titus
by HelpSystems

WHITEPAPER *(Data Classification)*

Titus for Military

The Gold Standard for Data Integrity & Protection in Military Environments

Swift action to commands based on operational understanding are hallmarks of a high-performing and responsive military. And the exchange of classified and even unclassified data – often in electronic form – are the lifeblood for any military organization to thrive and achieve mission success. The key is keeping sensitive data out of the hands of the wrong people.

"With the military, there is a higher burden on the end user," notes Matthew McCormick, director of Product Management for Titus.

From coordinating sensitive ship or troop movements to exchanging crucial defense system designs with defense contractors and DoD departments, military users require a seamless way to ensure their data is classified and labeled appropriately before being shared.

Compromised data can significantly degrade a military's technological superiority, weaken situational awareness and, depending on the breach, put both individual lives and national security at risk.

And make no mistake: bad actors are looking to get at sensitive military information. The Identity Theft Resource Center's 2021 End-of-Year Data Breach Report showed 66 data compromises impacting government entities, affecting more than 3.2 million victims. This is a considerable increase from 2020, where there were 47 data compromises impacting government entities and affecting more than 1.1 million victims.

In fact, the overall number of data compromises in 2021 is up 68% from 2020, and the new record for number of data compromises is 23% over the previous all time high.

With the explosion in electronic communication, it's not surprising that email represents an added data classification challenge to military users and civilian branches of government. Out of the 1,613 reported breaches related to cyberattacks, 33% were caused by phishing, and out of the 179 reported breaches related to human and system errors, 37% were caused by email correspondence."

No Longer An Island

"Data classification is a cornerstone of the protection of our classified information," says Manfred Haelters, CIS architect responsible for safeguarding Belgian Defence's classified networks. "Without good classification, it is impossible to correctly protect our systems in general and classified information in particular."

Data sharing becomes more important as militaries collaborate and coordinate responses to crises globally. Today's military and peacekeeping missions are highly interdependent. Multinational forces work side by side, and conventional forces work closely with national agencies, local governments, non-governmental agencies, and others. To function as an integrated team, these groups must be able to share information securely, quickly, and effectively, while ensuring that secrets are not leaked out.

Alliances such as the North Atlantic Treaty Organization (NATO) underscore this interdependence. Recognizing the imperative of secure information sharing, NATO has pushed for standardization agreements that include classification conventions across their 30-member countries worldwide.

"The speed of sharing information can spell the difference between mission success or mission failure," says Haelters. "Having a weak data classification system will not only slow down the process of sharing information between partners, but also as more manual actions are required, it could completely stand in the way, as partners do not have the required confidence that too-sensitive information might leak out of their network.

"Whether working as part of an allied member within NATO or partnering closely with a single country ally, militaries are increasingly dependent on secure communication to coordinate operations, and that means their classification systems need to interoperate.

"You don't go out on a mission by yourself. You don't operate independently. Standards play an important role," observes Daniel Brodhead, acurrent reserve Naval Combat Information Officer, who serves as Project Lead and IT Consultant, who currently serves as deputy project director and IT consultant for Canada's Department of National Defence.

Canadian Armed Forces' Unique Data-Classification Imperative

Brodhead emphasizes that within the Canadian Forces, "a realization has built up over time that we need better labeling of information and a better understanding of data security standards."

From 2001 to 2014, the Canadian Armed Forces participated in the NATO Afghanistan mission – during which time "it became clear that information needed to be marked," says Brodhead. Since that time, Canada has focused on standardizing their data classification and establishing mandates around metadata.

"Having well documented requirements always matters. Every military organization looks for tools that will meet their needs, and interoperability should be front and center," he says.

Because the Canadian Armed Forces are much smaller than the U.S. military, with approximately 40,000 Army soldiers as of 2018, compared to 5 million U.S. service members, it has put more pressure on Canada to cross-train its operators, soldiers and sailors in multiple duties, and with it, understanding information management and data classification processes to do their jobs.

"Canada has been very good at focusing on training people – they have to take on more roles – we see it across the military," Brodhead explains.

Just as guards, gateways, firewalls and other network controls are essential for safeguarding data in both government and commercial enterprises, "security markings are also critical to keep information flowing. When you reach more operational status – such as tactical environments, tyou need labeling that is quick, easy and painless for the operator," Brodhead says, adding that collaborating with key industry partners will help develop solutions to meet those requirements," Brodhead adds.

Belgium Defence Weighs in on NATO's Data-Centric Security Vision & Strategy

Given the global nature of conflicts around the world, individual countries seldom act alone and require close collaboration with allies in theater.

