FORTRA

GUIDE (Boldon James)

Protecting Government Classified Information

A Boldon James Whitepaper on Government Classification and Protective Marking Systems

Including

- Protective marking and other government classification schemes
- Why use protective markings?
- What systems do different countries use to mark or classify data
- Conducting business in a secure and effective way
- Providing deeper visibility and control of critical data
- Triggering action when data is at risk

Executive Summary

Big data, data governance, data management and securing sensitive data – these are everyday challenges for government organisations around the world, as well as making sure that sensitive data has the right security labelling applied. In this whitepaper we will explore how classification and protective marking schemes are helping government organisations better secure data. We will delve into different country classification and protective marking schemes, what these are and the type of information that requires this treatment as well as the importance of appropriate data categorisation, classification, and security labelling.

With government sensitive data it is paramount that organisations ensure the right people have access to the right data and in this whitepaper we will explore how Boldon James data classification solution provides organisations with just that - an effective data security programme – so that they remain secure, compliant and in control.

Overview

Serious data breaches and incidents of cyber-disruption have a powerful effect on driving regulatory change and activity. Governments have always had secrets. But keeping secrets secret, and private information private, is proving a challenge for the public sector, and government organisations have not been immune from large-scale incidents resulting in the exposure of millions of data records. For example, recently there have been the attacks on the Australian Government which have led to substantial publicity and debate around who the culprits are behind the cyberattacks.

In another incident, researchers discovered that Jailcore, a provider of prison services in the US, was leaking data related to 20,000 prison inmates. Likewise, private biometric company Suprema, which supplies organisations including London's Metropolitan Police, exposed a database that included more than one million fingerprints, usernames, passwords, and facial recognition data. And in August 2020 the details of more than 18,000 people who tested positive for coronavirus were published online by mistake by Public Health Wales. The health body said the data of 18,105 Welsh residents was viewable online for 20 hours on 30 August.

According to the Verizon Data Breach report, the public sector struggles with mis-delivery – sending sensitive information to the wrong recipients – and misconfiguration, when someone puts data in the cloud without the proper security measures in place. Of the breaches that do occur, just over half (51 percent) of data compromised in public sector data breaches documented by Verizon involved personal information.

Verizon also found that espionage was the key driver for government data breaches, with public sector cyber attacks making up 66% of all incidents. This is one of the reasons that protective markings or official classifications are so important.

1. Protective Marking And Other Government Classification Schemes

Government protective markings or classification systems are designed to help individuals determine, and indicate to others, the levels of protection required to help prevent the compromise of valuable or sensitive assets. The markings signal quickly and unambiguously, the value of an asset and the level of protection it needs.

Why Use Protective Markings?

Protective markings are security labels assigned to public sector information. They signify the confidentiality requirements of public sector information, usually determined via an information security value assessment or security framework or policy. Protective markings inform the minimum level of protection to be provided throughout the information lifecycle, including during its use, storage, transmission or transfer and disposal.

What information requires such markings?

Any public sector information (including personal information) obtained, generated, received, or held by or for a public sector organisation for an official purpose or supporting official activities. This includes both hard and soft copy information, regardless of media or format. However, not all public sector information requires a protective marking. That said, other security measures may still be required to protect the integrity and availability of this material.

Unofficial Or Unclassified Information

In contrast, unofficial or unclassified information - which is any information that has no relation to official activities, such as personal correspondence - does not need to undergo a security value assessment. This type of information has no bearing on official functions and, as such, need not have a protective marking applied to it. Whilst 'unofficial' or 'unclassified' are not recognised as a formal protective marking, they are used for email marking purposes in some organisations' email systems.

That said, it is useful to mark an unofficial or unclassified document in some way, so that the recipient of the document knows that the author has considered the content and made a choice of classification. An unclassified document should be treated as 'unknown'.

2. What Systems Do Different Countries Use To Mark Or Classify Data

2.1 UK Government Security Classifications Policy

Classified information in the UK is a system used to protect information from intentional or inadvertent release to unauthorised readers. The system is organised by the Cabinet Office and is implemented throughout central and local government and critical national infrastructure. The system is also used by private sector bodies that provide services to the public sector.

The current classification system, the Government Security Classifications Policy, replaced the old Government Protective Marking Scheme in 2014. Since classifications can last for 100 years many documents written using the old scheme still exist and need protection.

