WHITE PAPER

NEXTLABS

Enterprise Governance, Risk, and Compliance Solution for Information Export Control

AEROSPACE AND DEFENSE, HIGH TECH, AND INDUSTRIAL COMPANIES CAN IDENTIFY, CONTROL, AND AUDIT THE FLOW OF TECHNICAL DOCUMENTS TO ENSURE AND DEMONSTRATE ITAR AND EAR COMPLIANCE

EXECUTIVE SUMMARY

Export controls, such as the International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and similar regulations, govern the transfer of items including defense articles, services, and technical data from U.S. commercial companies to foreign persons outside or within the U.S. Effective compliance requires safeguards across several domains, including physical and network security, project management, and trade management, and includes effective controls on the flow of sensitive technologies, defense articles and related technical data.

The eGRC Solution for Information Export Control allows organizations to automate how technical data is identified, controlled, and audited to ensure that the disclosure or export of such data meets regulatory requirements. The solution integrates with other domains and solutions for a comprehensive approach. The eGRC Solution for Information Export Control enforces policies to govern:

- Access to export-controlled data and systems, such as those that are ITAR or EAR regulated, by non-approved or unauthorized persons.
- Handling of export-controlled technical data that could expose information to risks by providing accessibility to non-approved or unauthorized persons.
- Accounting for the export of technical data under an export license, technical assistance agreement (TAA), or global program management authorization (PMA).
- Contamination of commercial products with export-controlled technology.
- Transmission or storage of export-controlled technical data across or within systems that are administered by non-approved or unauthorized administrators, and are used for both defense and commercial applications.
- Accidental export or unauthorized access of technical data by mobile employees.
- Businesses can now control exposure of technical data where misuse and conflicts of interest can result in costly fines, audits, and related damages. Benefits include:
- Minimize the risk of inappropriate disclosure – reduce costly fines and penalties by actively preventing violations, and maintain national security integrity.
- Economize multi-use environments – reduce IT overhead by eliminating redundant controls used for both export-controlled and commercial projects.
- Quickly demonstrate compliance – expedite investigations by proving that information disclosure is appropriately controlled and documented.
- Educate users on procedures to protect technical data – ensure that users follow best practices to accelerate project productivity without incurring violations.

- Handling of export-controlled technical data that could expose information to risks by providing accessibility to non-approved or unauthorized persons.
- Accounting for the export of technical data under an export license, technical assistance agreement (TAA), or global program management authorization (PMA).
- Contamination of commercial products with export-controlled technology.
- Transmission or storage of export-controlled technical data across or within systems that are administered by non-approved or unauthorized administrators, and are used for both defense and commercial applications.
- Accidental export or unauthorized access of technical data by mobile employees.
- Businesses can now control exposure of technical data where misuse and conflicts of interest can result in costly fines, audits, and related damages. Benefits include:
- Minimize the risk of inappropriate disclosure – reduce costly fines and penalties by actively preventing violations, and maintain national security integrity.
- Economize multi-use environments – reduce IT overhead by eliminating redundant controls used for both export-controlled and commercial projects.
- Quickly demonstrate compliance – expedite investigations by proving that information disclosure is appropriately controlled and documented.
- Educate users on procedures to protect technical data – ensure that users follow best practices to accelerate project productivity without incurring violations.

The eGRC Solution for Information Export Control integrates seamlessly both within and across the extended enterprise to include partners, outsourcers and contractors. The platform approach, built on NextLabs®'s Data Protection®, IBM®'s Tivoli® Identity Manager, and SAP® GRC Global Trade Services, delivers a policy-based solution that leverages existing identity management and trade management applications for rapid time-to-value. Aerospace and Defense, High Tech, and Industrial firms can now quickly enforce controls that minimize risks to technical data and support the safe completion of export-controlled projects.

OVERVIEW

Many Aerospace and Defense, High Tech and Industrial companies use SAP GRC Global Trade Services (GTS) to manage compliance with the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) for export controls. Compliance includes two focus areas:

- Tracking and controlling the shipment of export-controlled product orders under an export license, and
- Tracking and controlling the transfer of export-controlled technical data that must also be made under an appropriate license or technical assistance agreement (TAA).

SAP GTS is optimized for tracking and controlling the shipment of export-controlled product orders. For such orders, companies obtain a license from the government to ship particular items to a foreign firm, government or individual. The license limits the shipment of goods under that license based on quantity, or quantity and value. When ITAR- or EAR-controlled orders are processed for shipment, SAP GTS manages compliance and approval of the shipment and decrements the appropriate license by the amount of the shipment.

Today, the transfer of technical data is not managed by GTS. As such, companies require a solution to track and manage transfers of technical data against TAAs in the same way that GTS manages shipments of export-controlled product orders. However, defense articles are both quantifiable and physical, while companies operate and use data within a complex, geographically diverse, environment. Compounding the problem, partners, suppliers, contractors, and outsourcers that help support business goals also multiply the risks to data confidentiality during collaboration.

Given the isolated point products available till now to protect data, the ability to maintain comprehensive control of technical data has been a daunting task. Current solutions fail to provide complete coverage or account for conditional business use of data that is inappropriate. As a result, many companies simply accept the risks and resign themselves to paying compulsory fines when data is misused as an inevitable cost for doing business with the U.S. Government.

To successfully fulfill contracts and manage business relationships, technical data controls need to move beyond simply "who has access to what" to a systematic determination of appropriate usage based on user roles, acceptable use activities, locations for doing business, data sensitivity, and a range of attributes that can be evaluated against export policies.

With the solution, companies can now:

- Identify and track information resources within the enterprise and across the extended enterprise to include the supply chain
- Monitor technical data access, movement, and use, and define boundaries for exposure, to ensure activities are aligned with export policies, and
- Audit and report technical data use and export with license and TAA tracking for export control accountability.

The solution operates transparently to ensure companies remain productive, while conforming to export regulation policies for technical data control. With this solution, data mobility is controlled to prevent unauthorized exposure, while all activities are centrally monitored to demonstrate export policy compliance. The solution provides a reliable means to control data in alignment with ITAR and EAR policies to reduce the risks that result in expensive fines, damage to business reputation, and costly remediation.

Benefits to Clients:

- Protect sensitive export-controlled technical documents, such as defense data, from being leaked to unauthorized recipients
- Collaborate securely with partners across dispersed networks
- Control data mobility across global business environments to prevent exposure risks
- Demonstrate regulatory compliance with accurate reporting across the entire organization

Definitions

ITAR - International Traffic in Arms Regulations

EAR - Export Administration Regulations

Links

US Department of State, Directorate of Defense Trade Controls

http://pmddtc.state.gov

Export Administration Regulations Database

PROBLEMS OF EXISTING APPROACHES TO CONTROL EXPORT DATA

Controlling ITAR- or EAR-related technical data disclosure and export, without gaps, requires the active enforcement of information policies for the use and export of controlled data within the enterprise and across the extended enterprise. Different systems, devices, applications, users, locations, and data types combine to create a complex business environment during export-controlled projects that today's approaches for protecting information disclosure fail to adequately resolve.

The lack of a comprehensive approach results in uncertain visibility and enforcement gaps that ultimately expose regulated companies to risks such as fines and costly remediation. Weaknesses with current approaches include the following:

Perimeter Security Control

Controls such as firewalls, and intrusion detection and prevention, primarily focus on external threats that enter or leave an organization's network. However, companies must be able to maintain openly productive information flow between employees, partners, outsourcers and contractors across multiple locations, without exposing data to risks. Because of the complexity of export-controlled information use during projects, perimeter controls do not adequately account for the complexity of today's supply chains that incorporate multiple locations and organizations. Existing solutions either leave enforcement gaps that risk disclosing classified information, or they impede the productivity of mixed commercial and export-controlled projects.

Application Controls

Application-based access and authentication controls are the most common protective measures for export-controlled technical data. These are based on trust, similar to perimeter controls. Once an authorized user legitimately enters an export protected application such as a database, its access and authentication controls do nothing to protect subsequent movement of technical data that is copied and transmitted outside the application. Violations, unintentional or otherwise, can occur immediately once an approved or authorized user distributes, copies, or stores data in a manner that is inconsistent with the export-control regulations.

