FORTRA™

SOLUTION BRIEF (Fortra)

Fortra Military Classification for NATO Security Compliance

Challenge: STANAGs 4774, 4778 And NATO today

Intelligence and military communities have historically worked in isolated silos. In recent years, these organisations have begun to embrace the need for sharing critical information with allies in an effort to receive similar critical information and intel in return.

Because the North Atlantic Treaty Organisation (NATO) includes 29 member countries, over 40 partner countries around the world and numerous partner organisations, it is imperative that information shared between these participants remains consistently classified and secured. To do so, standardisation agreements (STANAGs) must include classification conventions that create a defence fabric of international scope.

NATO, in conjunction with Commonwealth countries, has developed classification markings that permit collaboration between allies; however, navigating policies for classification of information internationally can be complex and confusing due to variation in tagging policies and end user understanding. To be effective, organisations need to employ tools that enable the use of metadata to provide access controls and visible markings that aid users in managing information. These tools must also be fully interoperable.

Users need to be able to identify and tag information using tools that follow a standardised system based on the sensitivity of the information in question. Otherwise, the potential for compromise of information is significant and this could threaten national security.

Solution: Proposed Approach

NATO has a data classification and information-sharing programme, under which all members of the organisation agree to abide by a series of rules to ensure the protection of critical data. However, the execution of this program remains incredibly difficult.

A data classification solution must enable markings and metadata to reflect the fluidity and shifts in NATO membership. Exact member groups and security access of countries within and outside of those groups is an ever-changing tapestry.

Metadata must include the date a group marking is applied as well as the identity of the countries that were part of that group at the time the document was created — because NATO groups may add or lose member nations at any time.

Fortra: How We Can Help

Fortra's Data Classification Suite (DCS) provides a common classification and policy solution that enables information-sharing in a way that minimises the risk of compromise for every country involved.

While most countries and organisations already have data security tools in place, DCS is extensible and, therefore, augments these solutions for more comprehensive protection.

The Fortra Solutions Includes The Following Capabilities:

- **Unlimited labels** — Allows for unlimited classification labels, providing organisations with a range of customisation options for NATO STANAGs or other regulation and compliance mandates.

- **Signed trusted labels** — Provides a higher level of assurance that labels have not been tampered with through cryptographical binding.

- **Classification selector** — Provides simple, inobtrusive ways for users to identify email and document sensitivity. Users are guided through the classification process with prompts and suggestions to increase accuracy and efficiency.

- **Visual markings** — Applies military-compliant visual markings in the form of headers, footers, watermarks and classification authority blocks to clearly identify information sensitivity.

- **Portion marking** — Applies classifications to individual portions of a document, and automatically upgrades the document classification to the highest portion marking in the document. A portion mark can be defined at many levels, such as a paragraph, table or image.

- **Metadata assist** — Stores user classification selections with the document as persistent metadata, which can be used to increase the accuracy and effectiveness of data loss prevention (DLP) technologies, archiving and perimeter security solutions.

- **Policy enforcement** — Inspects emails and documents for sensitive content such as personally identifiable information (PII), and provides immediate feedback so that the sender can correct any problems before the email or document leaves the desktop.

- **Security enablement** — Integrates existing security infrastructure investments with a wide range of partner solutions and provides an open extensibility model that allows for further custom integrations.

- **Administration** — Provides a centralised, web-based administration console for classification configuration and policy managementacross the entire DCS Suite of products. DCS generates user activity logs that can be monitored and analysed to measure the effectiveness of the security policies.

While NATO has created a framework for classification, member countries and partner organisations are left to execute on this classification system themselves. Without a tool to enforce classification and automate the application of markings, users across organisations apply markings inconsistently and incorrectly. Without a solution such as Fortra's Data Classification Suite Ultra Edition, these parties risk noncompliance with NATO's framework and increase the possibility of highly sensitive information—vital to international security— being compromised.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