Classifications must be capitalised and centrally noted at the top and bottom of each document page, except at OFFICIAL, where the document marking is optional. All material produced by a public body in the UK must be presumed to be OFFICIAL unless it is otherwise marked. Like the Protective Marking Scheme which it superseded, the GSCP classifications are applied only to the confidentiality of the data under classification.

TOP SECRET

Information marked as TOP SECRET is that whose release is liable to cause considerable loss of life, international diplomatic incidents, or severely impact ongoing intelligence operations. Disclosure of such information is assumed to be above the threshold for Official Secrets Act prosecution.

SECRET

This marking is used for information which needs protection against serious threats, and which could cause serious harm if compromised - such as threats to life, compromising major crime investigations, or harming international relations.

OFFICIAL

All routine public sector business, operations and services is treated as OFFICIAL. Many departments and agencies operate exclusively at this level.

The older protective marking scheme used five levels of classification, supplemented with caveat keywords. In descending order of secrecy, these were: Top Secret, Secret, Confidential, Restricted and Protect. The terms "UNCLASSIFIED" or "NOT PROTECTIVELY MARKED" were also used to indicate positively that a protective marking is not needed. Documents classified under the protective marking scheme still exist and need correct handling.

2.2 The US Classification System

The United States Government classifies information according to the degree in which the unauthorised disclosure would damage national security. Like many other countries the US has three classification levels. From the highest to the lowest level these are:

- Top Secret
- Secret
- Confidential

Government documents that do not have a classification can be marked as Unclassified.

2.3 The French Classification System

In France, classified information is defined by the Penal Code. The three levels of military classification are:

- Très Secret Défense (Very Secret Defence): Information deemed extremely harmful to national defence, and relative to governmental priorities in national defence.
- Secret Défense (Secret Defence): Information deemed very harmful to national defence. Such information cannot be reproduced without authorisation from the emitting authority, except in exceptional emergencies.
- Confidentiel Défense (Confidential Defence): Information deemed potentially harmful to national defence, or that could lead to uncovering some information classified at a higher level of security.

Less sensitive information is “protected”.

2.4 German Classification System

Similar to other countries the German classification system has four levels, which correspond to those used in the countries already mentioned:

- STRENG GEHEIM which is equivalent to Top Secret
- GEHEIM which is equivalent to Secret
- VS-VERTRAULICH which is equivalent to Confidential
- VS-NUR FÜR DEN DIENSTGEBRAUCH which is equivalent to Restricted.

Less sensitive information is “protected”.

3. Conducting Business In A Secure And Effective Way

Consistent use of protective markings or classifications, coupled with the adoption of appropriate security measures, enhances government’s ability to conduct business in a secure and effective manner. Classifications/ protective markings act as an important visual signal to anyone accessing or using the material, informing the minimum security obligations that need to accompany public sector information. They offer an easily identifiable way for information users (visually) and for systems (such as an entity’s email gateway) to identify and manage the handling and control of information at different levels.

It is essential that government organisations have the right solutions in place so that users can immediately understand how to appropriately classify a document. It is important that the organisation can effectively manage data, streamline operations and proactively respond to regulatory change.

Providing Deeper Visibility And Control Of Critical Data

In any data protection strategy, content scanning capabilities are critical to reducing the likelihood of a data loss incident and maintaining regulatory compliance. Harnessed through a data loss prevention (DLP) solution, content scanning has the greatest impact when combined with predictable, meaningful metadata that provide classification and labelling of data.

Integrated with Boldon James Classifier, DLP combines user-driven and automated classification with powerful data protection and governance capabilities to streamline data handling that enables deeper visibility and control of critical data. Boldon James multi-level classification solution, Classifier, includes levels for both the sensitivity of a document, as well as any caveats which then limit the distribution of a document to the appropriate degree.

Classification tools with the right blend of automated and user-applied classification support can significantly increase end-user awareness when handling data. Boldon James Classifier protects a document by adding metadata labels as well as visual markings. These metadata labels and visual markings reflect the classification given to the document. The visual markings are customisable and include headers, footers, watermarks, and title pages.

Having a comprehensive granular classification system is important to ensure the correct level of classification is assigned to a document but this can often be confusing for the user who is expected to correctly select the right classification. Boldon James Classifier structured Q&A asks the user a series of questions to help them classify the document correctly. The user does not need to remember exactly what the marking is as they are reminded when classifying the document. This is particularly useful when the system is first installed as it helps to teach users to select the correct level of classification. Once a user is familiar with the classification policy, they can select the classification level straight off the office ribbon, or even save it as a "favourite".

