Australian Government

Information Management Office

# Email Protective Marking Standard Implementation Guide for the Australian Government

May 2012 (V2012.1)

## Disclaimer

The Department of Finance and Deregulation (Finance) has prepared this document to provide guidance for agencies on implementation of the *Email Protective Marking Standard* (v2012-2).

This document and the information contained herein are provided on an "as is" basis and the contributors and the organisations they represent and are sponsored by disclaim all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.



**COMPLIANCE WITH THE PSPF AND THE ISM**

The *Email Protective Marking Standard Implementation Guide for the Australian Government (Version 2012-1* May 2012) has been developed to assist agencies in implementing email protective markings in accordance with the *Email Protective Marking Standard (version 2012-2, April 2012)*.

This document provides guidance for agencies on the implementation of the new email protective marking requirements of the *Australian Government Protective Security Policy Framework* (PSPF).

The *Australian Government Information Security Manual* (ISM), issued by DSD, stipulates that agencies must comply with the *Email Protective Marking Standard*.

## Contents

## INTRODUCTION

Email communications are a widely used and accepted form of communication by and within the Australian Government. As such, they provide evidence of the conduct of government business and are important information assets.

Government communications, including emails, must be controlled by standardised business processes and contained within information management regimes that protect the interests of citizens and the Australian Government.

The *Australian Government Protective Security Policy Framework* (PSPF) states that 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. (Mandatory Requirement: **INFOSEC 3**). The *Australian Government Information Security Manual* (ISM) further specifies that agencies must ensure that all official emails are marked with a protective marking that identifies the maximum classification and protection requirements for that information.

This document provides guidance for agencies on implementation of the new protective markings (which include Dissemination Limiting Markers) for email. It is important that implementation of the new protective markings is completed in a coordinated and consistent manner across government. This Implementation Guide should be read in conjunction with the PSPF, the ISM and the *Email Protective Marking Standard for the Australian Government (v2012.2).*

There are a range of issues that agencies will be required to address in relation to implementation of the Email Protective Marking Standard. Some of these are agency specific (such as training and awareness), others impact implementation of the Standard across Government. While people issues are internal to each agency, shared understandings and interpretations are important from the perspective of a consistent application of the new marking requirements across agencies.

The most significant factors in achieving a smooth transition to the new marking system are good communication and transparency. While agencies will use different email vendors and operate with different Gateway providers it is essential that open lines of communication exist to identify and resolve issues as they emerge. Implementing a Standard in a uniform and consistent manner across all agencies should generate efficiencies and therefore cost savings.

It will be important for agency staff directly involved in implementing the Standard to be aware of and participate in relevant forums to identify and resolve issues that may arise in the implementation phase.

To facilitate improved communication the following have been established:

- The Standard for email protective markings is published on the Finance website.
- Both the Defence Signals Directorate (through OnSecure) and AGIMO (through GovDex) have established forums whereby agency security personnel can exchange ideas and discuss issues in an open yet secure manner.
    - In addition, AGD can provide advice on the implementation of the PSPF. Enquiries should be sent to PSPF@ag.gov.au

The recommendations contained in this Implementation Guide are designed to achieve a consistent outcome across government.

## PROTECTIVE MARKINGS

When information (including an email) is created, the originator is required to assess the consequences of damage from unauthorised use or compromise of the information. If adverse consequences could occur or the agency is legally required to protect the information **it is to be given a protective marking.**

Further information on protectively marking and handling sensitive and security classified information can be found at: http://www.protectivesecurity.gov.au/informationsecurity/Pages/Supporting-guidelines-to-information-security-(including-the-classification-system).aspx

Official information not needing a protective marking may be marked UNCLASSIFIED.

Information needing increased protection is to be either security classified (identified by a security classification showing the level and protection required), assigned a Dissemination Limiting Marker (DLM) (based on the sensitivity of the information) or, when appropriate, marked with a caveat.

The PSPF identifies three types of protective markings:

- Security Classifications
- Dissemination Limiting Markers (DLMs), and
- Caveats.

Emails are to be marked:

- UNOFFICIAL[1]
- UNCLASSIFIED[2]
- PROTECTED
- CONFIDENTIAL
- SECRET
- TOP-SECRET

or with a DLM. DLMs are markings to be applied to emails where disclosure of the content of the email (including attachments) may be limited or prohibited by legislation, or where it may otherwise require special handling. The DLMs are:

- For-Official-Use-Only (used on UNCLASSIFIED information only)
- Sensitive
- Sensitive:Legal
- Sensitive:Personal
- Sensitive:Cabinet[3]

[1] UNOFFICIAL is not a security classification marking in the *Australian Government security classification system*. It is included in this standard to allow those agencies that choose to use it a way of distinguishing non work-related email on their systems.

