LEADING AEROSPACE COMPANY MEETS ITAR and EAR Compliance Requirements

Aerospace and Defense, high tech and industrial manufacturing companies face information sharing and security challenges in order to ensure compliance with International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). These regulations impose severe fines and penalties for inappropriate data loss. Demonstrating proper controls to support ITAR and EAR regulations is a major challenge, especially when it comes to competitive sensitivities, disparate customer requirements and government-enforced mandates regulating the sharing of intellectual property.

Company Profile

This leading International Aerospace Company has thousands of employees in multiple locations worldwide who are contractors for the government and on military projects. The company transfers sensitive technical data to and from outside countries, which may be subject to ITAR and EAR.

Business Situation

Like many aerospace and defense agencies, the company was handling highly sensitive technical data including competitive information, intellectual property and government data that needed to be protected from competitors, foreign military and government organizations. One of the company's biggest clients is the US government, and they are required under ITAR and EAR to ensure that information and material pertaining to defense and military-related technologies is shared only with US persons. US companies can face multi-million dollar fines if they provide non-US persons with access to ITAR and EAR-protected products or information, which makes managing and controlling ITAR and EAR-protected information critical for organizations dealing with this type of information.

Challenge

The IT team, in conjunction with the CIO, had identified the management of valuable corporate technical data as a top priority to ensure ITAR and EAR compliance. They needed to identify and protect technical data to prevent the transfer to a foreign person and ensure publicly available data was easily accessible. A major area of concern for ensuring compliance was email and related documents as it can be a challenge for users to clearly understand how to handle the flow of information. To support this strategy, the organization's IT team started to look for a solution that would enable them to not only address ITAR and EAR, but to deliver ease of use, raise awareness to the sensitivity of data and integrate within the existing Microsoft infrastructure.

Solution

To ensure that both email and documents were carefully controlled to prevent accidental data leakage and enforce ITAR and EAR compliance on all technical data, the company started out by defining their specific requirements, one of which was ease of deployment and management on an ongoing basis. With a large IT infrastructure to support, an information management solution needed to be both quick to deploy and require very little end user training. After examining different approaches and a number of solutions, the company selected TITUS Message Classification™ and TITUS Classification for Microsoft Office™ to label emails and documents.

By utilizing TITUS solutions, users are prompted to select pre-programmed ITAR and EAR markings from a drop down list in Microsoft Office® and Outlook® before they can send, save or print information. The TITUS solutions then automatically apply visual markings such as headers, footers and watermarks to increase awareness of sensitive information and ensure ITAR and EAR emails and documents are only sent to approved individuals. In addition, TITUS Message Classification can scan the content of emails for ITAR and EAR related information and warn the user of any ITAR and EAR content before the email can be released. For example, the solution can search for Export Control Classification Numbers (ECCN) and notify the user that

the content is present and should be marked accordingly. TITUS Message Classification and TITUS Classification for Microsoft Outlook have several security features that can help organizations apply and enforce security policy in an ITAR and EAR-controlled environment. A simple pop-up box can force users to select an appropriate ITAR or EAR label. The software can also ensure that only authorized or intended recipients receive ITAR or EAR related information, even in cases where different people with different privileges share the same name.

The labels automatically attach metadata to the email or document which can be read by existing security technologies to control and restrict access to the data as part of an ITAR or EAR compliance program. The organization was able to quickly deploy the solution enterprise-wide and have users trained and ready to go with email and document labeling, with no impact on their existing IT infrastructure.

Taking a user-driven approach to data identification was appealing to the company as they were able to have the originators of an email or document – who were most knowledgeable about the content – make the decision on what type of content was in the email and how that data should be handled. The added benefit is that this project helps to educate users and create an environment where everyone understands the importance of the data and can easily understand how to handle data with ITAR, EAR, and other concerns in mind.

Benefits

Helps automate ITAR and EAR compliance

The ability to automatically scan message content for sensitive ITAR and EAR content, along with the ability to immediately warn users ensures that technical data is protected. In addition, the software can automatically apply headers, footers and watermarks to emails and documents that are ITAR or EAR restricted to help automate email and document management, and ensure that sensitive ITAR and EAR information is only sent to the right people. TITUS Message Classification also includes attachment checking to ensure attached documents labeled with TITUS Classification for Microsoft Office are also ITAR and EAR-protected and can only be sent to those users who are eligible to receive ITAR and EAR information. This ultimately controls access to technical data and enforces export control polices with labels.

Prevents leakage of technical data

Since deploying TITUS Message Classification and TITUS Classification for Microsoft Office, the company has been able to prevent the leakage of technical data while supporting ITAR and EAR requirements. TITUS Message Classification checks recipient names in an email and ensures an ITAR or EAR-restricted email is never sent to an unauthorized recipient. As an aerospace company, this is a key benefit from both a competitive and contracting perspective. To maintain a competitive edge and continue to secure contracts, it is critical that all technical data is handled correctly.

Ease of use and management

For IT, the tight integration of TITUS Message Classification and TITUS Classification for Microsoft Office with the existing Microsoft infrastructure has driven ease of use and management as they were able to fit data labeling into the existing workflows with minimal impact to users. Now sensitive technical email and documents are quickly and easily identified and labeled.

Low total cost of ownership

From the CIO's perspective, the TITUS Message Classification and TITUS Classification for Microsoft Office solutions enabled them to address an immediate problem with minimal effort, and the solution delivers a low total cost of ownership compared with other approaches and offerings. ITAR and EAR regulations have introduced considerable challenges to the Aerospace industry. TITUS offers cost-effective interoperable solutions that label email and documents to meet these regulations. TITUS labels add structure to unstructured data and help manage access to sensitive technical data across boundaries, and according to corporate policy. TITUS solutions are applicable for all aerospace, defense agencies, contractors and suppliers dealing with ITAR and EAR protected information. The solutions are low cost, easy to deploy, and enable efficient sharing of sensitive information.

About TITUS

TITUS is the leading provider of security and compliance software that helps organizations share information securely while meeting policy and compliance requirements. Our solutions enable military, government, and large enterprises to raise awareness and meet regulatory compliance by visually alerting end users to the sensitivity of information. Products include TITUS Classification, the leading message, document and file classification and labeling solutions; TITUS Aware, products that enhance Data Loss Prevention by detecting sensitive information at the desktop; and the TITUS family of classification and security solutions for Microsoft SharePoint. TITUS solutions are deployed to over 1.5 million users within our over 300 military, government and enterprise customers worldwide, including Dow Corning, United States Air Force, NATO, G4S, Paternoster, Pratt and Whitney, Australian Department of Defense, and the U.S. Department of Veterans Affairs. For more information, visit www.titus.com.

TITUS

Security & Compliance Solutions | titus.com

HEADQUARTERS: 343 Preston Street, Suite 800 | Ottawa, Canada K1S 1N4 | Tel: +1 613.820.5111 | info@titus.com

USA: usa@titus.com | EMEA: emea@titus.com | Asia-Pacific: apac@titus.com