Applications that are typically used for storing ITAR and EAR data include the following:

- Enterprise Resource Planning (ERP)
- Product Lifecycle Management (PLM)
- Customer Relationship Management (CRM)
- Manufacturing Execution Systems (MES)
- Collaboration
- Portals

Document Management Systems (DMS)

DMS is used to store and track the use of documents, or images of documents. Users are often required to add descriptive "tags" to facilitate management of information in free-form files created with an office application, such as a word processor. The main use of DMS is for a small subset of enterprise documents with heavy workflow and long lifecycle requirements, such as for a legal department. However, these systems cannot protect technical data in files outside the DMS system, including those sent elsewhere outside the organization using e-mail or instant messaging.

Digital Rights Management

Technology that handles the description, layering, analysis, valuation, trading and monitoring of legal or access authorization rights of a digital work, DRM is used most often in context of electronic media such as music or movies. DRM may be used for export-controlled technical documents to prevent unauthorized tampering and to create an audit trail for compliance, but still has similar weaknesses to a document management system. DRM suffers from low scalability when applied to complex environments of millions of documents, using rights that are embedded within each file, and also lacks accounting when file movement requires tracking against export licenses.

Enterprise Content Management

ECM is a popular catch-all term for complementary systems that capture, store, retrieve, and disseminate digital files for use in an enterprise and their lifecycle management. It is closely related to DMS discussed above. These solutions often fail to understand the complexity of export-controlled projects and the business relationships that include user authorizations, extended enterprise collaboration, and user mobility.

A POLICY-BASED APPROACH SOLUTION

The eGRC Solution for Information Export Control ensures that information use and export are aligned with the requirements of export controls, such as ITAR and EAR, while ensuring that technical data is accessed only by approved or authorized employees, partners, outsourcers, and contractors.

This comprehensive approach allows companies within complex regulatory environments to systematically reduce risks. The solution automatically identifies user roles and systems; actively enforces controls wherever and whenever export-controlled technical data flows; and audits information access, movement, and use by integrating seamlessly with existing workflow and reporting systems. Controls, enforced across each point of use, ensure that companies avoid disclosure of export-controlled technical data. The solution includes:

The eGRC Solution Enforces Policies

The eGRC Solution for Information Export Control is a policy-based information control platform. The platform translates export control policies, expressed in business terms, into system level controls at all points where technical data is accessed and used.

A central policy authority maintains ITAR and EAR controls that govern technical data export to ensure regulatory compliance. Policies are enforced at each point of information use in real time. Enforcement includes extended enterprise locations including remote users, contractors and other partners. Information controls are effective when devices are disconnected from the network or even when connected to non-company networks.

The eGRC Solution for Information Export Control automates technical data controls for large, complex organizations. With the eGRC Solution, export control policies are developed, optimized, and distributed throughout the organization using Smart DeploymentTM. Policies may be updated as often as required based on new export control requirements. The solution provides export control policy analysts with information-in-use monitoring, auditing, and reporting. Instances of information misuse or inappropriate disclosure attempts are identified. Auditing and reporting allows the organization to demonstrate the effectiveness of export controls.

Enabling information export controls is made possible through the 4GL Active Control Policy Language (ACPL). This key innovation provides the ability to simplify and automate policy deployment from the top down. The eGRC Solution for Information Export Control automatically adapts information policies, classification rules, and information entitlements as the organization and underlying infrastructure change.

Single policy statements can control a large number of documents and users with minimal overhead. This simple, centralized, cost-effective process eliminates the need for a large staff to manage and operate the System even while providing the precision needed to meet technical data governance and export control requirements.

Identity Management for Applying Entitlements Appropriately

The eGRC Solution for Information Export Control incorporates details about user attributes and business environment resources to actively enforce export control policies. The solution automatically determines whether users are approved or authorized to access, use, disclose, or export technical data. It enforces export control policies across applications and systems where technical data resides, such as desktops, files servers, document repositories, and mobile devices. By leveraging existing identity management systems to track users and assets, the eGRC Solution for Information Export Control accurately enforces policies that understand complex regulatory-controlled environments, even as users and systems change over time.

Avoid Conflicts of Interest and Improper Disclosure of Technical Data

Today's Aerospace and Defense, High Tech and Industrial industries are under pressure to comply with export control regulations in order to protect the interests of national security, while attempting to efficiently operate within a complex business environment where information must be shared. However, a geographically dispersed supply chain, overlaps in resources used between government and commercial projects, and a highly mobile workforce combine to create risks and exposure for technical data. Companies struggle to avoid conflicts of interest and inappropriate data disclosure within this environment while trying to maintain the agility to satisfy business needs and optimize operations.

