NEXTLABS®

White Paper

Secure Global Collaboration with Information Labeling and Handling (ILH)

Using ILH To Implement A Sustainable Security Framework For Global Collaboration

EXECUTIVE SUMMARY

The Aerospace and Defense (A&D) industry is a significant target for what has become a common problem – the theft and corruption of proprietary information over the internet. The emergence and growing sophistication of Advanced Persistent Threat (APT) illustrates the urgency with which the Aerospace and Defense (A&D) industry must devise practical, usable solutions that can and should be used consistently to protect intellectual property.

A&D companies are tasked with guarding the proprietary information that passes through their hands during the course of contract performance. That same information must also be shared with customers, collaborating partners and suppliers in their engineering, manufacturing and logistical processes. Protecting that information requires hundreds of complex policies, regulations, contracts and licenses, many of them spanning national and international borders. Companies must be able to interpret those policies and regulations, identify data sensitivity and apply access and data protection controls consistently across organizations to meet information security requirements. Security technologies and standards do already exist, including digital policy management, data labeling, access control and rights management. But the A&D industry has lacked integrated solutions that bring those technologies together. An infrastructure that streamlines assured information collaboration for multiple programs is, at best, challenging to implement, scale and sustain. So, the industry continues to rely heavily on end users and manual security procedures that, because they are costly and cumbersome, can hinder their use and therefore obstruct a truly secure collaborative environment.

INTRODUCTION TO INFORMATION LABELING AND HANDLING (ILH)

The Transglobal Secure Collaboration Program (TSCP) recognized this gap in security solutions and has brought together leading A&D companies, government agencies and technology vendors to collaborate on the Information Labeling and Handing (ILH) specification.1 The result is an ILH specification with interfaces and good practice processes that bring together digital policy management, document labeling, access control and rights management that will enable consistent enforcement of security policies and regulations.

At the recent TSCP Expo in the Netherlands, TSCP's ILH team demonstrated key features of the specification that are supported by commercial products and are installed at three A&D organizations: Boeing, BAE Systems and Lockheed Martin. While the design platform used by TSCP is the A&D industry, the framework may be applied to any industry platform that must protect high-value intellectual property that is shared across organizations. Upon completion of the ILH v.1 specification and implementation guidance, companies will be able to choose their solutions from among commercial-off-the-shelf products available from vendors. They will use ILH to align security with policy and usability to streamline the administrative, end user and audit processes, bringing new technology to market more quickly, securely, and at lower cost.

This paper introduces ILH, its functional approach, components and application.

THE CHALLENGE OF SECURING GLOBAL COLLABORATION

To understand the challenge, it is helpful to recognize the context in which defense technology is shared. Today, large engineering and manufacturing projects are performed across borders, with all the accompanying laws and regulations that govern the export and import of hardware, software and intellectual property. Multiply a single program several times for each collaborator, and this may involve the participation of multiple countries, hundreds of companies and thousands of people, consuming and sharing terabytes of data. For example, the F-35 Lightning II Program, also known as the Joint Strike Fighter (JSF) Program, is a multinational cooperative development program comprised of nine partner nations: the United States, United Kingdom, Italy, The Netherlands, Turkey, Australia, Canada, Denmark and Norway. Members from these countries are spread across a dozen Integrated Product Teams (IPTs) for Component Design, Weapons Integration, Manufacturing, and Testing, among others.

MANAGING THE RULES OF ENGAGEMENT

Regulations, contracts and licenses that establish the policies for secure collaboration govern how the information is handled and exchanged between companies, including the classification, access and protection of data. But each company may have multiple programs, each with its own policies. Traditional strategies rely heavily on end users, Compliance Managers and IT Administrators who evaluate data manually. For example, it is common to require export, intellectual property and contract subject matter experts (SMEs) to review data exchange, and often, end users must work across multiple application silos to share information with multiple parties.

Automating or even streamlining policy enforcement must overcome:

1. Inconsistent interpretation of policy

- Export licenses or non-disclosure agreements are written in human-readable form and independently interpreted and implemented by legal, compliance and IT professionals, resulting in inconsistent interpretation.

