Australian Government

Information Management Office

Email Protective Marking Standard for the Australian Government

Australian Government

Information Management Office

| AUGUST 2012 (VERSION 2012.3)

Disclaimer

This document has been prepared by the Department of Finance and Deregulation (Finance) in consultation with industry and other agencies, including the Attorney-General's Department and the Defence Signals Directorate (DSD) to provide information to government bodies in relation to the use of email within the Australian Government.

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.

ISBN 978-1-922096-05-0 online

COMPLIANCE WITH THE PSPF AND THE ISM

The *Email Protective Marking Standard for the Australian Government Version 2012.3* (August 2012) has been developed to assist agencies implement email protective markings. Compliance with this document will assist agencies manage and protect Australian Government information in accordance with the protective marking requirements of the *Australian Government Protective Security Policy Framework* (PSPF) and the *Australian Government Information Security Manual* (ISM).

The ISM, issued by DSD, stipulates that agencies must comply with this Standard.

Abstract

This Standard defines the format of protective markings for Internet email message headers used for messages exchanged within and between Australian Government agencies. A protective marking conveys the protection requirements for information in a message, as defined within the *Australian Government Protective Security Policy Framework*. The protective marking may also contain additional information about the message that tells systems and system users how to appropriately disseminate the information contained in the message.

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 [PDF 830 KB]

Summary

Attribute	Subject Line (count)	Internet Message Header Extension (count)	Content format	Defined	Basis / Reference
VER	0	1	Fixed	2.11.13	This Standard
NS	0	1	Fixed	2.11.12	PSPF
SEC	0..1	0..1	Fixed set	2.11.4	PSPF, MTEE, This Standard
DLM	0..1	0..1	Fixed set	0	PSPF
CAVEAT	0..n	0..n	Fixed set & free text	2.11.6	PSPF, MTEE
EXPIRES	0..1	0..1	Fixed format	2.11.7	PSPF
DOWNTO			Fixed set		
NOTE	0	0..1	Free text	2.11.10	PSPF
ORIGIN	0	1	Fixed format	2.11.11	PSPF

Contents

1. Introduction

Official information generated by the Australian Government must be protected from unauthorised disclosure. Protective security requirements for the Australian Government are detailed in the *Protective Security Policy Framework* (PSPF). Within the PSPF, the *Australian Government Information Security Management Protocol* [1] describes how official information is to be protected. The *Australian Government security classification system* [2] gives guidance in identifying and grading the confidentiality requirements of official information, including when and how to apply a protective marking so that all those who handle it can apply the correct protective measures relating to the information.

This Standard defines how such protective markings are to be formatted for email messages.

This Standard will allow systems, such as an agency's email gateway, to control the flow of information into and out of the agency. For message recipients it also identifies whether an email requires special handling measures by virtue of confidentiality or legislation.

This Standard defines two ways in which protective markings can be applied to email messages:

1. appending the protective marking to the Subject field using a specified syntax
2. including the protective marking in an Internet Message Header Extension using a specified syntax.

These are basic syntaxes and are easy to implement in sending and receiving email agents.

Further advice in relation to implementation of this Standard can be found in the *Email Protective Marking Standard – Implementation Guide for the Australian Government*.

1.1 Document Terminology and Conventions

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [3].

1.2 Audience

This Standard is intended for information technology professionals involved in the development, configuration or administration of email infrastructure components used by Australian Government agencies.

This Standard may have some relevance to information technology professionals who develop, configure or administer the email infrastructures of non-government organisations who exchange messages with Australian Government agencies. These organisations may wish to exchange email messages with government agencies that contain protective markings compliant with this Standard.

1.3 Pre- and co-requisite reading

This Standard should be read in conjunction with RFC2822 [4]. This Standard utilises information in RFC2822 wherever possible. Ideally, the reader should also be familiar with the Augmented Backus-Naur Form syntax, as defined in RFC2234 [5].

The Standard relies on concepts and definitions promulgated in the *Australian Government Information Security Management Protocol*.

The *Australian Government Recordkeeping Metadata Standard version 2.0, July 2008 (AGRkMS)* [6] sets out the type of information that agencies should capture in a structured way to describe the identity, authenticity, content, structure, context and essential management requirements of records and includes a standard set of metadata for use with email messages. Agencies are also referred to the AGRkMS Implementation Guidance (June 2011) prepared by the National Archives of Australia.

1.4 Assumptions

The assumptions made by this Standard are that:

- the message format used by the communicating parties is RFC2822[1]
- email receiving agents will not experience fatal software exceptions on receipt of a message with an arbitrarily long Subject field[2]
- email receiving agents will not experience fatal software exceptions on receipt of a message with an Internet Message Header Extension field.

[1] This does not mean the message necessarily was transmitted over the Internet, only that it uses the RFC2822 standard for formatting the email message.

[2] The agents may not be able to display arbitrarily long Subject fields but such Subject fields will not cause a software exception in them.