"Almost no nation is capable of performing military operations alone anymore, and technology advancements in general will require all nations to look for better and faster means to securely exchange information," observes Haelters, a 20-year veteran of the Belgium Defence who helps protect Belgium's classified networks used by 25,000 full-time military and 3,000 civilian staff.

He points out that multi-country joint missions are already a fact today: "In almost all modern conflict theatres we intervene in alliances," he says, citing the interventions in Afghanistan, Iraq and recently in the Syrian region as examples.

Smaller countries such as Belgium frequently rely on mission partners to complement their capabilities, Haelters says, adding that even the strongest militaries such as the United States collaborate with others that have "niche information at their disposal."

Considering militaries' reliance on collaboration with other member nations, NATO has developed a common Data Centric Security Vision and Strategy. Recognizing that information sharing is vital for a healthy and battle-ready military organization, NATO has developed a set of classification markings and conventions – STANAGs 4774 and 4778 – that permit the sharing of sensitive information between allies.

STANAG 4774, for example, calls for common XML-based formats for metadata around confidential information.

But everyone knows that navigating policies for classification of information internationally can be complex and confusing. Country users neither follow the same tagging policies nor do they share the same understanding.

According to Haelters, Belgium was already applying security labels on its classified information before NATO's regulations were announced. With the arrival of NATO's data-centric security approach and related STANAGs, it now seeks industry support to enhance its existing data classification efforts, including making its information exchange gateways – or the links between classified networks – aware of these new standards.

"Over the last couple of years, Belgium has made some very significant investments in new weapons systems, which will add an order of magnitude to the quantity of exchanged information," he says.

Critical Importance of Metadata

To be effective, organizations 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 standardized 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.

"The explosion of information coming from new weapon systems, the fact that almost no nation is capable of performing military operations alone anymore and technology advancements in general will require all nations to look for better and faster means of securely exchanging information," says Haelters.

"Embracing NATO's Data Centric Security vision and strategy is key to accelerating Belgium Defence's goal of information, decision and execution superiority," he says.

Investing in user-friendly technology and automation tools that enable users to apply data classification "is a must," just as partnering with innovators in the data automation space.

"Without investments from commercial partners, nations will never be able to achieve true interoperability," Haelters says, noting that as the frequency and complexity of missions grow, NATO partners may not always be known in advance and will enter and leave ongoing missions, making interoperability "essential for a successful mission."

Data Classifcation's Military Origins

The concept of data classification – especially within government – is not new. The highly regimented practice of coding documents as "sensitive" or "classified" has been commonplace in the military and government for decades. The government and military arguably were the first to classify data. They typically could achieve sufficient data classification with approximately five "high-level buckets," with a series of sub-level, military-specific contents to further qualify its sensitivity. In contrast, today's enterprises demand granular solutions that require a "different" bucket brigade.

For this reason, military data classification is more complex, requiring a more informed user. According to Titus' Chivers, military users tend to require more guided classification where they select a value and must then pick another set of values, sometimes several levels deep.

Classification solutions that use commonly understood shortcuts like bookmark "favorites" for classification options offer one best practice Titus has employed to simplify how their government customers select from a complex set of data classification values.

The challenge is avoiding presenting users with too much complexity that interrupts their workflow.

To enable effective and secure information sharing, military organizations have historically relied on visual classification markings. But without a tool to enforce classification and automate the application of markings, users can apply markings inconsistently and incorrectly – increasing the risk of data spillage and inadvertent disclosure. Furthermore, legitimate information sharing is hindered due to cross-domain guards and rule sets rejecting the improperly formatted information.

Several government users have quickly embraced the built-in CUI feature available automatically with Office 365 subscriptions only to find that Microsoft Azure's solution doesn't meet compliance requirements. Before investing in a data classification tool, military and government users should look longer term at what their data classification needs will need to support in a rapidly evolving environment.

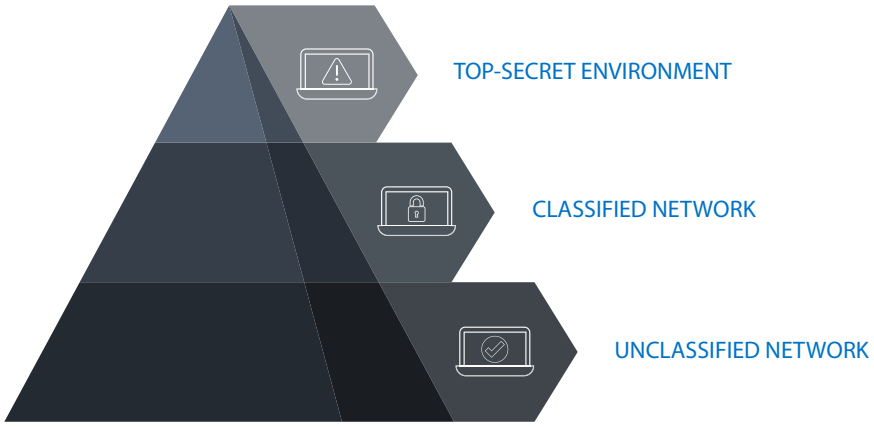
Simplifying CUI Compliance: DoD's Policy Approach

The Controlled Unclassified Information (CUI) Program, implemented in December 2017 for all DoD agencies, contractors and subcontractors, reflects this complexity. The program requires all contractors who process, store or transmit CUI – for example, the schema of a tank or unclassified nuclear information for the Department of Energy - meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards, or risk losing their DoD contracts.