2. Inconsistent labeling of information

- There is no shared scheme for labeling data, which results in inconsistent policy application.

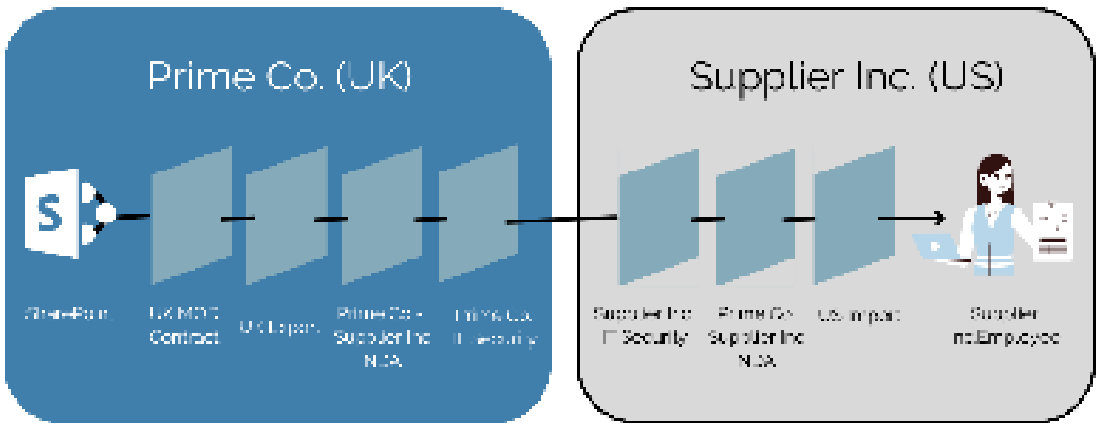
3. Absence of security metadata

- Automation of policy enforcement requires reliable metadata on information resources, so that security products can recognize information classification and sensitivity. Few labeling implementations provide reliable security metadata.

A prime contractor (Prime Co.) in the United Kingdom (UK) allows an external U.S partner (Supplier Inc.) to access technical drawings from a Microsoft Microsoft SharePoint application; access to the data must be compliant with policies from multiple jurisdictions and companies,
including:

- Contractual obligations required by the government customer
- Technology export regulations and licenses from UK agencies
- IP (Intellectual Property) licenses, such as Non-disclosure Agreements (NDA) between Prime Co. and the Supplier Inc.
- Technology import regulations from US agencies
- Prime Co and Supplier Inc Corporate policies, such as acceptable use or corporate
- hygiene.

The following diagram illustrates **the common act of accessing a document, which is governed by at least seven policies from four jurisdictions: the UK, the US, both companies, and the government agency customer.**



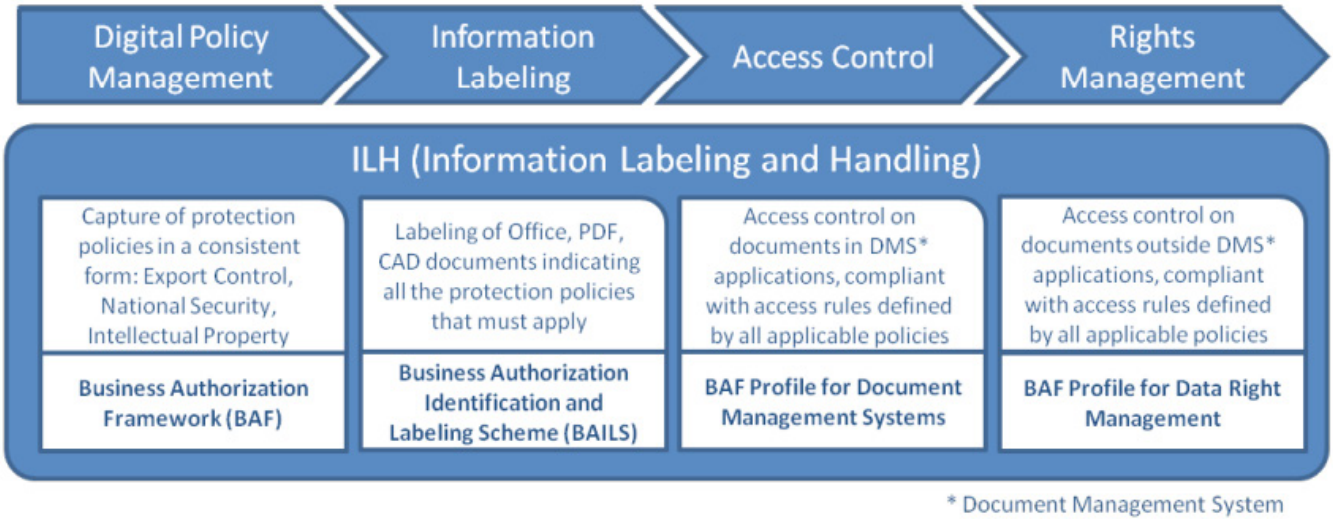
Supplier Access to Prime Contractor Technical Data