2. The standard

2.1 Scope

This Standard defines the format of protective markings in Internet email message (RFC2822) headers.

This Standard is mandatory for Australian Government agencies as defined in the PSPF and optional for non-government agencies. Specific compliance requirements for agencies are outlined in the *Australian Government Information Security Manual* (ISM) [7].

2.2 Out of Scope

The following topics are not addressed by this Standard:

- How a sending or receiving email agent should behave when creating or receiving an email message. This behaviour is defined in the ISM.
- The protective measures that need to be applied to an email message based on its protective marking. The PSPF and the ISM define the protective measures to be taken based on the protective marking of the information.
- The format of the protective marking when the marking is part of the body of an email message.
- The format of the protective marking when the marking is a digitally signed attribute of the message.
- Differentiation between protective markings for whole messages or different protective markings for parts or components of messages, including attachments and paragraphs. The protective marking is used to indicate the highest protection requirements of any part or component of the email message.

2.3 Version

The version number for this definition of the Standard is:

2012.3

2.4 Namespace

The protective markings described in this Standard use the security classification system defined in the *Australian Government security classification system.*

The syntaxes defined in this Standard contain elements to convey this namespace. The namespace for this Standard is:

gov.au

- This namespace value does not necessarily reflect the email domain of the sending and receiving parties. It is simply a short and convenient string that has been used to differentiate this namespace from another entity's.
- If an Australian State or Territory government agency wishes to use the Federal Government namespace and terms then it can use the above. If the state agency wishes to define and use its own namespace and rules, then it may do so provided it uses a different namespace value.

2.5 Syntax of the Protective Marking

This Standard specifies two ways in which the protective marking can be applied to an email message:

- Subject Field Marking
- Internet Message Header Extension.

The Internet Message Header Extension SHOULD be used in preference to the Subject Field Marking (see the *Implementation Guide* for further information).

2.5.1 Subject Field Marking

In this syntax the protective marking is placed in the Subject field of the message (RFC2822 "Subject").

- This approach is the least sophisticated of the techniques and is purposely designed so that a human user can construct and interpret the protective marking without the need for additional tools. Email gateways should be able to translate the email's subject between internal and Internet formats without any degradation. The syntax is sufficiently rich so an email agent, or extensions thereof, can include or parse the protective marking in an automated fashion. The overloading of the "Subject:" header could interfere with other uses of the Subject field. Furthermore, entry of this information by a human is prone to error, and could be easily misinterpreted by email systems. The approach is also included because it is backwards compatible with all Internet email agents and systems.
- 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.

Note that during message generation and transport, other agents may manipulate the subject.

2.6 Internet Message Header Extension

In this syntax the protective marking is carried as a custom Internet Message Header Extension "X-Protective-Marking".

- This approach is a more sophisticated technique that is an extension of the Subject field syntax. It is designed for construction and parsing by email agents (clients, gateways and servers) as they have access to Internet message headers. In this way a richer syntax can be used and email agents can perform more complex handling based on the protective marking.

2.7 Syntax Precedence and Quantities

Both techniques MAY be used in a single email message so long as the protective marking is consistent across both.

When a message contains both forms of the protective marking, information in the "X-Protective-Marking" SHALL take precedence over that in the Subject field.

As per RFC2882, an Internet email message can have at most one Subject field.

A message conforming to this Standard MUST contain at most one "X-Protective-Marking" field.

An email protective marking writer SHALL allow no more than one email protective marking in the subject line.

2.7.1 Non-Compliant Markings

When a reader encounters an email with multiple protective markings in a Subject line, precedence SHALL be given to the first protective marking in the subject line. "First" means "leftmost" when reading left-to-right.

2.8 Size of Protective Marking

The protective marking, in either Subject or Internet Message Header Extension form, MUST NOT exceed a length of 8192 ASCII characters.

- In principle, a protective marking may contain a number of DLMs/caveats. This could provide a means for attackers to cause resource exhaustion on receiving agents. In practice, the length of protective marking will be bounded to some reasonable size which accommodates all current and future possible values. The size constraint given here should accommodate such values and thus minimise avenues of attack.

2.9 Syntax Definitions

The syntax for each protective marking is defined using two methods. A *modified* regular expression syntax using a format derived from script language regular expressions and a formal syntax using the Augmented Backus-Naur Form (ABNF) notation as used by RFC2822.

If there are any ambiguities arising from the two syntaxes then the ABNF syntax SHALL be definitive.

2.10 Regular Expression Definition

The modified regular expression syntax of the protective marking, when it appears in the Subject field, is:

[(SEC=<*securityClassification*>|DLM=<*dlmValue*>|SEC=<*securityClassification*>, DLM=<*dlmValue*>)(, CAVEAT=<*caveatType*>:<*caveatValue*>)*(, EXPIRES=(<*genDate*>|<*event*>), DOWNTO=<*securityClassification*>)?]

The modified regular expression syntax of the protective marking, when it appears as an Internet Message Header Extension is:

X-Protective-Marking: VER=<*ver*>, NS=gov.au, (SEC=<*securityClassification*>|DLM=<*dlmValue*>|SEC=<*securityClassification*>, DLM=<*dlmValue*>)(, CAVEAT=<*caveatType*>:<*caveatValue*>)*(, EXPIRES=(<*genDate*>|<*event*>), DOWNTO=<*securityClassification*>)?(, NOTE=<*comment*>)?, ORIGIN=<*authorEmail*>

For both of the above definitions:

- ( )? delimits an optional element that MAY appear only once if used; the brackets and question mark do not actually appear if element is used.
- ( )* delimits an optional element that MAY be repeated any number of times; the brackets and star symbol do not actually appear if element is used.
- <*text*> denotes the variable value of an element; the angle brackets do not actually appear if the value is present. Any character in *text* may be preceded with '\'; the following characters must be preceded with '\': '\' and ',' only printable characters are permitted (see ABNF definitions for more detail).
- (a|b) denotes an OR option whether either a or b can be used, but not both. The brackets and bar symbol do not actually appear if element is used.
- The order of elements shown here is important – elements, if present, MUST appear in the order specified.
- Field names and values are case-sensitive.
- The security classification value used with the DOWNTO tag MUST be less than that of the SEC tag. The hierarchy of security classifications is outlined in the *Australian Government security classification system*.
- <securityClassification> corresponds to the *Australian Government security classification system* and two additional markings introduced specifically for email messages, and is one of:
  - UNOFFICIAL[3]
  - UNCLASSIFIED[4]
  - PROTECTED
  - CONFIDENTIAL
  - SECRET

[3] 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.

[4] 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 protective marking.

- TOP-SECRET

- Hyphens have been explicitly added to some of these forms in contrast to their form in the PSPF. This has been done to overcome issues seen with some email products that can split message header lines in a non-conformant manner. The extra hyphens are expected to make it simpler to parse a received protective marking of the email message.
- <caveatType> corresponds to the *PSPF Information Security Management Guidelines*[5] and is one of:
  - C, a Codeword caveat
  - SC, a SourceCodeword caveat
- RI, a ReleasabilityIndicator caveat
  - SH, a SpecialHandling caveat.
- *<caveatValue>* corresponds to the *Australian Government security classification system* and is one of:
  - A Codeword *<caveatValue>* is of type *<text>* and has maximum length of 128 characters
  - A SourceCodeword *<caveatValue>* is of type *<text>* and has maximum length of 128 characters.
- A ReleasabilityIndicator *<caveatValue>* is one of:
  - AUSTEO
  - *<countryCodes>* EO
  - AGAO
  - REL *<countryCodes>*
    - where *<countryCodes>* consist of one or more *<countryCode>*, separated by the '/' character
    - *<countryCode>* is a country code as defined ISO 3166-1 alpha-3.
- A SpecialHandling *<caveatValue>*s is one of:
  - ACCOUNTABLE-MATERIAL
  - EXCLUSIVE-FOR *<named person>*
  - *<indicator>*
    - where *<named person>* is the name of a person, has characters limited to those defined for *<text>* and has maximum length of 128 characters
    - where *<indicator>* is of type *<text>* and has maximum length of 128 characters.
- <dlmValue> is a Dissemination Limiting Marker (DLM), corresponds to the *Australian Government security classification system* and is one of:
  - For-Official-Use-Only
  - Sensitive
  - Sensitive:Legal

[5] *Australian Government security classification system*, Section 4.3

- Sensitive:Personal
- Sensitive:Cabinet.

- Values for DLMs that may be conditional on the value of *<securityClassification>* are shown in this table:

Security Classification/ Email Specific Marking	**Dissemination Limiting Marker (DLM)**
UNOFFICIAL	No DLM
UNCLASSIFIED	No DLM
NO SECURITY CLASSIFICATION REQUIRED[6]	For-Official-Use-Only
	Sensitive
	Sensitive:Legal
	Sensitive:Personal
PROTECTED	No DLM
	Sensitive
	Sensitive:Legal
	Sensitive:Personal
	Sensitive:Cabinet
CONFIDENTIAL	No DLM
	Sensitive
	Sensitive:Legal
	Sensitive:Personal
	Sensitive:Cabinet
SECRET	No DLM
	Sensitive
	Sensitive:Legal
	Sensitive:Personal
	Sensitive:Cabinet
TOP-SECRET	No DLM
	Sensitive
	Sensitive:Legal
	Sensitive:Personal

[6] See Implementation Guide

	Sensitive:Cabinet

- A maximum of one <*dlmValue*> is allowed in the protective marking in either the Subject line or in the Internet Message Header.
- The DLM MUST immediately follow the security classification marking. If an agency requires more than one DLM, secondary DLMs MUST be included in the body of the email.
- <*genDate*> is a date of the form *YYYY-MM-DD*(T*HH*:*II*:*SS*(.*F*)(Z|(+|-)*HH*:*II*)).

This is a minor variation of the date and time specification presented in RFC3339 [8]; as presented here the time component is optional – if missing the time is assumed to be T00:00:00Z.

  - *YYYY* is a four digit number representing the **y**ear, for example 2015.
  - *MM* is a two digit number representing the **m**onth, for example 02 for February.
  - *DD* is a two digit number representing the **d**ay of the month, for example 31 for the last day of January.
  - *HH* is a two digit number representing the **h**our of the day, for example 13 for 1pm.
  - *II* is a two digit number representing the m**i**nute of the hour.
  - *SS* is a two digit number representing the **s**econd of the minute.
  - *F* is a variable length number representing the fraction of the second; optional.
  - (Z|(+|-)*HH*:*II*) represents the **t**ime-**z**one and is an optional part of the genDate. Either set to Greenwich Mean Time (Z) or indicates variation from Greenwich Mean Time.
  - Midnight is represented by HH:II:SS = 00:00:00.
  - Example: 1996-12-19T16:39:57-08:00 represents 39 minutes and 57 seconds after the 16th hour of December 19th, 1996 with an offset of -08:00 from UTC (Pacific Standard Time). Note that this is equivalent to 1996-12-20T00:39:57Z in UTC.
- <*event*> corresponds to the *Australian Government security classification system* and is a free-text field; the permitted characters are limited to those defined for <*text*> and has maximum length of 128 characters.
- <*ver*> is the version of the protective marking specification. Format is YYYY.V where:
  - YYYY is a four digit number representing the **y**ear of ratification of the standard, for example 2015.
  - V is the minor version number for the particular year and is a non-negative integer; hence the first published version of the standard for a given year will have minor version number of 0.

- For this Standard, the version value is defined in Section 2.3.

- NS appears in the Internet Message Header Extension is used to convey the namespace of the terms used in the protective marking. For Australian Government agencies it has the value gov.au.
  - For the Subject field form, the namespace is implied from the sender's "From" address – if the domain part of the sender's email address ends with .gov.au then the namespace is that of the Australian Government. This technique therefore cannot be used when a sender from an Australian Government agency wishes to send a message to an international recipient and use their namespace. The alternative in this case is to use the Internet Message Header Extension form of the protective marking.
- *<comment>* is a free-text field where the sender can specify some free-form information to include additional security classification information; the permitted characters are limited to those defined for *<text>* and has maximum length of 128 characters.
- *<authorEmail>* captures the author's email address so that the person who originally classified the email message is always known. This is not necessarily the same as that in the RFC2822 From field.

2.11 Augmented BNF Definition

The Augmented BNF syntax is defined in RFC2234 and is used in RFC2822 to define the syntax for Internet Message Headers. Hence, it is appropriate to use the same language to clearly define the protective marking syntaxes for the Subject Field Marking and the Internet Message Header Extension method, as both of these are Internet Message Header fields.

This Standard assumes the reader is familiar with the core rules of the Augmented BNF syntax, as defined in Section 6.1 of RFC2234.

This Standard includes modified rules from RFC2822 and RFC3339. In particular, the following definitions from those documents are used by this standard:

Rule Type	Rule Name	RFC Section
Primitive Tokens	NO-WS-CTL	RFC2822 – 3.2.1
	text	
	specials	
Quoted characters	quoted-pair	RFC2822 – 3.2.2
Folding white space and comments	FWS	RFC2822 – 3.2.3
	ctext	
	ccontent	
	comment	
	CFWS	
Atom	atext	RFC2822 – 3.2.4
	atom	
	dot-atom	
	dot-atom-text	
Quoted Strings	qtext	RFC2822 – 3.2.5
	qcontent	
	quoted-string	
Miscellaneous tokens	word	RFC2822 – 3.2.6
	phrase	
	utext	
	unstructured	
Internet date time format	date-fullyear	RFC3339 – 5.6
	full-date	
	full-time	

2.11.1 Base tokens

comma-FWS	=	"," FWS	; comma folding
			; whitespace
escaped-special	=	("\" ",") /	
		("\" "\")	
safe-char	=	%d32-43 /	; US-ASCII
		%d45-91 /	; not including
		%d93-126	; "," or "\"
safe-char-pair	=	2 safe-char	; two safe-char
safe-duple	=	safe-char-pair /	
		escaped-special	
one-to-128-safe-text	=	[safe-char]	; This rule
		[safe-char]	; allows for 1 to
		1*63(safe-duple))	; 128 ASCII chars
		[safe-char]	

2.11.2 Email address specification

Derived from RFC2822, but with fewer optional rules and no CFWS allowed in dot-atom:

simple-dot-atom	=	dot-atom-text	; no CFWS allowed
simple-email	=	simple-addr-spec	
simple-addr-spec	=	simple-local-part	"@" simple-domain
simple-local-part	=	simple-dot-atom	
simple-domain	=	simple-dot-atom	

2.11.3 Security classification literals

```
unofficial      =  %d85.78.79.70.70.73.67.73.65.76      ; UNOFFICIAL
unclassified    =  %d85.78                              ; UN
                   %d67.76.65.83.83.73.70.73.69.68      ; CLASSIFIED
protected       =  %d80.82.79.84.69.67.84.69.68         ; PROTECTED
confidential    =  %d67.79.78.70                        ; CONF
                   %d73.68.69.78.84.73.65.76            ; IDENTIAL
secret          =  %d83.69.67.82.69.84                  ; SECRET
top-secret      =  %d84.79.80 "-" secret                ; TOP-SECRET
```

2.11.4 Security classification rules

classification-tag	=	%d83.69.67	; SEC
classification-value	=	unofficial /	; Unofficial emails
		unclassified /	; Unclassified emails
		protected /	; Classified emails
		confidential /secret / top-secret	
classification	=	classification-tag "="	
		classification-value	

2.11.5 Caveat literals

codeword	=	%d67	; C
source-codeword	=	%d83.67	; SC
releasability-indicator	=	%d82.73	; RI
special-handling	=	%d83.72	; SH
accountable-material	=	%d65.67.67.79.85.78.84.65.66.76.69 "-" %d77.65.84.69.82.73.65.76	;ACCOUNTABLE-MATERIAL
exclusive-for	=	%d69.88.67.76.85.83.73.86.69	; EXCLUSIVE
		"-" %d70.79.82	; -FOR
indicator	=	one-to-128-safe-text	
austeo	=	%d65.85.83.84.69.79	; AUSTEO
eo	=	%d69.79	; EO

```
agao            =   %65.71.65.79            ; AGAO
rel             =   %d82.69.76              ; REL
country-code    =   3 %d65-90               ; ISO 3166-1
                                            ; Alpha-3
                                            ; eg AUS
country-codes   =   country-code
                    *( "/" country-code )
```

2.11.6 Caveat rules

```
caveat-tag          =   %d67.65.86.69.65.84                    ; CAVEAT
codeword-caveat     =   codeword ":" one-to-128-safe-text
source-caveat       =   source-codeword ":" one-to-128-safe-text
release-caveat      =   releasability-indicator ":"
handling-caveat     =   ( austeo /
caveat-pair         =   country-codes eo /
caveat              =   agao / rel "/" country-codes )
                        special-handling ":"
                        ( accountable-material /
                        exclusive-for FWS one-to-128-safe-text /
                        indicator )
                        codeword-caveat /
                        source-caveat /
                        release-caveat /
                        handling-caveat
                        caveat-tag "=" caveat-pair
```

2.11.7 DLM literals

```
dlm-tag             =   d68.76.77                              ; DLM
for-official-use-only   =   %d70.111.114 "-"                   ;For-Official-Use-Only
                        %d79.102.102.105.99.105.97.108 "-"
                        %d85.115.101 "-" 79.110.108.121
```

```
sensitive           =   d83.101.110.115.105.116.105.118.101          ; Sensitive
sensitive-cabinet   =   %d83.101.110.115.105.116.105.118.101 ":"     ; Sensitive:
                        %d67.97.98.105.110.101.116                   ; Cabinet

sensitive-legal     =   %d83.101.110.115.105.116.105.118.101 ":"     ; Sensitive:
                        %d76.101.103.97.108                          ; Legal
sensitive-personal  =   %d83.101.110.115.105.116.105.118.101 ":"     ; Sensitive:
                        %d80.101.114.115.111.110.97.108              ; Personal
```

2.11.8 DLM Rules

```
dlm-value   =   for-official-use-only / sensitive /
                sensitive-legal /
                sensitive-personal /
                sensitive-cabinet
Dlm         =   dlm-tag "=" dlm-value
```

2.11.9 Expiry rules

```
expires-tag         =   %d69.88.80.73.82.69.83          ; EXPIRES
expires-date        =   full-date ["T" full-time]       ; RFC3339
expires-event       =   expires-date / event-description
event-description   =   one-to-128-safe-text
downgrade-tag       =   %d68.79.87.78.84.79             ; DOWNTO
Expires             =   expires-tag "=" expires-event
                        comma-FWS downgrade-tag "="
```

classification-value

2.11.10 Note rules

```
note-tag        =   %d78.79.84.69                   ; NOTE
note-value      =   one-to-128-safe-text
note            =   note-tag "=" note-value
```

2.11.11 Origin rules

```
origin-tag      =   %d79.82.73.71.73.78             ; ORIGIN
Origin          =   origin-tag "=" simple-email     ; example:
                                                    ; ORIGIN=
                                                    ; neville.jones@ato.example.org
```

2.11.12 Namespace rules

```
namespace-tag   =   %d78.83                         ; NS
namespace-value =   "gov.au"                        ; case-insensitive
namespace       =   namespace-tag "=" namespace-value   ; NS=gov.au
```

