BACKGROUND

TSCP Information Labeling and Handling

Today, companies in all sectors along with governments around the world are challenged to protect their networks and their proprietary data from the threat of covert internet attacks. Large global companies with their numerous collaborators and deep supply chains can be especially vulnerable to network compromise and the loss and corruption of data, since that very relationship and the processes that enable collaboration can create gaps, and therefore vulnerabilities, while sharing among customers, partners and suppliers in their engineering, manufacturing and logistics. The aerospace and defense industry continues to rely heavily on end users and manual security procedures that are costly and cumbersome. Without integrated technology solutions, the system will continue to be inconsistent and therefore obstruct a truly secure collaborative environment.

TSCP's Information and Labeling and Handling project is producing specifications that will lay the groundwork for commercial-off-the-shelf (COTS) solutions to ensure consistent interpretation and enforcement of existing policies, regulations, contracts and licenses by instituting the following:

Digital Policy Management will allow the analysis and capture of information protection requirements from a human-readable form to computer-processable forms that can be distributed to stakeholders to support consistent enforcement of the requirements.

Information Labeling allows organizations to label information with the indication of all the information protection requirements that must apply. This indication, consistent within and across organizations, provides support for enforcement by human users as well as by automated protection mechanisms.

Information Protection allows automated protection of information in accordance with the applicable protection policies indicated by information labels. ILH provides consistent protection within as well as outside Document Management Systems (DMS) through Data Rights Management Systems.

The ILH specifications are being tested and implemented by some TSCP technology partners so that upon completion, they can be leveraged to deliver COTS support for any of the three areas outlined above. The ILH specification documents will provide important information, guidance and resources to enterprises that are planning to use ILH.

Business Authorization Framework (BAF)

This specification supports Digital Policy Management by defining a process model, a logical data model, and interchange formats, that organizations can use in order to: analyze and capture the policy requirements using a consistent set of constructs, which can be distributed across organizations in an interoperable manner. 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 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.

Business Authorization Identification and Labeling Scheme (BAILS)

The BAILS specification supports Digital Labeling of information objects by defining a data model of security labels, a TSCP profile that customizes the data model to TSCP needs, and bindings to actual document formats.

BAF Profile for Document Management Systems

This specification provides prescriptive guidance on the implementation of the access rules set out by the BAF on Document Management Systems (DMS) applications. The profile supports the legacy DMS applications, which access management mechanism rely on Access Control Lists (ACL), together with the more modern DMS applications that can be integrated with Attribute Based Access Control (ABAC) systems.

BAF Profile for Rights Management Systems

This specification provides prescriptive guidance on the implementation of the access rule, set out by the BA, on data protection mechanisms based on Digital Rights Management (DRM) technologies. Once extracted from the protection of Document Management Systems, documents are encrypted; any utilization of such DRM encrypted document requires an interaction with the license server, ensuring appropriate protection wherever the documents reside. Shared information can be protected on the user desktop, by meeting the same information protection policies that were already applied in the DMS systems where it came from.

ILH Policy Authoring Guidelines

This document describes the business steps that start at the contracts phase and end at the production of an implementable Business Context Protection Profile. This document provides guidelines on how to accomplish each step, independently of any specific toolset, and provides information as to how these steps can be performed using a reference tool, the Information Labeling and Handling v.1 Policy Authoring Tool. Finally, this document provides an overview of the cognitive activities involved in such a process.

ILH Policy Implementation Guidelines

This document describes the business steps that start with the acquisition of an implementable protection profile and end with its implementation among collaboration partners.

Requirements to Platform Vendors for Ensuring Data Centric Information Protection

TSCP ILH aims to provide organizations with means to protect information in accordance to all applicable protection policies, and on all types of applications

required for collaboration. One key marketplace gap that TSCP ILH has uncovered is the difficulty to ensure the same consistent protection between various types of applications, platforms, and usage. This challenge needs to be addressed at the platform level.

(Copyright TSCP, verbatim from https://www.tscp.org/ilh/)

LibreOffice 5.2 provides the following default classification, which can be personalized according to enterprise needs: