



**Australian Government**

**Department of Finance and Deregulation**

Australian Government Information Management Office

# Email Protective Marking Standard for the Australian Government



**September 2011**

Version 2011.1

## Disclaimer

This document has been prepared by the Department of Finance and Deregulation (Finance) and the Defence Signals Directorate (DSD) to provide information to government bodies in relation to the use of email within 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.

© Commonwealth of Australia 2011

ISBN 978-1-921600-35-7

Apart from any use permitted under the Copyright Act 1968, and the rights explicitly granted below, all rights are reserved.

You are free to copy, distribute and transmit the work as long as you attribute the authors. You may not use this work for commercial purposes. You may not alter, transform, or build upon this work.

Except where otherwise noted, any reference to, reuse or distribution of all or part of this report must include the following attribution:

*Email Protective Marking Standard for the Australian Government*, Copyright Australian Government 2011.



Licence: This document is licensed under a Creative Commons Attribution Non-Commercial No Derivs 3.0 licence.

To view a copy of this licence, visit: <http://creativecommons.org/licenses/by-nc-nd/3.0/legalcode>.

Any of the above conditions can be waived if you get our permission. Requests for permission should be addressed in the first instance to:

Assistant Secretary  
Cyber Security Branch  
Department of Finance and Deregulation  
John Gorton Building  
King Edward Terrace,  
Parkes ACT 2600

## Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Other photographs are from the Department of Finance and Deregulation collections.

### COMPLIANCE WITH THE PSPF AND THE ISM

The *Email Protective Marking Implementation Guide for the Australian Government Version 2011.1* (September 2011) and the *Email Protective Marking Standard for the Australian Government Version 2011.1* (September 2011) were developed to assist agencies in implementing protective markings. DSD mandates their use by agencies in the *Australian Government Information Security Manual (ISM)* for the implementation of protective markings in an agency environment.

Compliance with these documents will ensure 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 ISM.

## 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 is used to convey 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.

## Summary

Attribute	Subject Line (count)	Internet Message Header Extension (count)	Content format	Defined	Basis / Reference
VER	0	1	Fixed	0	This Standard
NS	0	1	Fixed	0	PSPF
SEC	1	1	Fixed set	0	PSPF, MTEE, This Standard
CAVEAT	0..n	0..n	Fixed set & free text	0	PSPF, MTEE
EXPIRES	0..1	0..1	Fixed format	0	PSPF
DOWNT0			Fixed set		
NOTE	0	0..1	Free text	0	PSPF
ORIGIN	0	1	Fixed format	0	PSPF

## Table of Contents

1	Introduction .....	5
1.1	Document Terminology and Conventions.....	5
1.2	Audience.....	5
1.3	Pre- and co-requisite reading.....	5
1.4	Assumptions.....	6
2	The Standard.....	6
2.1	Scope.....	6
2.2	Out of Scope .....	6
2.3	Version .....	7
	Namespace .....	7
2.4	Syntax of the Protective Marking .....	7
3	References .....	18
4	Glossary.....	19
5	Appendix A.....	21
5.1	Change Log .....	21
5.2	Conventions used in this document.....	23
6	Appendix B .....	24
6.1	Registration of Message Header with IANA .....	24
6.2	Examples .....	24

# I Introduction

Official information generated by the Australian Government must be protected from unauthorised disclosure. The *Australian Government Information Security Management Protocol* [1] describes when to apply a protective marking so that the protective measures relating to the information are conveyed to all those who handle it.

This Standard defines how such protective markings are to be formatted for intra-agency and inter-agency 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. It also enables the message recipient to appropriately handle and protect the information contained within the message.

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

1. appending the protective marking to Subject field using a specified syntax; and
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.

## 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 [2].

## 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 [3]. 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 [4].

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

The *Australian Government Email Metadata Standard (AGEMS)* [5] presents a standard set of metadata for use with email messages. The set is based on the *Australian Government Recordkeeping Metadata Standard (AGRkMS)* [6]. This document 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.

The Department of Finance and Deregulation (Australian Government Information Management Office) has developed and published the *Implementation Guide for Email Protective Markings for Australian Government* [7] to assist agencies in implementing this Standard.

## 1.4 Assumptions

The assumptions made by this Standard are that:

- the message format used by the communicating parties is RFC2822<sup>1</sup>;
- email receiving agents will not experience fatal software exceptions on receipt of a message with an arbitrarily long subject field<sup>2</sup>;
- email receiving agents will not experience fatal software exceptions on receipt of a message with an Internet Message Header Extension field.

## 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 and optional for non-government agencies. Specific compliance requirements for agencies are outlined in the *Australian Government Information Security Manual (ISM)* [8].

### 2.2 Out of Scope

The following topics are not addressed by this Standard.

