NEXTLABS®

White Paper

Electronic Export Compliance

Control and Audit the Use of Technical Data and Information Flow to Comply with ITAR and Export Regulations

Solution Highlights

Control access to and protect information subject to export regulations

Comply with ITAR and EAR regulations by implementing:

- Information access and handling controls including enforcement
- Export License Management
- Automated assistance to satisfy export control regulations

INAPPROPRIATE DISCLOSURE OF TECHNICAL DATA

The Aerospace and Defense (A&D) industry faces a set of unique information security challenges in order to comply with ITAR and EAR export regulations. ITAR and EAR regulations impose fines and penalties for inappropriate disclosure of controlled information, e.g. data of importance to national defense.

Satisfying ITAR and EAR regulations is a major challenge for A&D firms, especially those with global presence, mobile workers, offshore operations, joint ventures, and extensive collaboration or supply chains. Guidelines or standards around key concepts like deemed exports are loosely defined.

NextLabs® and SAP® have teamed to provide a solution that helps A&D firms comply with ITAR and EAR export regulations.

The solution protects information within the enterprise, ensures compliance with export regulations when dealing with global suppliers, and restricts access to controlled information to authorized users, and provides detailed reports to demonstrate compliance and support audits.

THE SOLUTION

The NextLabs and SAP Electronic Export Compliance solution is designed to address export control requirements dealing with the handling and protection of defense or other technical data. The solution consists of three major components: identity management, information access control and enforcement, and export license (e.g. TAA's) management.

The solution addresses technical data export requirements by enabling project teams to:

- Define authorized users
- Identify controlled
- technical data
- Control technical data access and use according to defined business policies
- Control export of technical data corresponding with approved licenses and defined business policies, and Provide a full audit trail detailing technical data flow history to satisfy regulatory compliance requirements.

The solution actively enforces export controls by understanding the complex, business context variables for appropriate technical data handling and disclosure. Collaboration inside and outside the extended enterprise, including supply chain partners and a mobile workforce, can safely take place.

LEVERAGING SAP FOR GTS ITAR TECHNICAL DATA EXPORTS

SAP GRC Global Trade Services (GTS) provides enterprises with the ability to manage the physical export of goods against agreements/licenses which are necessary to comply with government regulations, such as ITAR and EAR. Comprised of 3 modules (Compliance, Customs and Risk), GTS manages the export process from receiving the license through operational management and documentation.

The Compliance Management module manages international trade in three main areas: sanctioned party screening, export license management and import license management. The Customs Management module facilitates communications between the company's enterprise and customs agencies, the creation of documentation and production classification. The Risk management module deals with trade preference agreements and financial integration for letter of credit.

In an integrated environment, GTS is linked with the ERP, sales and/or shipping systems to provide seamless export compliance. Sales order and shipment data is sent to GTS, processed within the Compliance management module and evaluated for compliance with export licenses. Then documentation needed to facilitate the export (i.e., US CBP forms) is delivered via the Customs management module. Reporting and audit capabilities are then made available against each license at the transaction level.

However, as mentioned earlier, when the export is a transmittal of technical data to a supplier or customer, there is not necessarily a transaction in the ERP or shipping system that captures the export. Without a transaction, GTS does not have visibility to the export or a means to associate it with the applicable export agreement/license. If there was a way to have the technical data transfer represented as a physical shipment, then the GTS provided functionality could be used as designed and compliance improved.

With the addition of NextLabs' suite of Information Risk Management software, transfers of data can be tracked and monitored discretely. Each of these movements can be transferred to GTS as if they were a physical shipment using the standard API. GTS will then process the shipment through license determination, license association and track the transfer against the license for audit purposes. This provides a permanent record of each instance and when technical data was transferred against a license. Additional information about the transfer, such as file name, can then be retrieved, if necessary.

SCENARIOS TO PROTECT ITAR TECHNICAL DATA

The Electronic Export Compliance solution is centered on a best-practice ITAR Policy Library that addresses the greatest areas of technical data control risk. Additional libraries to address EAR, or custom libraries for export controls based on client needs, can be easily included or designed. Recognizing that the determination of ITAR jurisdiction can be a subjective process, policies are managed through collaboration between Export Officers at the corporate level and Project Managers in each of the business units. Policy is deployed across enforcement points of relevant applications and systems to control data access and use. Controls are measurable and demonstrable via a set of audit dashboards, reports, and integration with export trade management systems. Existing infrastructure, such as Identity Management, Access Management, HR, and corporate directories are directly leveraged to minimize manual maintenance and allow policies to easily adapt to changes when underlying infrastructure is updated.