The program standardizes the way all U.S. government agencies and military entities handle unclassified information that requires safeguarding. It clarifies and limits what kinds of information to protect, defines what is meant by "safeguard," reinforces existing legislation and regulations, and promotes authorized information-sharing.

The biggest chunk of government data classification needs fall under the unclassified umbrella if one imagines a pyramid. The top peak is the top-secret environment, the middle of the pyramid is the classified network and the final section is the unclassified environment.

"CUI is everywhere – at the bottom, in the middle and on the top," notes Wiesner. "But everyone lives on the unclassified environment – that's how they communicate to the world."



To date, CUI includes some 240 categories, which prompted the DoD to create their own CUI policies, distilling the extensive guidance into a manageable, simplified marking standard for every military department and agency to follow.

"The number one challenge is how to handle the complexity of the CUI program and make it relevant to their agency, without overburdening users," says Garrett Wiesner, director of Canadian and US Public Sector Sales for Titus. He advises involving users whose inherent knowledge can best guide how data gets identified and marked as CUI and handled properly. A key challenge, however, concerns determining the right mix of technology versus human intervention. "What is the balance of how much you configure automation plus user involvement into a solution?"

Value of CUI Goes Beyond Markings

Wiesner sells Titus classification solutions to both military and civilian government agencies. He notes that CUI remains new to civilian departments, with several still evaluating their requirements to assess user impact. Many are taking time to ask, "What value does it have?" "What other areas can it positively impact our environment from how the data actually gets protected?" and "How can we integrate CUI with other tools or help with our retention policy or records management?"

The risks are high for not getting it right – namely, loss of sensitive data and actionable intelligence. These organizations also struggle with how best to involve other stakeholders in this environment, Wiesner explains. Collectively, they need widespread buy-in to help vent CUI as the benefits that come from proactively identifying sensitive data can be broad, touching IT security, legal governance and privacy, leading to a more protected infrastructure.

"The value of CUI goes beyond just markings," explains Wiesner, adding that a unique challenge for the military is how to avoid co-mingling classified data markings and CUI data markings

Civilian Government Agencies also Grapple with CUI

Agencies, particularly civilian science-focused organizations, are currently exploring these questions as they look at the right solution and training approach to ensure CUI compliance that will minimize interruptions of their busy research staff. Another major challenge users face is how to evolve the current CUI system over time. They recognize that too much complexity can hurt adoption and user understanding, something today's military and civilian government departments cannot afford.

Limitations of AIP

That's why several government users embraced the CUI feature that comes automatically with Microsoft® Office 365, namely, the Microsoft Azure Information Protection (AIP) for classification/labeling. Many users have quickly discovered the solution's limitations if a government agency's data classification needs to go to the next level. AIP is a fixed framework that can only apply label or markings to specific conditions. Examples of use cases that go beyond AIP's capabilities include attaching sensitive files to an Outlook calendar invitation (AIP cannot apply markings or metadata in such an event), or copying and pasting into Word sensitive documents and either printing to a physical printer or to a PDF.

A phased implementation is best, starting simple, with the ability to evolve it over time, say experts. "Make sure you are building into your capabilities the ability to evolve the solution and tie it into other tools. If you have a best-of-breed security infrastructure in place or a roadmap for the future, you want to make sure CUI can integrate with these other tools to protect data more efficiently," Wiesner advises. "Avoid being locked into a single set of solutions – look for flexibility so that how you are marking data today and how that integrates with your current security stack of solutions adapts to future plans."

Australia: A Classification Standard Champion

The Australian Government has embraced a common data classification standard for more than 15 years. An early adopter of security marking standards to meet compliance requirements established by the country's legislature, Australia uses its Email Protective Marking Standard (EPMS V2018.2) to mandate how Australia's military personnel must use and format protective markings in all email messages exchanged within and between government agencies.

EPMS requires all emails in any Australian government department to carry labels, including what the metadata attached to those emails should look like. "It's a very structured, well laid out approach," says Chivers.

The Australian EPMS has been updated several times since it was first rolled out in 2005, and throughout these iterations it has continued to leverage user-friendly automation tools.

