FORTRA

GUIDE (Boldon James)

Protecting Government Classified Information

A Boldon James Whitepaper on the Australian Protective Marking Scheme

Including

- The Australian Protective Security Policy Framework
- What are Protective Markings?
- Conducting business in a secure and effective way
- Ensuring new updates to the Standard are met
- Triggering action when data is at risk

Executive Summary

Data security has never been as high on the agenda for the Australian Government at both a Federal and State level. Big data, data governance, data management, securing sensitive data and ensuring sensitive data has the correct security labelling applied are all everyday challenges to be addressed.

In this whitepaper, we will explore how the Australian Protective Security Policy Framework is helping government agencies. We will look at Protective Markings, the type of information that requires Protective Markings, as well as the importance of appropriate data categorisation, classification and security labelling.

With sensitive data in government, organisations must ensure the right people have access to the right data. In this whitepaper, we will explore how Boldon James data classification solutions provide Federal and State government departments with just that - an effective data security programme – so that they remain secure, compliant, and in control.

Overview

Data breaches and cyber-attacks can be hugely disruptive and profoundly influence regulatory change and activity. Australia has seen what feels like an ever-increasing number of such attacks. As recently as September 2022, one of Australia's largest telecoms company was targeted. The data of up to 10 million customers, including home addresses, drivers' licenses and passport numbers, was compromised.

On other occasions, government departments themselves have been targeted. In July 2020, the then Prime Minister, Scott Morrison, announced that $1.35 billion in existing defence funding would be spent over the next decade to boost the cybersecurity capabilities of the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC). The Federal Government said it would create more than 500 new jobs in its cyber intelligence agency as part of what it said was Australia's largest cybersecurity investment.

1. The Australian Protective Security Policy Framework

In 2010, the Australian Government implemented its Protective Security Policy Framework (PSPF)i, which was developed to assist government agencies in protecting their people, information, and assets. The PSPF articulates government protective security policy. It also guides entities to support the effective implementation of the policy across the areas of security governance, personnel security, physical security, and information security.

One of the mandatory requirements of PSPF states, 'Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.

In October 2018, the Government updated the PSPF and gave agencies one year to adopt the new Protective Marking scheme. It was updated further in 2022, and agencies that do not adopt the mandatory requirements and put in the appropriate data protection controls can be prevented from transacting with federal organisations.
To appropriately guard against information compromise, entities must consider:

- Confidentiality – who should be able to see the information and why?
- Integrity – assurance that information is only being created, amended or deleted by the intended, authorised means and is correct and valid.
- Availability – ensuring authorised persons have access to information when and as needed.

What Are 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. 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.

[i] Details on the Australian Protective marking Scheme can be found here:
https://www.cyber.gov.au/acsc/view-all-content/referral-organisations/protective- security-policy-framework

What Information Requires Protective 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 necessary to protect the integrity and availability of this material.

Unofficial Information

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

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

The Email Protective Marking Standard

With the rapid growth of email, especially for inter-agency communications within the Australian government, a strong security case was made for a standardised and readable marking scheme for email. To meet this need, the Email Protective Marking Standard (EPMS) was created as part of the Protective Security Policy Framework (PSPF).

The Australian EPMS has since been updated several times, with incremental updates to the marking standards.

2. Conducting Business In A Secure And Effective Way

Consistent use of Protective Markings and adopting appropriate security measures enhance the government's ability to conduct business securely and effectively.

Protective Markings act as an important visual signal to anyone accessing or using the material, informing the minimum security obligations that must accompany public sector information.

> ‘Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.'

Protective Markings offer an easily identifiable way for information users (visually) and systems (such as an entity's email gateway) to identify and manage the handling and control of information at different levels. More detail on each of these is outlined in Figure 1.

Information Management Markers (IMMs)

Information Management Markers (IMMs) have been designed to reflect 'rights properties' for certain content and can inform access restrictions. While IMMs are not mandatory, they are metadata indicators that provide a standard set of terms ensuring common understanding and consistency where access or disclosure of information is to be limited as:

- disclosure of the material is limited or prohibited by legislation,
- special handling of the material is required; and,
- dissemination of the material needs to be controlled.