SUSTAINABLE SECURITY MANAGEMENT

ILH is a specification of data structures and good practice processes that define consistent interface formats between digital policy management, data labeling, access control and rights management. The ILH specification applies existing technology standards and works hand-in-hand with other TSCP specifications for authentication, identity federation and secure communications. It provides companies with prescriptive guidance that can be implemented using commercial-off-the-shelf (COTS) products from participating technology vendors.

Figure 2 illustrates that ILH is comprised of multiple components, including the Business Authorization Framework (BAF), Business Authorization Identification and Labeling Scheme (BAILS) and access control profiles for document management and rights management.

Figure 1: ILH Overview



A legal or compliance professional can transform human-readable policy documents such as regulations, licenses or contracts into consistent and interoperable information protection profiles called Business Authorizations. The Business Authorizations are collected and enriched with information to produce a Business Context Specific Protection Profile (BCSPP), which provides implementation detail to participating organizations. A set of Business Authorizations created for use within a specific business context, such as an A&D program, are collected in a BCSPP.

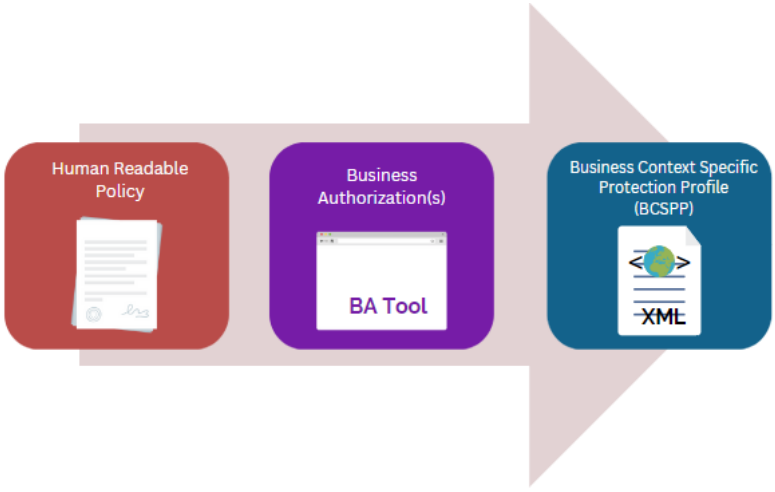


Figure 2: Business Framework Authorization Process

In the context of an A&D program, Business Authorizations may represent export licenses, intellectual property licenses and national security requirements for a program. The Business Authorization data structure holds detailed and consistent interpretation of source policy terms that, when combined with defined security categories and user attributes, establish the criteria and rules for determining access, thus addressing the challenge of inconsistent interpretation of policy. With input from legal subject matter experts, Business Authorizations are designed to support a number of relevant policy types, including common export licenses and intellectual property agreements. BAF-enabled digital policy management tools, as illustrated in Figure 3, will soon become commercially available from TSCP technology members.

