



# Aerospace & Defense

**Information Risk Management Solutions that Control and Audit Information Flow to Comply with Export Regulations, and Protect Sensitive Data from Conflicts of Interest and Loss**



## Information Risk Management Challenges

Today's aerospace and defense industry is under intense pressure to comply with regulatory controls, and protect sensitive data against conflicts of interest and leakage, within a complex networked environment. A geographically dispersed supply chain, resource overlap between government and commercial projects, multiple client projects, and a mobile workforce combine to create a challenging environment to manage risk and compliance when the workforce collaborates and discloses export restricted information (ERI) or intellectual property (IP). Companies struggle to avoid severe penalties and loss of business integrity within this environment, while also trying to stay agile to business needs.

Automating and maintaining effective, top-down policies that can efficiently drive information compliance and protection is difficult. Monitoring data access and export license compliance, applying consistent data loss controls across all communication channels and endpoints, and preventing conflicts of interest, are daunting tasks. As a result, many companies resign to paying regulatory fines when information is compromised, suffer brand damage and client lawsuits, while accepting the consequences as inevitable.

## The Solution

The Solution for aerospace and defense companies from NextLabs® improves compliance and reduces data loss. A&D companies can now

comply with regulations for ERI, prevent IP leakage throughout the global supply chain and during product lifecycles, prevent internal conflicts of interest, and stop data loss at endpoints. The Solution helps to safeguard information within the enterprise, ensure compliance with export regulations when dealing with employees and global suppliers, mitigate data loss at endpoints, and restrict access to controlled information to authorized users.

## Identity-Driven Policy to Enforce Data Confidentiality and Data Protection Controls

The Solution is designed to address requirements that deal with the disclosure and protection of ERI, IP, and confidential data. It integrates with, and leverages, existing infrastructure to apply identity-driven policies across users and resources. Identity-driven policies understand user context and environment variables to enforce appropriate policies to prevent data loss and inappropriate disclosure.

Solutions address information risk management requirements by enabling A&D companies to:

- Identify authorized users and define proper access controls
- Identify controlled ERI, IP, and confidential data
- Control data access, use, and disclosure according to defined policies and regulations
- Align controls with corresponding business policies, regulatory rules, and contractual obligations, and

## Aerospace & Defense Applications

- **Export Control for Technical Data**  
Control and audit information flow to comply with export regulations
- **Intellectual Property Protection**  
Prevent data loss across the supply chain and during the product lifecycle, and stop conflict of interest activity between project teams
- **Data Loss Prevention**  
Stop leakage and improper data loss, inside and outside the enterprise



- Provide a full audit trail of data flow history and user activity to satisfy internal and regulatory compliance requirements.

### Key Applications

The Solution includes three (3) key applications to address information compliance and protection problems and workflow scenarios that are specific to Aerospace & Defense firms.

#### Export Control for Technical Data

Technical data disclosure is tracked and audited to comply with authorized use and export licenses, while denying improper party access, as information is accessed and handled across borders, extended enterprises, and the global supply chain. In addition, users are educated of safe handling policies, remediation procedures are automated to enable compliance, and inappropriate disclosure is prevented.

#### Intellectual Property Protection

It is essential to protect intellectual property across global supply chains and during product lifecycles to reduce risk of data loss, and enable safe and compliant communication and collaboration between project teams. The application enforces non-disclosure internally between teams to avoid conflicts of interest and IP misuse. Appropriate handling procedures are automated to improve compliance, avoid loss, and inappropriate disclosure. Most importantly, confidentiality is protected across extended enterprises to support partner collaboration. Data loss across endpoints and com-

munication channels is prevented, with complete auditing and reporting during the product lifecycle and supply chain collaboration to ease audit and compliance.

#### Data Loss Prevention

Information on desktops or mobile devices is easily leaked when copied to removable media, uploaded or copied to unsafe areas such as unsecured FTP, or misdirected via e-mail or IM to wrong recipients. It is important to protect ERI, IP, and confidential client data from inappropriate access and disclosure, even when users are off the network or disconnected—while educating them of policies, and automating document workflow and remediation procedures to eliminate user errors and simplify information use.

#### Solution Deployment

NextLabs utilizes a combination of GRC and security expertise, industry best practices, and proven services and implementation methodology to deliver a solution built on its leading information risk management software.

The deployment process includes:

- **Step 1:** Monitor, record, and analyze information handling activities to discover and identify the risks of data loss.
- **Step 2:** Author, manage, and deploy policies using a XACML-based 4GL policy language (ACPL<sup>®</sup>) to achieve information compliance and data protection controls across applications and communication channels.

- **Step 3:** Apply controls to educate users about policies and procedures; automate workflow and remediation to improve data handling; or block activities or alert policy stakeholders.
- **Step 4:** Measure the effectiveness of information compliance and protection controls with reporting, continuous audit, and compliance analysis.

### About NextLabs

NextLabs<sup>®</sup>, Inc. is the leading provider of policy-driven information risk management software for Global 5000 enterprises. Our software offers a cohesive solution for improving compliance and mitigating information risk by preventing internal and external data loss, eliminating conflict-of-interest activity, and ensuring proper access to applications and data.

Our flagship products, Enterprise DLP<sup>™</sup> and Compliant Enterprise<sup>®</sup>, combine identity-driven policy with fine-grained access control and data loss prevention technology to protect data and enforce entitlements. By reducing the risk of data loss and unauthorized access to applications and data, NextLabs helps organizations ensure public confidence, demonstrate compliance, and maintain competitive advantage.

**For More Information, Visit [www.nextlabs.com](http://www.nextlabs.com) or Call 800-898-3065**

© 2007-2008 NextLabs, Inc. All Rights Reserved. NextLabs, the NextLabs Logo, Compliant Enterprise, and Enterprise DLP, are trademarks or registered trademarks of NextLabs, Inc. in the United States. All other trademarks trademarks are the property of their respective owners. 3-08