[2] UNCLASSIFIED is not a security classification in the *Australian Government security classification system*. It is included in this standard in order to allow agencies to recognise work-related emails that do not carry a security classification or other marking.

[3] This DLM can only be applied to security classified information.

## Dissemination Limiting Markers

Dissemination Limiting Markers (DLMs) are explained in the Information Security Management Guidelines— Australian Government Security Classification System.

The PSPF requires each agency to determine the appropriate protective markings—including DLMs—on its documents based on its own unique risk profile. As emphasised in the PSPF, the impact of compromise should be the deciding factor when applying protective markings.

Agencies, at their discretion, may choose to apply protective markings requiring a higher level of control where it is determined that information is of a highly sensitive nature—for example commercial or personal information.

Indicative guidance to the mapping of old Security Classifications and the new DLMs is at Attachment 1.

**NOTE**: There is a difference in formatting of the DLMs and the security classification TOP SECRET in hard copy and in header information in an email. In email header information, software requirements mean there is no space after the colon for the Sensitive markings, and in TOP SECRET and For Official Use Only, a hyphen must be placed between each separate word in the marking.

Agencies MUST make their own determination regarding the mapping of old to new.

NOTE : Any use of the DLM 'Sensitive: Cabinet' MUST be accompanied by a protective marking of at least PROTECTED.

## Caveats

Certain security classified information, most notably some national security classified information, may bear a security caveat in addition to a security classification. The caveat is a warning that the information has special requirements in addition to those indicated by the protective marking.

Caveats are not classifications in their own right and are not to appear without the appropriate security classification marking.

The following categories of security caveat are used:

- codewords
- source codewords
- Eyes Only
- Australian Government Access only
- Releasable to
- special handling caveats, and
- Accountable Material.

# IMPLEMENTATION ISSUES

## IMPLEMENTING PROTECTIVE MARKINGS

The standard provides two ways of implementing protective markings, either in the:

- Subject Field Marking, or in the
- Internet Message Header Extension.

Email filter systems must be capable of managing markings that appear in either location. The standard recommends that:

*The Internet Message Header Extension SHOULD be used in preference to the Subject Field Marking.*

Agencies have flexibility to place markings in either the Subject Field or the Message Header Extension. Email filter systems must be capable of accommodating markings in both locations.

To offset the risk that an email reader does not see the marking in the Message Header Extension agencies should consider placing the marking in both locations.

**RECOMMENDATION**

Agencies SHOULD place markings in BOTH the Subject Field AND Message Header Extension.

## CHANGEOVER

Any email created after **31 July 2012** SHOULD be classified using the new Australian Government security classification system.

From **1 August 2013** agencies MUST (unless granted dispensation) only be using the Australian Government security classification system.

Emails received from another agency after 31 July 2012 which use a superseded marking (X-IN-CONFIDENCE, RESTRICTED and HIGHLY PROTECTED), may continue in use with the old marking/s during the 12 month grandfathering period.

Therefore email marking systems MUST be able to accommodate both old and new protective markings until **31 July 2013**.

- Filters will also have to accommodate old classification on emails originating from those agencies granted dispensations until **July 2014.**

Where an agency does NOT accept an email that originated from the .gov.au Namespace that uses either an old protective marking or a protective marking higher than the classification of the agency's ICT system it SHOULD advise the sender of the email both of that fact and also that the recipient has not been advised of the original email being sent.

Agencies MUST establish (and communicate) rules in relation to the handling of emails being sent or received with a protective marking that is not approved for use on the system.

## EMAIL - INTERNET OR SECURE NETWORK?

Emails marked UNOFFICIAL may be sent across public network infrastructure, such as the Internet.

Emails marked UNCLASSIFIED with no DLM may be sent across public network infrastructure, such as the Internet if there is a specific business purpose for doing so.

DLM-marked material even where UNCLASSIFIED is **not for public release.**

However, this does not mean it cannot be sent outside the Australian Government.

Where a business purpose requires communication between government and an external entity (eg businesses, citizens) then an agency can send DLM-marked material outside government.

Agencies MUST implement appropriate security controls when sending emails across public network infrastructure such as the internet. Relevant security controls can be found in the *Cryptography* chapter of the ISM.

Agency controls for the protection of DLM-marked information SHOULD protect such information in accordance with legislative requirements under the Freedom of Information Act 1982, the Privacy Act 1988, other agency-specific legislation, or where limited damage may occur if it is compromised.

Within Government, FedLink provides an encrypted channel for sending Sensitive information and information classified up to, and including, PROTECTED.

Cabinet documents, including pre-exposure drafts, exposure drafts, drafts for coordination comments, final submissions, and coordination comments MUST be marked Sensitive:Cabinet and MUST only be circulated via the CABNET network.