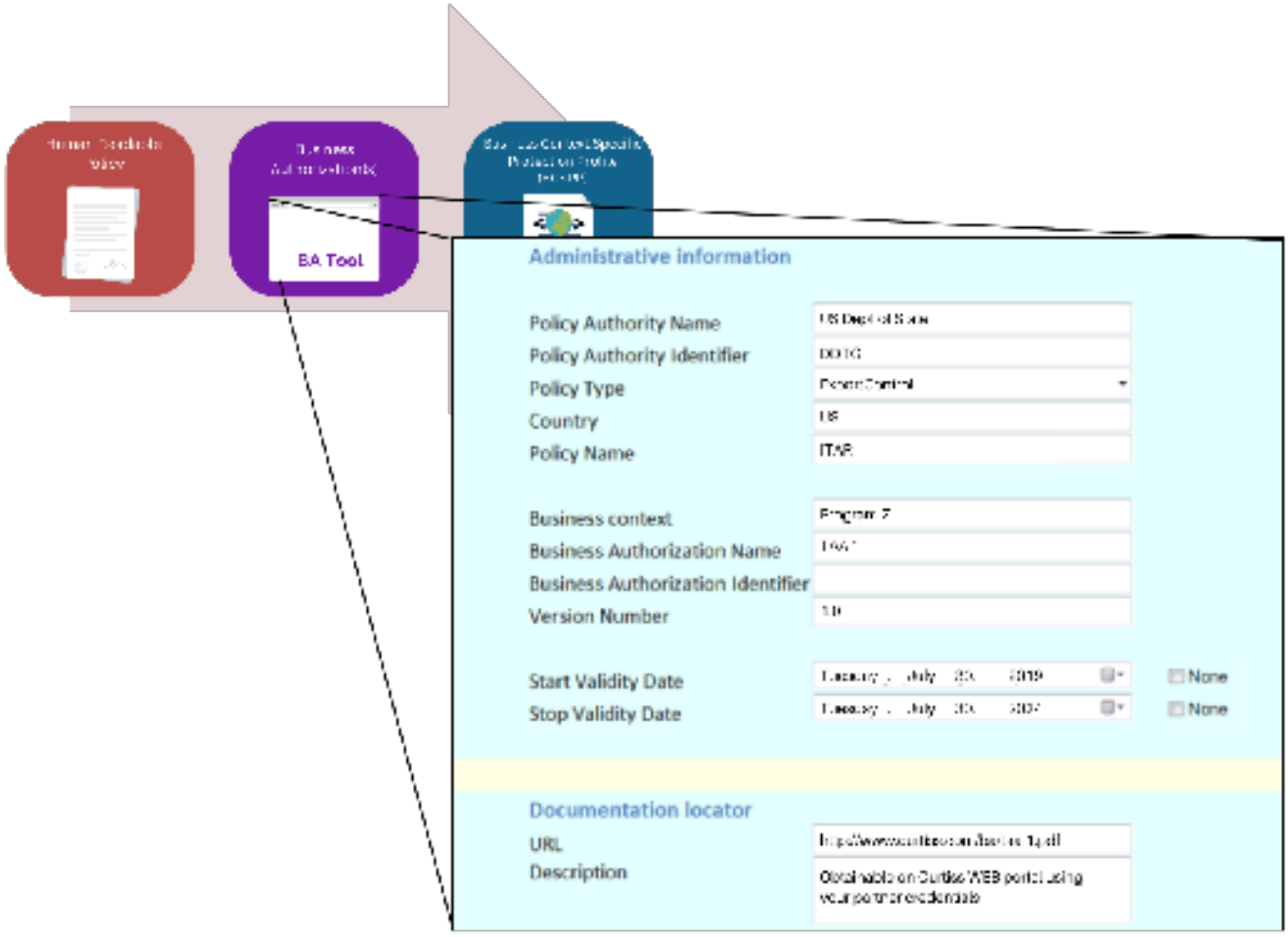


Figure 3: Business Authorization Creation

BUSINESS CONTEXT SPECIFIC PROTECTION PROFILE (BCSPP)

A Business Context Specific Protection Profile (BCSPP) allows multiple Business Authorizations to be grouped together and shared among multiple collaborating organizations. It also includes the parameters needed to configure labeling systems, access control systems and data handling controls, including requirements for user attributes used to make authorization decisions across partners.