2.11.13 Version rules

```
version-tag          =   %d86.69.82                    ; VER
major-version        =   date-fullyear                 ; RFC3339
minor-version        =   1*DIGIT
version-value        =   major-version "." minor-version
version              =   version-tag "=" version-value ; example
                                                       ; VER=2012.3
```

2.11.14 Protective Marking

```
classification-dlm          =   Classification comma-FWS dlm
protective-mark-short-form  =   classification /dlm /
                                classification-dlm
protective-mark-medium-form =   protective-mark-short-form
                                *(comma-FWS caveat)
                                [comma-FWS expires]
protective-mark-long-form   =   Version
                                comma-FWS namespace
                                comma-FWS protective-mark-medium-form
                                [comma-FWS note]
                                comma-FWS origin
protective-marked-subject   =   "Subject:" [unstructured] [FWS]
                                "[" protective-mark-medium-form
                                "]" [FWS] [unstructured] CRLF
protective-marked-header    =   "X-Protective-Marking:"
                                [FWS] protective-mark-long-form
```

3. References

[FWS] CRLF

Key	Reference
[1]	*Australian Government Information Security Management Protocol*, July 2011 http://www.protectivesecurity.gov.au/Pages/default.aspx
[2]	*Australian Government security classification system* July 2011 http://www.protectivesecurity.gov.au/Pages/default.aspx
[3]	RFC2119 (BCP14), *Key words for use in RFCs to Indicate Requirement Levels*, March 1997 http://www.ietf.org/rfc/rfc2119.txt
[4]	RFC2822, *Internet Message Format*, April 2001 http://www.ietf.org/rfc/rfc2822.txt
[5]	RFC2234, *Augmented BNF for Syntax Specifications: ABNF*, November 1997 http://www.ietf.org/rfc/rfc2234.txt

Key	Reference
[6]	Australian Government Recordkeeping Metadata Standard (version 2.0, July 2008) http://www.naa.gov.au/Images/AGRkMS_Final%20Edit_16%2007%2008_Revised_tcm16-47131.pdf and Australian Government Recordkeeping Metadata Standard Implementation Guidelines (version 2.0 June 2011) *http://www.naa.gov.au/Images/AGRkMS%20Implementation%20Guidelines_tcm16-50156.pdf* National Archives of Australia
[7]	ISM, *Australian Government Information Security Manual*, 2012 http://www.dsd.gov.au/infosec/ism/index.htm
[8]	RFC3339, *Date and Time on the Internet: Timestamps*, July 2002 http://www.ietf.org/rfc/rfc3339.txt
[9]	RFC2821, *Simple Mail Transfer Protocol*, April 2001 http://www.ietf.org/rfc/rfc2821.txt

4. Glossary

These definitions have been sourced from a number of IETF standards, the ISM and the PSPF.

Caveat	A marking that indicates that the information has special requirements in addition to those indicated by any security classification. The term covers codewords, source codewords, releasability indicators and special-handing caveats.
DLM	Dissemination Limiting Markers are markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling. DLMs are NOT security caveats. Where the information is unclassified, they provide the lowest level of protection for official information.
Email Gateway	A device or a system that receives mail from a client system in one transport environment and transmits it to a server system in another transport environment.
Email Protective Marking Reader	An agent which reads and interprets a protective marking from an email message. This may be a human, an email gateway or an email client, or other.
Email Protective Marking Writer	An agent which inserts a protective marking into an email message. This may be a human, or an extension to an email client, or other.
Host	A computer system attached to the Internet (or, in some cases, to a private TCP/IP network) and supporting the SMTP protocol.
IETF	Internet Engineering Task Force – A large open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet – see http://www.ietf.org/
ISO	International Organization for Standardization - see http://www.iso.org/
ITU	International Telecommunication Union – An international organization within the United Nations System where governments and the private sector coordinate global telecom

	networks and services - see http://www.itu.org/
MIME	Multipurpose Internet Mail Extensions - IETF standard for email content allowing multiple types of objects to be included as part of text data message.
MTA	Mail Transfer Agent - a host that acts as an SMTP server and client and therefore provides a mail transport service.
MUA	Mail User Agent – Normally thought of as the sources and targets of mail. At the source, an MUA might collect mail to be transmitted from a user and hand it off to an MTA; the final ("delivery") MTA would be thought of as handing the mail off to an MUA.
Protective marking	The combined set of classifications, DLMs, caveats and other indicators applied to information to indicate the level of protection that should be applied over the information's lifetime.
Relay	An MTA system that receives mail from an SMTP client and transmits it, without modification to the message data other than adding trace information, to another SMTP server for further relaying or for delivery.
RFC	Request for Comments – The official publication channel for Internet standards documents and other publications of the Internet community.
Security Classification	A protective marking to indicate official information which requires increased security to protect its confidentiality. Each security classification has specific handling guidance in the PSPF, while the ISM provides guidance on the ICT controls for protection of such information.
SMTP	Simple Mail Transfer Protocol - Internet email delivery protocol as defined in RFC2821 [9].
SMTP Client	The sender of an email message (a.k.a. SMTP Sender).
SMTP Server	The recipient of an email message (a.k.a. SMTP Receiver).