This Standard DOES NOT:

- prescribe how a sending or receiving email agent should behave when creating or receiving an email message. This behaviour is defined in the ISM;
- prescribe 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.
- prescribe the format of the protective marking when the marking is part of the body of an email message.
- prescribe the format of the protective marking when the marking is a digitally signed attribute of the message.
- allow differentiation between protective markings for whole messages or different protective markings for parts or components of messages, including attachments and

---

<sup>1</sup> This does not mean the message necessarily was transmitted over the Internet, only that it uses the RFC2822 standard for formatting the email message.

<sup>2</sup> The agents may not be able to display arbitrarily long subject fields but such subject fields will not cause a software exception in them.

paragraphs. The protective marking is hence 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:

2011.1
--------

## Namespace

The protective markings described in this Standard use the classification system defined in the *Australian Government Information Security Management Protocol*.

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 agency wishes to use the Federal Government namespace and terms then they can use the above. If they wish to define and use their own namespace and rules, then they may do so too provided they use a different namespace value.

## 2.4 Syntax of the Protective Marking

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

1. Subject Field Marking
2. Internet Message Header Extension.

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

### Subject Field Marking

In this syntax the protective marking's placement is at the start of the message's subject field (RFC2822 "Subject").

- ▢ This approach is the least sophisticated of the techniques and is purposely designed so that a human user could both 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, could 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.

## 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.

## Syntax Precedence and Quantities

Both techniques **MAY** be used in a single email message so long as the implied 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 conformant to this Standard **MUST** contain at most one X-Protective-Marking field.

## 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 an unlimited number of caveats. This alone 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. It is believed that the size constraint given here will accommodate such values and thus minimise avenues of attack.

## 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 regarded as definitive.

### Regular Expression Definition

The modified regular expression syntax of the protective marking, when it appears at the **end** of the subject field, is:

```
[SEC=<securityClassification>(, CAVEAT=<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>(, CAVEAT=<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 Information Security Management Protocol*.
- <securityClassification> corresponds to the *Australian Government Information Security Management Protocol* and some additional markings introduced specifically for email messages, and is one of:
  - UNOFFICIAL<sup>3</sup>
  - UNCLASSIFIED<sup>4</sup>
  - PROTECTED
  - CONFIDENTIAL
  - SECRET
  - 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

---

<sup>3</sup> UNOFFICIAL is not a security classification marking as listed in the PSPF. It is included in this standard to allow those agencies that choose to use it as a way of distinguishing non work-related email on their systems.

<sup>4</sup> UNCLASSIFIED is not a security classification listed as in the PSPF. It is included in this standard in order to allow agencies to recognise work-related emails that do not carry a security classification and to provide a protective marking to be used in conjunction with dissemination limiting markers as the latter can not be used on their own in email markings.

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 Australian Government Information Security Management Protocol and is one of
  - Codeword
  - SourceCodeword
  - ReleaseabilityIndicator
  - SpecialHandling
  - Dissemination
  - Codeword is of type *<text>* and has maximum length of 128 characters
  - SourceCodeword is of type *<text>* and has maximum length of 128 characters
  - Valid *<caveatValue>*s for *<caveatType>* of ReleaseabilityIndicators:
    - AUSTEO
    - *<countryCode>* EO
    - AGAO
    - REL *<countryCode>*
  - where *<countryCode>* is of type *<text>* and typically consists of country codes, as defined by ISO 3166, separated by either the “\” or “,” character.
  - Valid *<caveatValue>*s for *<caveatType>* of SpecialHandling:
    - 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
  - Valid *<caveatValue>*s for *<caveatType>* of Dissemination:
    - FOR-OFFICIAL-USE-ONLY
    - SENSITIVE
    - SENSITIVE:LEGAL
    - SENSITIVE:PERSONAL
    - SENSITIVE:CABINET
  - *<caveatValue>*s for *<caveatType>* of Dissemination that are conditional on the value of *<securityClassification>* are shown in this table:

Security Classification	Dissemination Limiting Marker
UNOFFICIAL	None
UNCLASSIFIED	FOR-OFFICIAL-USE-ONLY
	SENSITIVE
	SENSITIVE:LEGAL
	SENSITIVE:PERSONAL
PROTECTED	SENSITIVE
	SENSITIVE:LEGAL
	SENSITIVE:PERSONAL
	SENSITIVE:CABINET
CONFIDENTIAL	SENSITIVE
	SENSITIVE:LEGAL
	SENSITIVE:PERSONAL
	SENSITIVE:CABINET
SECRET	SENSITIVE
	SENSITIVE:LEGAL
	SENSITIVE:PERSONAL
	SENSITIVE:CABINET
TOP SECRET	SENSITIVE
	SENSITIVE:LEGAL
	SENSITIVE:PERSONAL
	SENSITIVE:CABINET

- `<genDate>` is a date of the form  
`YYYY-MM-DD(THH:II:SS(.F)(Z|+|-)HH:II)`  
This is a minor variation of the date and time specification presented in RFC3339 9; 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 **year**, for example 2015
  - MM is a two digit number representing the **month**, for example 02 for February

- *DD* is a two digit number representing the **day** of the month, for example 31 for the last day of January
  - *HH* is a two digit number representing the **hour** of the day, for example 13 for 1pm
  - *II* is a two digit number representing the **minute** of the hour
  - *SS* is a two digit number representing the **second** of the minute
  - *F* is a variable length number representing the **fraction** of the second; optional
  - *(Z|+|-)HH:II* represents the **time-zone** 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 Information Security Management Protocol* 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 **year** 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 Australia 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.

## 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 9. 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	

## Base tokens

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