More general Cabinet-related communications such as those with broad reference to Cabinet deliberations SHOULD be marked PROTECTED (as a minimum) and Sensitive: Cabinet but can be sent across other appropriately secure networks, for example, an email stating 'we need to discuss policy X in order to produce a Cabinet submission for the meeting of day X'.

Agencies SHOULD educate staff in relation to the appropriate marking and transmission of Cabinet and Cabinet-related documents.

The Cabinet Handbook contains information on classification and handling of Cabinet and Cabinet related material.

Emails marked with a higher security classification (CONFIDENTIAL, SECRET and TOP SECRET) MUST be sent across the appropriate secure network.

## USE OF UNCLASSIFIED

Official information not needing protection may be marked UNCLASSIFIED. The need to know principle is to be applied to all official information[4].

UNCLASSIFIED information is "Information that is assessed as not requiring a classification". Under the ISM, UNCLASSIFIED information with no DLM is information that an agency deems able to be publicly released.

Information needing increased protection is to be either security classified and identified by a protective marking showing the level and protection required, assigned a dissemination limiting marker (DLM) or, when appropriate, a caveat.

NOTE
Australian Government employees are to have agency authorisation to release any information to members of the public. Authorisation may be granted by the agency head or a person authorised by the agency head. When personal information is involved, any release is to comply with the Privacy Act 1988 (the Privacy Act).

UNCLASSIFIED information marked with a DLM is not for public release and requires a level of protection. Such information may be sent over the Internet where there is a business requirement such as corresponding with an external entity.

Version 2011-1 of the Standard required both a security classification at the UNCLASSIFIED level and a DLM.

Version 2012-2 of the Standard requires emails to be marked EITHER:

- UNCLASSIFIED with no DLM

Or

- only a DLM

as follows:

| | |
|---|---|
| UNCLASSIFIED | No DLM Required. |
| NO SECURITY CLASSIFICATION REQUIRED | For-Official-Use-Only |
| | Sensitive |
| | Sensitive:Legal |
| | Sensitive:Personal |

4 See: Government information security management guidelines - Australian Government security classification system (19 July 2011).

The change is because:

- The appearance of UNCLASSIFIED conflicts with the 'sensitive' DLM marking because UNCLASSIFIED is a marking associated with information that is not sensitive.
- The appearance of UNCLASSIFIED undermines staff education that the DLMs replace IN-CONFIDENCE for sensitive information (below PROTECTED).
- Staff understand IN-CONFIDENCE is higher than UNCLASSIFIED.
- The presence of UNCLASSIFIED in addition to a DLM will potentially increase the risk of security breaches related to email transmission.
- The presence of UNCLASSIFIED will potentially increase the risk of security breaches related to physical security of hardcopy information.

## AGENCY NETWORKS

Each control in the ISM has an applicability indicator that indicates the information and systems to which the control applies. The applicability indicator has up to five elements, indicating whether the control applies to:

- G: Government systems[5] containing UNCLASSIFIED but sensitive information not intended for public release, such as that marked with a DLM;
- P: PROTECTED information and systems
- C: CONFIDENTIAL information and systems
- S: SECRET information and systems
- TS: TOP SECRET information and systems.

In the ISM, UNCLASSIFIED and IN-CONFIDENCE have been removed and replaced with 'GOVERNMENT' controls as a baseline level of security for systems storing **UNCLASSIFIED but sensitive information not intended for public release**, such as DLM information.

| **Material Classified or Marked** | **Minimum Level of ICT System Accreditation** |
|---|---|
| TOP SECRET material (includes TOP SECRET classified material also marked with a Sensitive DLM) | TOP SECRET only |
| SECRET material (includes SECRET classified material also marked with a Sensitive DLM) | SECRET or above |
| CONFIDENTIAL (includes CONFIDENTIAL classified material also marked with a Sensitive DLM) | SECRET or above |

5 Note 'Government' is not a security classification under the Australian Government Security Classification System

| | |
|---|---|
| PROTECTED (includes Sensitive: Cabinet and other PROTECTED classified material also marked with a Sensitive DLM) | PROTECTED or above |
| UNCLASSIFIED (includes FOUO/ unclassified material marked with a Sensitive DLM, except Sensitive: Cabinet) | UNCLASSIFIED (DLM) ICT systems / Government system ISM controls or above |
| UNCLASSIFIED (includes official material prepared for public distribution, and official material not otherwise qualifying for protective marking.) | UNCLASSIFIED ICT systems and above |

## COALITION PARTNER ALIGNMENT

This represents a special case for a sub-set of agencies that have regular engagements with governments outside Australia who may (or may not) have their own email marking requirements.