BUSINESS AUTHORIZATION IDENTIFICATION AND LABELING SCHEME (BAILS)

In order to apply appropriate controls to data, we must be able to identify it. The ILH specification uses Business Authorization Identification and Labeling Scheme, or BAILS, which defines a logical model of metadata for representing policy requirements on information objects.

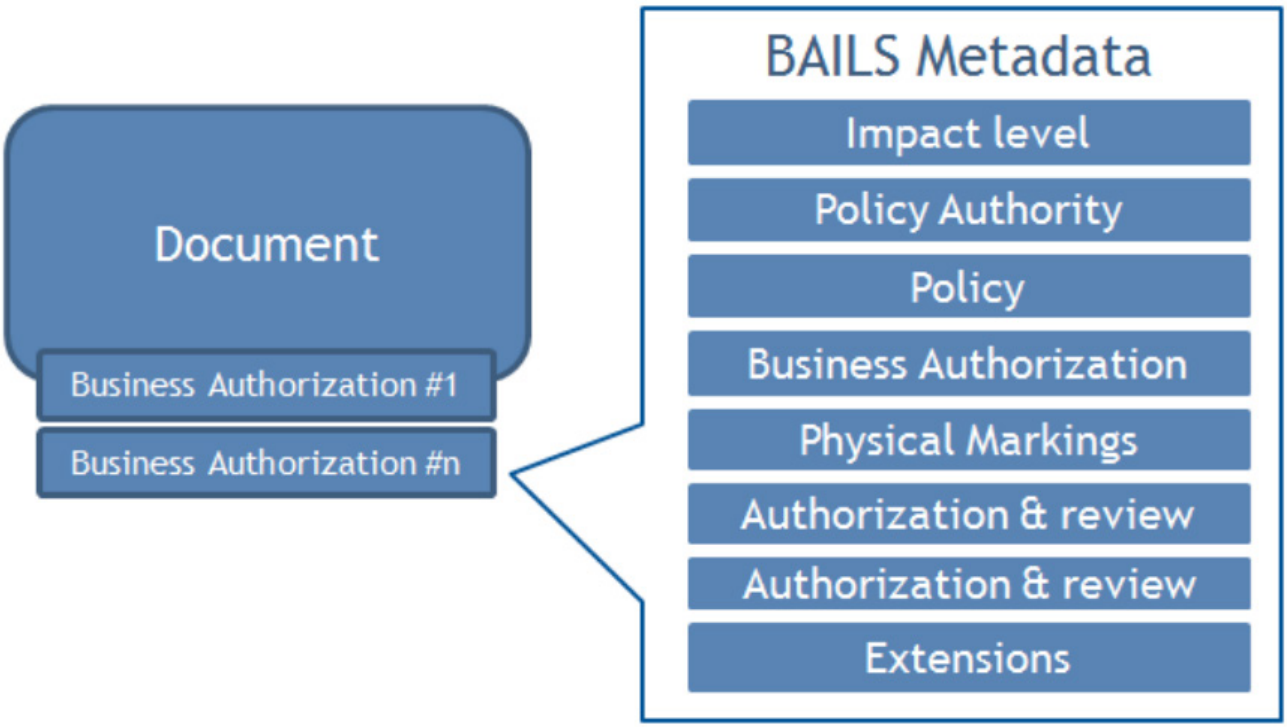


Figure 4: Logical View of BAILS

DOCUMENT MANAGEMENT ACCESS CONTROL PROFILE

Defining Business Authorizations and applying security metadata to data resources makes it possible to automate the management of Access Control. The Document Management Access Control Profile specifies how to apply the BCSPP to document management systems like Microsoft Microsoft SharePoint. The profile maps BCSPP business authorizations to different types of access control mechanisms, including traditional access control lists (ACL), role-based access control (RBAC) and attribute-based access control (ABAC) models. If a company chooses ABAC technology, the BCSPP specifies the attribute requirements to be used to make the decision, such as country, company, and business authorization.

RIGHTS MANAGEMENT PROFILE

The Document Management profile ensures proper access control on the server, but does not protect the data once it is downloaded to desktops, email and beyond. The Rights Management Profile defines how to apply persistent protection on unstructured data to enforce the access control and handling (sharing, printing, duplication) requirements. Leveraging BAILS metadata, rights consistent with business authorizations are applied directly to the document so there is persistent data protection, even after the document leaves a document management system.