5. Appendix A

5.1 Change Log

This is a log of changes that occur in the Standard from version to version. Readers who are conversant with a previous version of the Standard can use this change log to understand what important changes have been made to the newer version of the Standard.

Changes from 2012.2

- Clarified relationship between security classification and email specific markings and DLMs
- Changed country code character from '2' to '3'.
- Revised coding error in relation to DLM literals.

Changes from 2012.1

- Allow choice of security classification, dissemination limiting marker, or combination of both.
- Introduced the abbreviated caveat type markings of C, SC, RI and SH so that the protective marking also conveys information about the type of caveat to simplify interpretation by email gateways and clients.
- Allowed for use of multiple country codes in ReleasabilityIndicator where they are separated by forward slash character (backslash character reserved as escape character delimiter).
- Clarified style for Security Classifications and DLMs.

Changes from 2011.1

- Cleaned up syntax around caveats.
- Proposal for UNCLASSIFIED
- Proposal for multiple DLMs and their position
- Proposal for use of ISO 3166-alpha 3.
- Proposal for treatment of markings in subject line.
- Clarified source of authority for markings.
- On advice from Attorney-General's Department, changed case of DLM caveats to proper case.

- On advice from Attorney-General's Department, changed 'Classification' to Security Classification' in the glossary and updated the definition.

Changes from Version 1.0

- Modified classifications and caveats to align with the new classification scheme as published in the PSPF.

Changes from 2005.6

- Modified the use of categories to allow them to be used with any classification.
- Modified classifications to allow CONFIDENTIAL to be used with CABINET-IN-CONFIDENCE.
- Removed the classification of PERSONAL.
- Added AGAO as a releasability caveat.
- Modified the use of releasability indicators to allow for greater flexibility.
- Modified the use of special handling caveats to allow for greater flexibility.

Changes from 2005.5

- Modified the formatting of CABINET-IN-CONFIDENCE.
- Modified the format of category. The ", CAT=" tag has been replaced by a colon ":". This allows for category information to be carried in the DOWNTO attribute as now the DOWNTO has the same format as SEC.
- Added summary table to content of protective marking.
- Increased scope to include email communications with state, territory and local governments, and the private sector.

Changes from 2005.4

- Included URL for discussion forum
- Clarified wording around the simple regular expression definition for Subject line form so that it is clear the protective marking occurs at the end of the subject and that no text is to occur after it, but may have no text before it.
- Modified ABNF rule for Subject line form so that an email message does not have to have any subject in terms of unstructured text.
- Completed ABNF rule on safe-text, now substituted with one-to-128-safe-text and added appropriate constituent rule definitions.
- Replaced most occurrences of SP with "-" in ABNF definitions, for release-caveat used a forward slash instead. These replacements are to simplify the processing of implementation artefacts that might be inserted during message transit.
- Added one-to-128-safe-text to category-value ABNF rule.
- Removed optional FWS from category ABNF rule.
- Completed Definition of Terms in Introductory section.
- Removed Glossary section at end.
- Added examples.
- Removed redundant references and merged remainder into single list.

Changes from 2005.3

- Specified Internet Message Header Extension as preferred mechanism over the Subject Field Marking.
- Clarified distinction between a protective marking and a classification after discussions with Attorney-General's Department and Defence Signals Directorate.
- Modified name of Internet Message Header Extension field from X-Security-Classification to X-Protective-Marking to be consistent with distinction between the two.
- Used term "protective marking(s)" throughout the document rather than "protective mark(s)".
- Proposed future direction of standard in terms of an Internet standard component and an Australian Government specific implementation of the global standard.
- Added security considerations on the assuredness and validity of the protective marking.
- Removed the term sensitivity from the document and modified ABNF literals to use the term classification instead.
- Added the classification of UNOFFICIAL so that unofficial information sent via email messages can be distinguished from official information.
- Replaced spaces with hyphens in literals "HIGHLY-PROTECTED" and "TOP-SECRET".
- Added maximum length constraint of protective marking value.

Changes from 2005.2

- Clarified audience definition in Section 1.3
- Included PSM as pre-requisite in Section 1.4
- Modified wording of security consideration in Section 1.7
- Added information on future directions of Standard in new Section 1.8
- Added network model diagram in Section 1.12
- Modified name of a syntax definition from "Simple Definition" to "Regular Expression Definition" in Section 2.5.4.1
- Removed PUBLIC DOMAIN from the list of allowed sensitivities in line with PSM 2005

Changes from 2005.1

- Modified Augmented BNF definition of email address specification in Section 2.11.2 (now called simple-email, was called author-email) used by the Origin element. The 2005.1 version permitted use of dot-atom from RFC2822 which supported optional CFWS elements. To keep the email address specification as simple as possible only dot-atom-text is now permitted, so in essence simple-email = dot-atom-text "@" dot-atom-text.
- Created additional Augmented BNF rules in Section 2.11.14 so as to have separate rules for the protective marking string without the RFC2822 field definitions contained in the rule. This is to allow other related standards to re-use the ABNF definitions herein.
- In Section 2.11.14 corrected rule for a Subject field which has a protective marking contained within it; now using unstructured token as per RFC2822.
- In ABNF definitions of sensitivity literals, changed from FWS to SP.
- Clarified that the minor-version number is a non-negative integer, so hence begins from zero for the first version of a given year (major version number).
- Added known category literals to Section 2.5.4.2.5.