Likewise, Boldon James Classifier supports other kinds of markers through the metadata attached to every document. This metadata drives all policy associated with the document including sharing, emailing, or printing of the document. The result is enhanced user engagement and accountability, improved security awareness, and a reduction of data security risk across the organisation.

Triggering Action When Data Is At Risk

Classifying information is the vital first step, but due to the dynamic nature of data and growing volume of digital documents, relying solely on knowledge workers to carry the full burden of data handling practices may not be realistic or sufficient. Combined with automation, such as Data Loss Prevention (DLP) technologies, organisations can identify critical data as it moves throughout the business and trigger an action if or when data is at risk. For example, let's assume a user accesses an official document. The user copies/pastes a paragraph of text into a new Word document and attempts to save it to a USB storage device. With a DLP solution, an alert is triggered and an official label is automatically applied to the newly created document. This automated response reduces the risk of human error to ensure critical data is protected without obstructing user productivity. This enhanced and automated data protection and governance of data flows across the organisation is an elegant and effective solution to the demands of data security and regulatory compliance.

Conclusion

Regardless of any compliance obligations government organisations face, it is good security practice for them to implement and enforce data classification systems to reduce the risk of inadvertent or intentional data loss.

That said, data classification is a complex process and not for the faint-hearted. But if government organisations work with the right provider who can take the complexity out through flexible, fit-for-purpose software with businesscentric labelling that provides meaningful and easy choices for the user, then this will keep the organisation secure, compliant and in control. Above all, we recognise how important it is that people are at the heart of any decisionmaking process, assisted by automation. The combination of Boldon James data classification solutions with DLP technologies provides organisations with just that - an effective data security programme, with the ability to make those human-assisted decisions.

Addendum

How government classification markings differ from country to country.

Country	Top Secret	Secret	Confidential	Restricted
Australia	Top Secret	Secret	Confidential	Protected
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Belgium	Zeer Geheim / Très Secret	Geheim / Secret	Vertrouwelijk / Confidentiel	Beperkte Verspreiding / Diffusion restreinte
Croatia	Vrlo tajno	Tajno	Povjerljivo	Ograničeno
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst Hemmeligt (YHM)	Hemmeligt (HEM)	Fortroligt (FTR)	Til Tjenestebrug (TTJ) Foreign Service: Fortroligt (thin Black border)
European Union (EU)	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
European Union (Western) (WEU)	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Finland	Erittäin salainen (ST I)	Salainen (ST II)	Luottamuksellinen (ST III)	Käyttö rajoitettu (ST IV)
France	Très secret défense	Secret défense	Confidentiel défense	Diffusion restreinte
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	VS-NUR FÜR DEN DIENSTGEBRAUCH
Hungary	Szigorúan Titkos	Titkos	Bizalmas	Korlátozott Terjesztésű
Iceland	Algert Leyndarmál	Leyndarmál	Trúnaðarmál	Þjónustuskjal
Ireland (Irish language)	An-sicreideach	Sicreideach	Runda	Srianta
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Netherlands	STG. Zeer Geheim	STG. Geheim	STG. Confidentieel	Departementaal Vertrouwelijk
New Zealand	Top Secret	Secret	Confidential	Restricted
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
Poland	Ściśle tajne	Tajne	Poufne	Zastrzeżone

Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Slovak Republic	Prísne tajné	Tajné	Dôverné	Vyhradené
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Spain	Secreto	Reservado	Confidencial	Difusión Limitada
Sweden	Kvalificerat Hemlig (KH); Hemlig/Top Secret (H/TS)	Hemlig (H); Hemlig/ Secret (H/S)	Hemlig/Confidential (H/C)	Hemlig/Restricted (H/R)
Switzerland		GEHEIM / SECRET	VERTRAULICH / CONFIDENTIEL	INTERN / INTERNE
Turkey	Çok Gizli	Gizli	Özel	Hizmete Özel
United Kingdom	TOP SECRET	SECRET	OFFICIAL-SENSITIVE (formerly CONFIDENTIAL)	OFFICIAL (formerly RESTRICTED)
United States	Top Secret	Secret	Confidential	no direct equivalent