ALIGNING SECURITY WITH POLICY

Alignment with business policy is critical for sustainable security management. As shown in Figure 5 using the BAF process, an organization designated as an administrative authority, perhaps a prime contractor, codifies policies originating from multiple policy authorities, such as national defense organizations or regulatory agencies. The administrative authority analyzes the human-readable contracts or agreements and generates Business Authorizations.

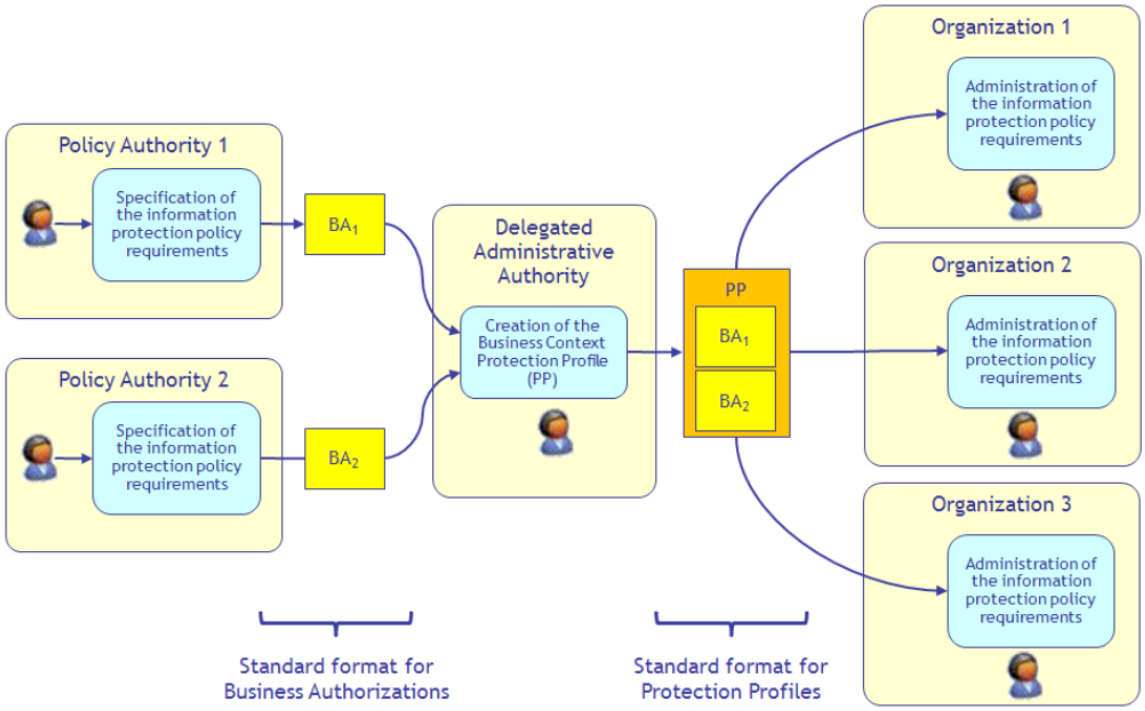


Figure 5: Management of Information Protection Policies

With the knowledge of the business context and its operational constraints, the administrative authority is able to collect relevant Business Authorizations to produce an actionable BCSPP, which is distributed to collaborating parties to be enforced consistently as security controls within their systems. In this way, ILH creates an end-to-end path from legal or regulatory policy to automated labeling, access control and handling controls, aligning IT systems directly to business requirements with minimal human translation. Depending on the security technologies in place, the implementation of labeling, access control and handling controls can be achieved either procedurally, following implementation guidance, or automatically by leveraging products with built-in support for the ILH BCSPP specification.

USE CASE 2. GLOBAL COLLABORATION - STREAMLINED ADMINISTRATIVE PROCESS

Step 1: Codifying Legal Authorizations

The administrative authority, Prime Co., establishes contracts and license agreements with the government customer and regulatory agencies respectively. These legal authorizations are codified as Business Authorizations using BAF.