- Modified rules for categories in Section 2.5.4.2.6 to be stricter.
- Modified rules for caveats in Section 2.5.4.2.8 to be stricter.

5.2 Conventions used in this document

This document uses the following typographical conventions:

Constant width is used for:

- Denoting literal content that appears in the protective marking of an email message.
- Rules written in Augmented BNF syntax.

Constant width italic is used for

- Indicating placeholders where text with a variety of values may appear in the protective mark.
- Notes to this standard are depicted like this: 🗎. The notes convey information which assists to describe the standard, but are not part of the standard themselves.
- Notes may also be shown in tables. Column headings will be shown as “Notes”. These notes are for informational purposes only, not for standardisation purposes.

6. Appendix B

6.1 Examples

For the sake of clarity, some examples of protective markings are included below.

A message containing:

1. unclassified information
2. sensitive but unclassified personal information
3. PROTECTED information, but which shall become unclassified on the 1st of July 2015
4. SECRET information, that is, ACCOUNTABLE MATERIAL and which can only be released to AUSTEO members
5. commercial information.

6.2 Subject Line Examples

A message containing unclassified information

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <42113213312443432456743 5@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

Subject: This is an example subject line [SEC=UNCLASSIFIED]

This is an example message body.

Bye,

Neville

A message containing sensitive but unclassified personal information

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <421235754275725475724 2@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

Subject: This is an example subject line [DLM=Sensitive:Personal]

This is an example message body.

Bye,

Neville

A message containing PROTECTED information, but which shall become unclassified on the 1st of July 2015

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <421345464528248698658653 8@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

Subject: This is an example subject line [SEC=PROTECTED,

EXPIRES=2015-07-01, DOWNTO=UNCLASSIFIED]

This is an example message body.

Bye,

Neville

A message containing SECRET information, that is, ACCOUNTABLE MATERIAL and which can only be released to AUSTEO members

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <421454363775474374734774 5@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

Subject: This is an example subject line [SEC=SECRET,

CAVEAT=SH:ACCOUNTABLE-MATERIAL, CAVEAT=RI:AUSTEO]

This is an example message body.

Bye,

Neville

A message containing commercial information

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <42113213312443432456743 5@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Neville Content-Transfer-Encoding: 7bit

Subject: This is an example subject line

[DLM=For-Official-Use-Only]

This is an example message body.

Bye,

Neville

6.3 Internet Message Header Extension Examples

A message containing unclassified information

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <42214398989048329832409 8@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

X-Protective-Marking: VER=2012.3, NS=gov.au,

SEC=UNCLASSIFIED,

ORIGIN=neville.jones@ato.example.org

Subject: This is an example subject line

This is an example message body.

Bye,

Neville

A message containing sensitive but unclassified personal information

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <42224324593289349082349 8@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

X-Protective-Marking: VER=2012.3, NS=gov.au,

DLM=Sensitive:Personal,

ORIGIN=neville.jones@ato.example.org

Subject: This is an example subject line

This is an example message body.

Bye,

Neville

A message containing PROTECTED information, but which shall become unclassified on the 1st of July 2015

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <42234464363728908943732 5@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

X-Protective-Marking: VER=2012.3, NS=gov.au,

SEC=PROTECTED,

EXPIRES=2015-07-01,

DOWNTO=UNCLASSIFIED,

ORIGIN=neville.jones@ato.example.org

Subject: This is an example subject line

This is an example message body.

Bye,

Neville

A message containing SECRET information, that is, ACCOUNTABLE MATERIAL and which can only be released to AUSTEO members

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <422424344364274828965885585@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

X-Protective-Marking: VER=2012.3, NS=gov.au,

SEC=SECRET,

CAVEAT=SH:ACCOUNTABLE-MATERIAL,

CAVEAT=RI:AUSTEO,

ORIGIN=neville.jones@ato.example.org

Subject: This is an example subject line

This is an example message body.

Bye,

Neville

A message containing commercial information

From: neville.jones@ato.example.org

To: alice@example.org

Message-ID: <421132133124434324567435@ato.example.org>

MIME-Version: 1.0

Content-Type: text/plain; charset=ISO-8859-1

Content-Transfer-Encoding: 7bit

X-Protective-Marking: VER=2012.3, NS=gov.au,

DLM=For-Official-Use-Only,

ORIGIN=neville.jones@ato.example.org

Subject: This is an example subject line

This is an example message body.

Bye,

Neville