At the same time, companies must be able to provide accurate records of who has access to sensitive export-controlled data, when the data was accessed, and why that individual requires access. Providing employees with the right level of access to the right information sometimes take days or even weeks, as multiple people have to sift through approval requests.

Automating and maintaining controls over technical data has become a daunting task. Current solutions fail to provide complete coverage or account for a complex business environment. Additionally, every application developed in house or purchased from vendors requires customization to provide regulatory mandated security access. As a result, companies resign to paying fines if regulated technical data is exposed, while accepting risk consequences as inevitable.

Identity Management

Security is a critical issue for organizations of all sizes and in all industries, and will continue to be for many years. To safely complete projects while maintaining technical data protection, information controls need to move beyond who has access to what. Controlling technical data use and export may require certifying users, restricting access locations, logging access attempts, and checking additional attributes prior to authorizing a process.

Advanced identity management solutions are a critical component of managing access to export-controlled data. Today's federated business models include global suppliers and manufacturers that require access to sensitive data in order to deliver products and components. Managing proper access to sensitive information is a monumental task that requires provisioning both internal and external users. Identity management solutions offer assistance in this regard by providing automatic provisioning and federated identity management solutions.

Identity management systems help improve cost efficiencies, enable effective processes, and promote user satisfaction while providing a high degree of security. It facilitates the overall identity management process with tools and methodologies for centralizing the management of users and their access to resources, delegating administration to different business units or groups, and bringing users, systems and applications online quickly. Identity management systems provide a full audit trail to assist in demonstrating export controls and regulatory compliance.

The eGRC Solution for Information Export Control allows project teams to authenticate and authorize approved users, control use and export of export-controlled technical data in accordance with business policies, and audit data flow to demonstrate regulatory compliance. Combining all three elements provides an end to end security solution that enables companies to demonstrate compliance with export control regulations, while minimizing any impact to normal business operations.

The solution actively enforces controls by understanding the complex, business context variables for appropriate data use and export. Collaboration within the enterprise and across the extended enterprise, which includes the supply chain and a mobile workforce, can now safely take place to prevent inappropriate exposure while all use activities are centrally monitored and audited to demonstrate export policy compliance.

Global Trade Management Support for License Auditing

Systems such as SAP GRC Global Trade Services can be integrated in order to consistently manage trade processes for ITAR- and EAR-related technical data, as well as hardware products. The solution can identify data associated with export licenses or technical assistance agreements (TAAs) tracked through GTS, and report to GTS the status of data use and export movement against valid licenses.

LEVERAGING SAP 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 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 the NextLabs' NextLabs Data Protection application, 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 in NextLabs Data Protection, if necessary.

SCENARIOS TO PROTECT ITAR TECHNICAL DATA

The eGRC Solution for Information Export Control 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.

The eGRC Solution for Information Export Control

To prevent inappropriate disclosure, and ensure data use and export complies with regulatory policies, the eGRC Solution for

Information Export Control solution provides the following controls:

The eGRC Solution for Information Export Control 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.

The eGRC Solution for Information Export Control

To prevent inappropriate disclosure, and ensure data use and export complies with regulatory policies, the eGRC Solution for Information Export Control solution provides the following controls:

Limiting Access to ITAR Technical Data

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 eGRC Solution for Information Export Control, 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 bridge 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 eGRC Solution for Information Export Control 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 eGRC Solution for Information Export Control 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 eGRC Solution for Information Export Control 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 eGRC Solution for Information Export Control, 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 eGRC Solution for Information Export Control 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 end point 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 eGRC Solution for Information Export Control 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 EXPORT CONTROL 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 prove export control regulatory compliance meets business goals.

Minimize the Risk of Inappropriate Disclosure

The eGRC Solution for Information Export Control enforces export control policies in real time at each point of information use to insure 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 eGRC Solution for Information Export Control 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 eGRC Solution for Information Export Control across the enterprise, businesses can now mitigate risks by actively protecting data across systems shared by both export-controlled and commercial projects. The solution is 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 eGRC Solution for Information Export Control 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.

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.

NEXTLABS