**Recommendation**

Coalition partner requirements SHOULD not take precedence over Australian Government requirements.

## SYSTEM GENERATED EMAILS

Identification and configuration of system generated emails will be a significant activity.

- For example out of office replies which are automatically generated will require appropriate marking.

**Recommendation**

Agencies should choose a marking appropriate to the content of the automated response email, including history where relevant.

Where a system generated email includes or attaches the history of sent/received emails then the automated email MUST carry the same classification and marking as the highest classified email in the history.

Agencies may choose to not send system generated emails at levels of classification above PROTECTED

## MULTIPLE DLMs

The 2011-1 version of the Standard specifies one DLM per email (the same as the current X-IN-CONFIDENCE regime).

Version 2012-2 of the Standard will allow more than one DLM to accommodate scenarios where an email may include for example information that satisfies the requirements of both Sensitive:Legal and Sensitive:Personal.

**Recommendation**

The current specification in the Email Protective Marking Standard is to be retained – a single Protective Marking and/or a single DLM in the Subject Field and the Message Header Extension.

If business requirements mandate a second DLM then this MUST be placed by the email writer in the body of the email and a reason provided for its inclusion.

Additional DLMs are for handling guidance only.

DLM treatment/usage rules SHOULD be consistent across agencies.

Agencies SHOULD use the 'Government' ISM controls for transmitting Unclassified but not for public release (i.e. DLM) material.

## POSITION OF THE PROTECTIVE MARKING

Agencies SHOULD position the Protective Marking at the end of the Subject Field.

Agencies SHOULD, where possible, implement mitigation strategies to minimise the risk of the Protective Marking being truncated from the end of the subject line

Implementing this recommendation comes with a risk that the Protective Marking will truncate if the subject line is too long. This risk is considered low, however, agencies are encouraged to implement strategies to mitigate this risk if appropriate and where possible.

The issue to be addressed by agencies becomes one of a balance between useability and efficient information management (sorting by Subject) and security (risk of truncation).

In considering the placement of the protective marking agencies should consider:

- the risk of the truncating the protective marking if it is placed at the end of the subject line;
- the key purpose of the email subject field to describe the main subject of the email as this facilitates effective and efficient browsing, sorting, retrieval and viewing of emails over time.
- systems which capture and manage emails as records usually automatically capture the email subject field as the record title.
- retrieving multiple email titles commencing with the same security classification data is not efficient and will impede location and retrieval of emails required for business or legal discovery purposes.

- it will also compromise reuse and publication of information as required by the Office of the Australian Information Commissioner.
- emails of ongoing significance to Australia will be transferred in digital form, with their metadata, to the National Archives of Australia. The email subject line is important to facilitate access to the emails.

## 3 LETTER COUNTRY CODES

The 2011-1 version of the Email Protective Marking Standard specified the use of 2 letter Country Codes.

Version 2012-2 of the Standard requires agencies to use 3 letter country codes (ISO 3166-1 Alpha-3).

The rationale for the change is to ensure consistency with international developments.

**Recommendation**

Agencies SHALL use 3 letter country codes (ISO 3166-1 Alpha-3).

## CONSULTATION WITH EMAIL VENDORS AND GATEWAY PROVIDERS

The manner in which agencies implement the new marking regime will require the engagement of email vendors and Gateway providers.

**Recommendation**

Subject to any security considerations, Agencies SHOULD share internal policies and procedures with email vendors and Gateway providers to ensure implementation of a practical marking regime.

## ATTACHMENT 1

**Indicative Guidance**

Note: The following indicative mappings provide possible examples of how agencies might apply markings under the PSPF to previously classified information (X-IN-CONFIDENCE). However, the mapping process will vary from agency to agency based on the relevant risk assessments. For example, an agency might generally mark a current COMMERCIAL –IN-CONFIDENCE document For Official Use Only (FOUO), while classifying its more sensitive commercial information PROTECTED.

FOUO may be the appropriate DLM to replace the following superseded security classifications:

AUDIT-IN-CONFIDENCE

CLIENT-IN-CONFIDENCE

LEGAL-IN-CONFIDENCE

PERSONNEL-IN-CONFIDENCE

SECURITY-IN-CONFIDENCE

STAFF-IN-CONFIDENCE

However, depending on the content, and context, one of the Sensitive DLMs markings such as 'Sensitive: Personal' might be applicable, for example, with regard to MEDICAL-IN-CONFIDENCE.

When agencies apply a DLM of 'Sensitive', they are to include in the body of the email, information that identifies the reason for the Sensitive marking and the handling requirements for the document as a result of the marking. For example:

<Reason for marking, e.g. This document may contain 'protected information' as defined under the Social Security Act 1991.

This document is to be handled……..>