Open to AI

Artificial Intelligence (AI) systems are coming into play in the data classification world as a capability that can speed data detection and protection by helping apply data classification policies to ensure sensitive data is properly protected, regardless of where it resides. According to Brodhead, government and military users are definitely open to AI solutions if they can help with the complexity issue.

"Simplicity is key. The more automation you put in the better," he says.

Brodhead points out that every time an agency must retrain operators on data classification, they run the risk of the user going around the policy if they find it too complex or cumbersome. "Government and military users want to see these sorts of solutions – they want to make it easy for operators; it just needs to be proven."

Haelters with Belgium Defence notes that AI already supports image analysis and can be a far better analysis tool than simple keyword detection, because the technology can help users avoid false positives and negatives.

"Rather than replacing human analysts, AI can help them connect the dots. As a technology AI will become indispensable in the future – there will simply be too much information available for human to process," he adds.

Complying with ITAR

Over the past few years, the United States has increasingly cited national security concerns as reasons for enhanced export controls within the defense supply chain. The U.S. government's International Traffic in Arms Regulations (ITAR) deals with the export and import of defense-related articles and services on the United States Munitions List, and was implemented to ensure that sensitive materials don't fall into the hands of foreign or nefarious parties.

Complying with these mandates can be daunting without a smart data management strategy. ITAR regulations affect firms with direct contracts on defense projects as well as independent upstream suppliers of parts, components, services and software that are ultimately used in the defense sector. Non-compliance with ITAR regulation can result in significant fines, brand and reputation damage, and even potential loss of business to a competitor. The penalties for ITAR violations include civil fines up to $500,000 per violation and criminal fines of up to $1 million and/or 10 years imprisonment per violation. Even more sobering: regulatory costs are expected to double over the next five years.

Effective data security practices for ITAR include creating a data security and compliance policy, classifying your data, implementing a data leakage prevention plan, and controlling who can access data.

In an episode of our podcast series, "Titus Talks Cybersecurity," Matt Henson, CEO and co-founder of Trade Collaboration Engine, noted that the complexity of trade regulations has caused companies to trust more in automation.

"Manual processes are too slow and not responsive enough," he notes, explaining that automation and machine learning technology have advanced to the point where these technologies with human involvement are becoming more attractive to defense suppliers concerned about ITAR compliance.

As firms look at how to classify terabytes of data, they must tag the data at time of creation. Earlier automation technologies that simply scanned key words against a database frequently resulted in a high number of false positives, requiring human intervention, leading many organizations to be skeptical about automation solutions. That's all changed. Now, automation technologies have advanced to the point that if companies provide "a good data set," the software can train itself.

ITAR in a Box

Henson points out that suppliers often want a single solution – i.e. "ITAR in a box." But that approach is shortsighted. A data stewardship program that encompasses multiple regulation compliance issues is a much more strategic approach that will deliver greater value to your organization long term.

"Companies need tools that are extremely flexible," Henson says. With limited resources, they should first attack a highrisk use case like trade compliance and then expand it to other areas like General Data Protection Regulation (GDPR) controls.

"Companies have to put in tools that can take a phased approach to burn down their IT compliance risk" he says.

Final Conclusion

To conclude, the need for a simple process for marking and classifying information will continue to be important in the military environment; however, simplicity doesn't mean classification programs are static or won't benefit from deeper analytics and automation.

As military information management decision makers begin to adopt CUI and other compliance vehicles for their data classification, they need to take a strategic view of automation solutions with an eye toward flexibility. Invest in automation solutions that can evolve as their needs change and that ideally can support new levels of intelligence and context over time.

"Classification is not fixed. It continues to evolve and change," concludes Brodhead.

Defense users should take a more long-term strategic view of their data classification requirements across the regulatory landscape before investing in a single technology or tool. Afterall, an effective automated classification program takes deep user engagement to be truly effective. It's a journey, not a race.

Learn More

To learn more, access Titus's military classification solution for NATO security compliance solutions brief, visit Titus' ITAR compliance web page, read CUI compliance tips from Titus' blog or download the company's CUI white paper.

ABOUT TITUS FOR MILITARY

Titus Classification for Military easily integrates into defense environments to immediately enforce compliance to information protection policies. The solution provides an unobtrusive method for user-driven classification as well as machine learning detection capabilities to streamline workflows while educating end users.

Titus Classification for Military is a marking and information protection suite of tools for Microsoft Office (Word, Excel, PowerPoint) and Microsoft Outlook. The solution helps organizations:

— Comply with military marking standards
— Protect PII & other sensitive information
— Automates handling instructions
— Confidently share information within the mission environment

titus
by HelpSystems
www.titus.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.