Technical Controls for Electronic Export Compliance

To prevent inappropriate disclosure, and ensure data use and export complies with regulatory policies, the Electronic Export Compliance solution provides the following controls:

Limiting Access to ITAR Technologies

ITAR policies require that access to technical data is restricted to US persons. Typically, technical data is managed in document management systems or on file servers, and while in a repository, local controls may prevent ITAR access violations. However, these controls are insufficient to meet ITAR requirements once data is removed from the repository where no usage controls exist, allowing data to be misused.

As an example, an authorized user may need to copy a design file to an engineering workstation to complete the design. Once copied to the workstation, no further controls exist for where the file may be saved or sent. A violation, even unintentional, now has the opportunity to occur. With the Electronic Export Compliance solution, access controls are maintained when technical data flows between systems. Furthermore, files may only be saved within or distributed to approved locations as the data flows across the business environment.

Mixed-Use Environments

In many Aerospace and Defense, High Tech, and Industrial firms, engineering design, development, and manufacturing resources are used for both ITAR projects and commercial projects. Such multi-use environments create potential for accidental disclosure of technical data and contamination of commercial projects. In these environments, users, systems, and applications are a potential breach and leakage point.

For example, an engineer copies design files to a workstation that is accessible to foreign persons. Similarly, a server application with ITAR-controlled designs may be administered by a foreign person, potentially exposing the files. While utilizing shared resources across ITAR controlled and commercial environments allows companies to economize by reducing infrastructure costs, it also increases potential for inappropriate exposure. The Electronic Export Compliance solution protects the integrity of mixed-use environments by enforcing appropriate access and use for technical data that allows businesses to realize the economies of managing information across shared resources.

Technical Data Export With Trade Management

Export of technical data occurs any time that information is sent outside of the US or provided to foreign persons within the US. Many of these types of exchanges are, however, allowed under license. Transfers of technical data under licenses must be accounted for and reported, similar to the export of physical goods. Accounting and tracking data movement can be difficult since transfer of electronic technical data can occur over multiple channels, including email, instant messenger, FTP, or Web upload. Because the transfer of electronic data is so frictionless, it is difficult to accurately account for exported information as required by regulations.

The Electronic Export Compliance solution ensures that technical data export is tracked and in alignment with export licenses by enforcing controls over ITAR technical data access, movement, and use across systems and applications. SAP GTS can process the technical data export as a shipment and apply the GTS service checks, such as license determination, to the transaction. Auditing and reporting, integrated with the trade management system, verifies and proves compliance is being met.

SUPPLY CHAIN COLLABORATION ON ITAR PROJECTS

In the design and manufacture of defense articles, companies often collaborate across a complex supply chain. A single product may include parts from suppliers, and each part may have several companies involved in design and manufacture. In these cases, technical data is shared between organizations. The transfer of data requires approved distribution methods to prevent exposure during transmission.

For example, if data travels through systems or networks that are administered by foreign persons, there is opportunity for inappropriate disclosure. The receiving organization must also handle technical data appropriately; for example they are required to ensure it is not exposed, return the information after it has been used, and destroy copies once a project is complete.

The Electronic Export Compliance solution enforces policy-based controls within the enterprise and across the extended enterprise to include partners, outsourcers, and contractors for compliance throughout the supply chain. Controls can require that collaboration make use of specific communication channels with additional protection technologies enforced, such as encryption, to maintain information integrity while in transit. With the Electronic Export Compliance solution, data that is physically maintained on partner, outsourcer, and contractor systems can also be controlled with the same degree of integrity as if the system was managed directly within the enterprise.

CONTAMINATION VIA SEE-THROUGH

ITAR will control a commercial item if a product or component that is subject to ITAR control is incorporated into it.

For example, if a part originally designed for a military aircraft is used in a commercial airliner, the airliner is subject to ITAR while that ITAR controlled part remains integrated into the airliner. This situation presents unique risks when applied to ITAR technical data, such as specifications and software, where documents and code are easily reused between products. To prevent the contamination described above, it is important that data pertaining to defense articles be kept separate from commercial data, with any mixing of technical data prevented.

The Electronic Export Compliance solution can identify data based on locations, such as applications, repositories and devices, as well as data attributes, such as document tags, to actively control exposure. Classes of information or specific documents can be restricted from use in projects that would present conflicts by using a solution that is scalable across the entire environment.

MOBILE DATA AND REMOTE ACCESS USE

Access to ITAR technical data from locations outside the US, even by approved or authorized persons, is considered an export of technical data. Similarly, the transport of technical data on a mobile device such as a laptop computer, outside the US, is considered an export of technical data. These export activities are either prohibited or allowed under an existing export license. Furthermore, data access requires that controls are applied based on the current location of the end user and endpoint system, along with a means to identify ITAR data that is stored on a mobile device, to ensure that the device is free of technical data before it is brought outside the country.

The Electronic Export Compliance solution enforces controls by integrating with identity management systems that track users and devices for applying policies. When users and devices are mobile, they are evaluated against policies to apply enforcement accurately, even when off the network or disconnected. When conditions indicate that users are in locations subject to ITAR restrictions or they are accessing the network remotely, policies can restrict data access, movement and use to ensure ITAR compliance is maintained. The solution can also require dependencies for increased protection to ensure additional safeguards are enforced, such as encrypted storage or communications.

SOLUTION BENEFITS FOR ELECTRONIC EXPORT COMPLIANCE

With active controls applied to the access, movement and use of export controlled technical data, companies can now avoid costly fines resulting from inappropriate disclosure, as well as audit the export of technical data, to align the movement of technical documents with valid export licenses. Moreover, The solution provides auditing and reporting to provide much needed visibility to ensure export control regulatory compliance meets business goals.

Minimize The Risk Of Inappropriate Disclosure

The Electronic Export Compliance solution enforces export control policies in real time at each point of information use to ensure that technical data is accessed, handled, distributed, communicated, and exported appropriately. By applying information controls, Aerospace and Defense, High Tech, and Industrial firms can reduce fines and penalties, and legal and remediation costs, as well as protect customer and stockholder trust, by actively preventing violations, while maintaining national security integrity as a responsible organization.

Quickly Demonstrate Compliance

The Electronic Export Compliance solution allows organizations to monitor, log and report all information use activities, regardless of policies put in place, to ensure technical data access, movement and use is aligned with compliance goals. By demonstrating policies are enforced appropriately, along with clear visibility into all information use activities, companies can assist investigations by proving that information disclosure occurs appropriately and policies actively protect sensitive information.

Economize Multi-Use Environments

Large, global companies with significant investments in infrastructure need the ability to use all available resources productively, given the alternative of maintaining dual infrastructures for export-controlled data and other programs. However, the lack of adequate solutions for protecting technical data as it flows within the enterprise and across the extended enterprise has required businesses to create physically isolated environments. By applying the Electronic Export Compliance solution across the enterprise, businesses can now mitigate risks by actively protecting data across systems shared by both export-controlled and commercial projects. The solutionis effective even across the complexity of heterogeneous systems, applications, devices and data types.

Educate Users To Policies For Protecting Technical Data

Large companies often depend on the goodwill of employees and supply chain partners to enforce export control policies for the safe handling of regulated technical documents. However, misuse can often occur accidentally or through an unintended combination of entitlements. The Electronic Export Compliance solution takes the guesswork out of enforcement by automatically notifying users when they are in potential violation of policies before the violations occur, and actively preventing misuse at the same time. By automatically educating users with warning notices, companies can ensure that users accelerate project productivity by following best practices for the safe access, movement, and use of export-controlled technical data.

SOLUTION BENEFITS FOR ELECTRONIC EXPORT COMPLIANCE

NextLabs and SAP follow a proven method for implementing The solution by utilizing a combination of expert product knowledge and a services best practices methodology. When Electronic Export Compliance is deployed, clients will be assisted in identifying their controlled documents, as well as defining access control policies.

The following method defines The solution deployment process:

Step 1: Review Identity Management System

An identity management system must exist to identify and authenticate users accessing controlled data. The existing identity management system will be reviewed to determine if any enhancements are required in order to work effectively as part of the Electronic Export Compliance solution. This process must function regardless of domain or locality.

Step 2: Identify Controlled Technical Data

Technical data subject to export controls will be identified in order to control access, usage, and distribution of information.

Step 3: (If Not Yet Deployed) Deploy SAP GRC Global Trade Services

GRC Global Trade Services provides an integrated and unified report on the export of both manufactured goods and technical data. Technical data is associated with export licenses and a full report of all technical data transfers is created.

Step 4: Deploy NextLabs Information Risk Management Software

NextLabs' Information Risk Management software actively controls technical data handling and disclosure to maintain alignment with regulatory compliance. Policies are enforced at the point of data use, including extended enterprise locations across the business and supply chain, and across devices when users are mobile, even when they are disconnected from the network.

Step 5: Define Controlled Technical Data Authorized Users

Users authorized to access controlled technical data are identified in order to define appropriate access controls. Users will be granted access to information subject to defined usage restrictions that are automatically enforced.

Export compliance policies are defined and may cover various aspects of information access and usage to assure compliance with information export regulations, e.g. restricting communications of controlled information only over approved channels, preventing controlled information from contaminating commercial projects, and others.

Detailed reports cover denied information exports and approved information exports are matched to the covering TAA licenses for comprehensive auditing. Reports can be accessed through a single interface that covers exports of both physical goods and services, and electronic data.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.