Step 2: Generate Business Context Specific Protection Profile

A collection of related Business Authorizations are assembled into a BCSPP and enriched with detailed information that maps business authorizations to specific identity and labeling configurations. The process is designed to be collaborative, so that the resulting BCSPP can incorporate requirements from customers, prime contractors and suppliers.

Step 3: Distribute Protection Profile

Once codified, Prime Co. shares the BCSPP with the internal IT application owners and Supplier Inc. as an XML document, with support for the XACML standard, distributed using secure email.

Step 4: Implement Security Controls

Using the BCSPP, the IT teams at Prime Co. and Supplier Inc. implement security controls for labeling and Microsoft SharePoint access control. The BCSPP is imported into Prime Co.'s chosen labeling tool, making BAILS labels available to end users. BAILS labels are interoperable, even across organizations using different labeling tools. The BCSPP is also imported into Prime Co's Microsoft SharePoint application, either by using an ILH compatible tool that can automatically turn a BCSPP into ABAC or by following ILH guidance, which provides detailed instructions on implementing a BCSPP using standard Microsoft SharePoint permissions.

ALIGNING SECURITY AND USABILITY

Usability is often overlooked as a challenge to sustainable security. If not usable, security tools can be rejected by end users, hindering productivity and eroding the integrity of the security system. In the past, inadequate automated security controls forced users and compliance personnel to manually review and package technical data and distribute that data to each supplier separately. The ILH specifications imbed security procedures directly into the information lifecycle, streamlining the end-user workflow. Labeling, marking, access control and data handling are automated, reducing manual procedures and minimizing mistakes. Security usability is enhanced in three key areas:

VISUAL MARKING AND SECURITY METADATA

Procedural information protection (information protected by human users who follow standard procedures) still plays an important role in protecting data. Good practice suggests always marking data. Policy may also require that controlled data be marked so that consumers of the data are aware of the sensitivity and associated handling requirements. While BCSPP ensures consistent visual markings across organizations, support for BAILS from existing COTS labeling tools from Boldon James, NextLabs and TITUS , as shown in Figure 6, enables technical interoperability and simplifies the end-user workflow for applying both visual markings and security metadata.

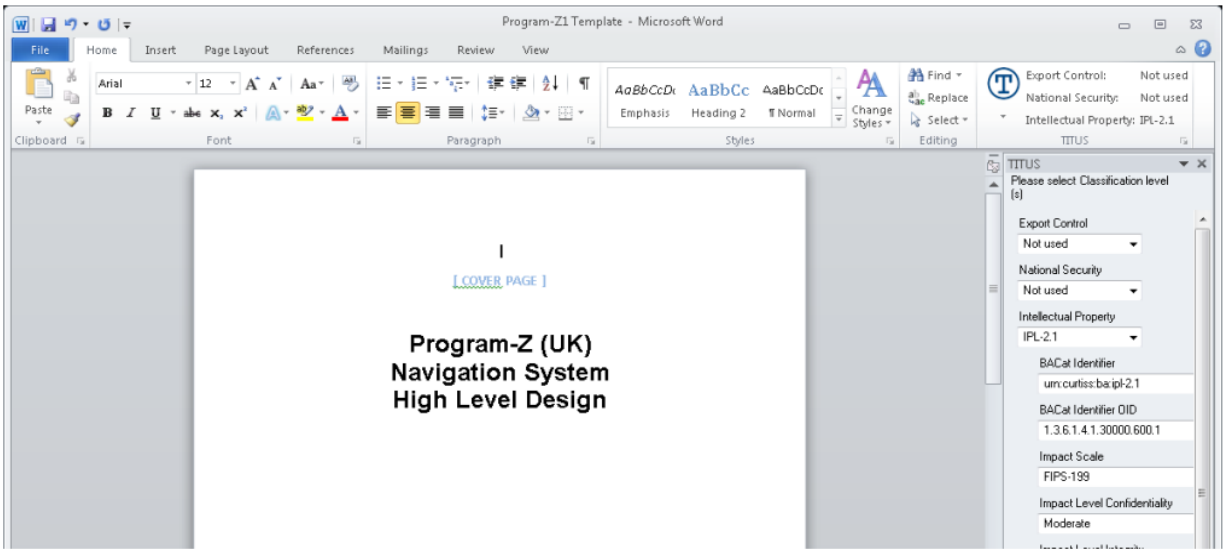


Figure 6: COTS Labeling and Marketing Enforcement

Because these tools support the BAILS specification, the user action of selecting visual markings also inserts security metadata automatically. With BAILS and BCSPP, metadata and markings created by different tools are interoperable, so that as data is shared between companies, labels and marketing are consistent, regardless of the tool used.

