security policies are applied consistently and automatically across all your sensitive content in SharePoint. These solutions ensure the right people access the right information, and promote end user awareness and accountability for sensitive information.

With the Titus Security Suite for SharePoint, organizations can:

- Implement consistent and strong Data Governance
- Enforce dynamic, fine-grained security
- Automate security using identity and metadata
- Comply with regulations such as ITAR

The suite is made up two products: Titus Metadata Security automatically applies permissions and access control for sensitive content in SharePoint based on metadata properties combined with trusted user claims. Titus Document Policy Manager automatically converts documents to PDF and applies visual labels to raise awareness of sensitive content, providing users with education on how to handle sensitive data.

Titus Information Classification Solutions

Titus offers a complete family of information classification and marking solutions for email and documents. With a wide range of customizable functionality, the Titus Classification solutions enable your organization to:

- Empower users to identify and protect export-controlled information
- Reduce risk and raise user awareness by applying consistent ITAR markings (including disclaimers) to documents and email

- Enforce export control policies to ensure the right people access the right information
- Prevent common export control violations such as accidentally sending email to unauthorized recipients in a distribution list

Titus Classification solutions include:

- Message Classification™ for the classification, marking and protection of email in Microsoft Outlook®, Outlook Web App®, Lotus Notes®, and mobile devices
- Classification™ for Microsoft Office™ for the classification, marking and protection of Microsoft Office Word®, PowerPoint®, and Excel® documents
- Classification for Desktop™ for the classification and protection of any file type in a Windows® environment, including PDF, CAD, and multimedia files

Ease of Use

Titus ITAR solutions integrate seamlessly into current Microsoft Office and Microsoft SharePoint environments and are very easy to use. There are no new applications for users to learn.

Users familiar with SharePoint will interact in the same way as they interact with other SharePoint applications. The additional ITAR security is transparent to users.

Titus ITAR solutions are also integrated into Microsoft Office, Outlook and Windows Explorer. The user simply selects the appropriate ITAR label for the document or email from the list of available labels.

As a result of their design, training requirements for Titus ITAR solutions are minimal, and can be deployed within organizations very quickly.

Conclusion

ITAR regulations have introduced considerable challenges to the aerospace and defense industry. Titus offers cost-effective interoperable solutions that ensure the security of sensitive ITAR information. By providing a wide selection of ITAR solutions, Titus enables organizations to deploy the solution that most closely fits their requirements and their current infrastructure.

Titus solutions are applicable for all aerospace, defense agencies, contractors and suppliers dealing with ITAR protected information. The solutions are low cost, easy to deploy, and enable efficient sharing of sensitive information.

To find out how Titus can help your organization comply with ITAR and other export control regulations, please visit www.titus.com.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.