Depending on the content, some information may require multiple IMMs. In these instances, organisations using IMMs should apply each required marker as appropriate.

Figure 1 – Different Levels of Protective Marking[ii]

Protective Marking	Basis For Protective Marking
BIL 1 OFFICIAL	This protective marking may be applied to public sector information that requires some form of protection, as any compromise of this information may cause **minor** harm/damage to government operations, organisations and/or individuals. This protective marking signals that the material has undergone an information assessment and visually describes its security value to the end user. However, it is recognised that the application of this protective marking **(OFFICIAL)** may not always be appropriate and, as such, does not need to be mandatorily applied.
BIL 2 OFFICIAL: Sensitive	Apply to public sector information where secrecy provisions or enactments apply to the content or where disclosure of the material may be **limited** or prohibited under legislation. This indicates where compromise of the confidentiality of the information may cause **limited** harm/damage to government operations, organisations and/or individuals.
BIL 3 PROTECTED	Apply to public sector information where compromise of the confidentiality of the information may cause **major** harm/damage to government operations, organisations and/or individuals.
BIL 4 SECRET	Apply to public sector information where compromise of the confidentiality of the information may cause **serious** harm/damage to government operations, organisations and/or individuals.
CABINET-IN-CONFIDENCE	To be applied to Cabinet information, based on exemptions under the Freedom of Information Act 1982. A document is described as 'Cabinet-In-Confidence' if it is: • An official record of any deliberation or decision of the Cabinet. • A document that has been prepared by a Minister or on their behalf or by an agency for the purpose of submission for consideration by Cabinet. • A document prepared for the purpose of briefing a Minister in relation to issues to be considered by Cabinet. • A document that is a draft of, or contains extracts from a document referred to above. • A document which refers to any deliberation or decision of Cabinet, other than a document by which a decision of Cabinet was officially published. The marking of 'Cabinet-In-Confidence' must be used in conjunction with a security classification of either PROTECTED or SECRET.

The security classification of **TOP SECRET** is not referenced as an available Protective Marking for use. If an organisation assesses its material as requiring a security classification of TOP SECRET, it would usually seek guidance from the PSPF on managing this material.

[ii] Figure 1 extract from The Office of the Victorian Information Commissioner (OVIC) Practitioner Guide on Protective Markings : https://ovic.vic.gov.au

Caveats

Caveats indicate that public sector information has special requirements in addition to those identified by a protective marking, further restricting access to the material. Caveats cannot be applied to 'Unofficial' material. There are different levels of caveats that can be applied, but typically these are:

- **Commonwealth** – most found on information relating to material that could impact the national interest (Inc. national security). Caveats at a Commonwealth level must be used in conjunction with a security classification.
- **Specific to a government** – these are authorised caveats to be used with a government only and must be used in conjunction with a security classification.
- **Organisation/agency specific** – these are for internal application and use only. They should be removed from the information before transfer or transmission outside the organisation.

3. Ensuring New Updates to the Standard are Met

With new updates coming into the scheme regularly, Government agencies must have the right solutions in place. It is essential, therefore, 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. Content scanning has the most significant impact when combined with predictable, meaningful metadata that provides classification and labelling of data.

Boldon James' multi-level classification solution includes levels for both the sensitivity of a document, as described in this paper, as well as all the caveats outlined above, which then limits the distribution of a document to the appropriate degree.