ACCESS CONTROL

Having access to the right information is a common usability issue. End users are required to consider access control every time they create, store, copy and retrieve data. Placing a document in the wrong location can create a data spill (provide access to unauthorized users), or make data inaccessible to authorized users. ILH can automatically limit the containers where data can be uploaded based on its BAILS metadata, and enforce proper access control, consistent with the relevant Business Authorizations.

End User Information Lifecycle

Step 1. **Easy and Consistent Labeling and Marking**

Using an ILH compatible labeling tool, when Prime Co. employees create documents, they can select labels for export compliance, national security, and intellectual property. Doing so automatically applies the required visual markings and security metadata to the document.

Step 2: Controlled Upload and Application of Access Control

When a user uploads a document to Microsoft Microsoft SharePoint, BAILS labels are automatically checked to prevent data spills and transferred to Microsoft SharePoint document columns, so that classification is visible to the end-user. Once uploaded, the correct access control is automatically applied to the document.

Step 3: Enforcement of Required Access Control

When a US employee of Supplier Inc. logs into the Prime Co. Microsoft Microsoft SharePoint portal the documents visible to the user is determined by access controls consistent with the BCSPP. Her access to the document uploaded in Step 2 is evaluated based on the current BCSPP, attributes of the user asserted as federation claims, and document metadata derived from BAILS. In this use case access is based on UK Export, NDAs between Prime Co. and Supplier Inc. and UK MOD contract requirements.

Step 4: Persistent Information Protection

When the user opens the document, she has created a copy of the document on her local workstation. At this point the protecting the document copy is left up to the end user, who is able to use the visual markings to inform her of the required handling procedures. In the future ILH will specify the application of Rights Management, available from multiple COTS

PERSISTENT DATA PROTECTION

Typically, once data leaves a managed server, reliance on end-users for security increases. With the Rights Management Profile, persistent protection is automatically applied to data, minimizing the need for users to either manually apply data protection or rely solely on manual information handling procedures.

ALIGNING SECURITY ACROSS DIVERSE ORGANIZATIONS

In practice, companies will adopt security technologies such as labeling, ABAC and rights management at different times. ILH is required to coordinate security across multiple organizations, and each company must participate in the BAF process to come to agreement on security requirements.

The agreement, articulated via the BSCPP, takes into account the systems within each participating organization. At the same time, ILH recognizes that each company has different business processes and IT environments. ILH allows each company to make its own choices about technology by providing specifications for the interfaces between organizations rather than requiring specific tools to be implemented within an organization. To enable this, ILH supports procedural protection in a consistent manner, with automated protection by capturing information required to support implementation of procedural controls. When a company decides that a security tool makes sense for them, selection of a COTS product that supports the ILH specifications will ensure compatible and interoperable collaboration among partners. This unique approach allows each organization to combine procedural and systematic security controls based on its IT maturity, size and resources.

A FRAMEWORK FOR SUSTAINABLE AND SECURE SHARING OF INTELLECTUAL PROPERTY

While the industry has experience with the use of many security products, the unification of best-of-breed products from different vendors into a sustainable solution has been lacking. ILH has taken a practical approach to design specifications that can be adopted by a diverse set of organizations, without prerequisites for technology adoption. The ILH specification fills the gaps with specifications and good-practice processes supported by COTS tools.

While the design center for ILH is the A&D industry, the framework will be useful in any industry where sensitive information is shared across organizations. Within A&D, we believe the application of ILH will help companies collaborate more efficiently and securely, bringing new products to market more quickly and at lower cost.

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.