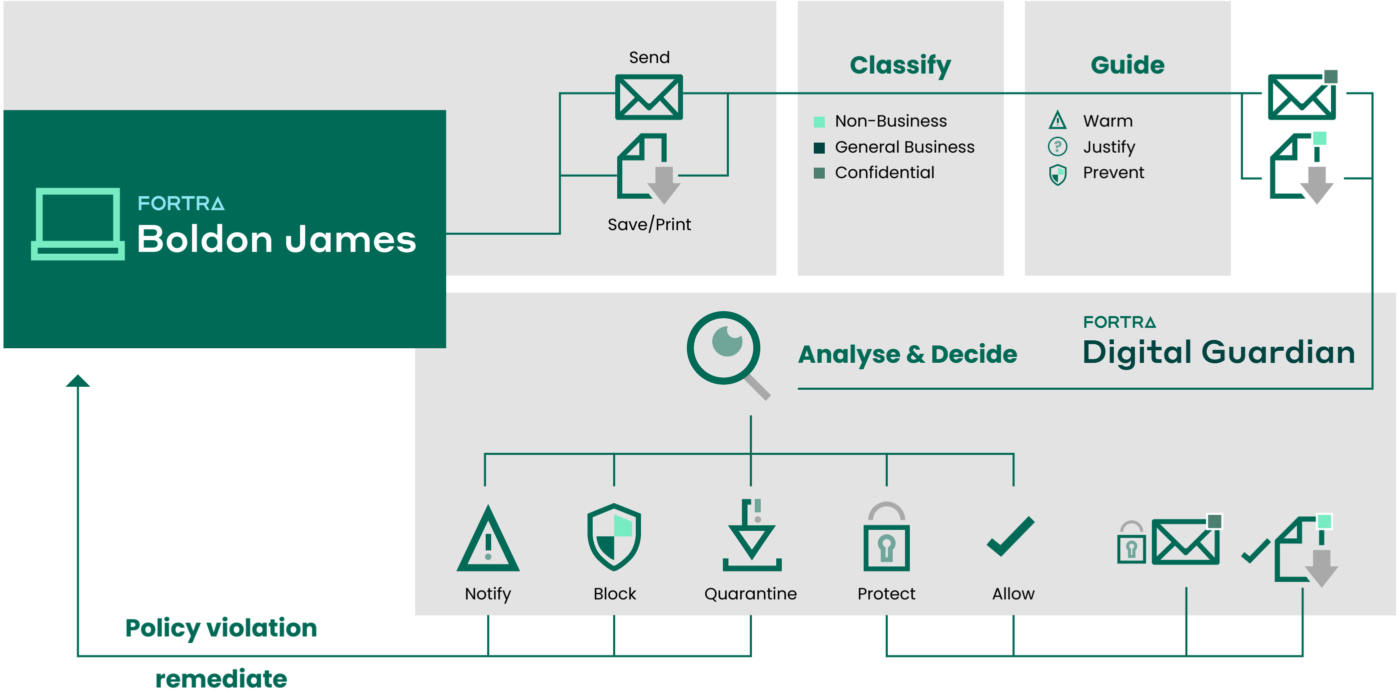
$1.35 billion in existing defence funding is to be spent over the next decade to boost the cybersecurity capabilities of the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC)

Classification tools with the right blend of automated and user-applied classification support can significantly increase end-user awareness when handling data. Boldon James protects a document by adding "hidden" metadata labels to the document 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 granular classification system is important to ensure the correct level of classification is assigned to a document but can be confusing for the user who is expected to select the right classification correctly. Boldon James' 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 'Official Sensitive' 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 classification level. Once a user is familiar with the classification policy, they can choose the classification level straight off the office ribbon or save it as a "favourite."

Likewise, Boldon James supports multiple Information Management Markers through the metadata attached to every document. This metadata drives all policies associated with the document, including sharing, emailing, or printing of the document.

The result is enhanced user engagement and accountability, improved security awareness, and reduced data security risk across the organisation.



Conclusion

In this whitepaper, we have referenced specifics according to the State of Victoria and how it adheres to the PSPF with its protective markings. However, other states are aligned with this, including New South Wales (NSW), Queensland (QLD) and South Australia. All these are states with very similar protective marking classification in place, as does Federal Government.

Regardless of any compliance obligations Australian agencies face, it is good security practice for them to implement and enforce data classification systems to reduce the risk of accidental or intentional data loss. Keeping government departments protected against data breaches is a true challenge, and data classification is a complex process and not for the faint-hearted. But suppose government agencies work with the right provider who can take the complexity out through flexible, fit-for-purpose software with business-centric labelling that provides meaningful and easy choices for the user.. In that case, this will keep the organisation secure, compliant, and in control.

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.