```
1*63( safe-duple ) ) ; 128 ASCII chars  
[ safe-char ]
```

### **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
```

### **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
```

### **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
```

### **Caveat literals**

```
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
```

```

agao = %65.71.65.79 ; AGAO
rel = %d82.69.76 ; REL
country-codes = one-to-128-safe-text
for-official-use-only = %d70.79.82 "-" ; FOR-
                        %d79.70.70.73.67.73.65.76 "-" ; OFFICIAL-
                        %d85.83.69 "-" 79.78.76.89 ; USE-ONLY
sensitive = %d83.69.78.83.73.84.73.86.69 ; SENSITIVE
sensitive:cabinet = %d83.69.78.83.73.84.73.86.69 ":" ; SENSITIVE:
                  %d67.65.66.73.78.69.84 ; CABINET
sensitive:legal = %d83.69.78.83.73.84.73.86.69 ":" ; SENSITIVE:
                 %d76.69.71.65.76 ; LEGAL
sensitive:personal = %d83.69.78.83.73.84.73.86.69 ":" ; SENSITIVE:
                   %d80.69.82.83.79.78.65.76 ; PERSONAL

```

### **Caveat rules**

```

caveat-tag = %d67.65.86.69.65.84 ; CAVEAT
codeword-caveat = one-to-128-safe-text
source-caveat = one-to-128-safe-text
release-caveat = austeo /
                 country-codes eo /
                 agao /
                 rel country-codes
handling-caveat = accountable-material /
                 exclusive-for FWS one-to-128-safe-text /
                 indicator
dissemination-caveat = for-official-use-only /
                       sensitive /
                       sensitive-legal /
                       sensitive-personal /
                       sensitive-cabinet
caveat-pair = codeword-caveat /
              source-caveat /
              release-caveat /
              handling-caveat /
              dissemination-caveat
caveat = caveat-tag "=" caveat-pair

```

### **Expiry rules**

```

expires-tag = %d69.88.80.73.82.69.83 ; EXPIRES
expires-date = full-date ["T" full-time] ; RFC3339 9

```

```

expires-event      = expires-date / event-description
event-description  = one-to-128-safe-text
downgrade-tag      = %d68.79.87.78.84.79           ; DOWNT0
expires            = expires-tag "=" expires-event
                   comma-FWS downgrade-tag "="
                   classification-value

```

### Note rules

```

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

```

### Origin rules

```

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

```

### Namespace rules

```

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

```

### Version rules

```

version-tag        = %d86.69.82                   ; VER
major-version      = date-fullyear                 ; RFC3339 9
minor-version      = 1*DIGIT
version-value      = major-version "." minor-version
version            = version-tag "=" version-value ; example
                   ; VER=2011.1

```

### Protective Marking

```

protective-mark-short-form = classification
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
                           "[" protective-mark-medium-form
                           "]" [FWS] CRLF
protective-marked-header  = "X-Protective-Marking:"
                           [FWS] protective-mark-long-form
                           [FWS] CRLF
```

## 3

## References

Key	Reference
[1]	Australian Government Information Security Management Protocol, July 2011 <a href="http://www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_Part6-CoreProtectiveSecurityPolicies_6.2-AustralianGovernmentInformationSecurityManagementProtocol_AustralianGovernmentInformationSecurityManagementProtocol">http://www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_Part6-CoreProtectiveSecurityPolicies_6.2-AustralianGovernmentInformationSecurityManagementProtocol_AustralianGovernmentInformationSecurityManagementProtocol</a>
[2]	RFC2119 (BCP14), Key words for use in RFCs to Indicate Requirement Levels, March 1997 <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
[3]	RFC2822, Internet Message Format, April 2001 <a href="http://www.ietf.org/rfc/rfc2822.txt">http://www.ietf.org/rfc/rfc2822.txt</a>
[4]	RFC2234, Augmented BNF for Syntax Specifications: ABNF, November 1997 <a href="http://www.ietf.org/rfc/rfc2234.txt">http://www.ietf.org/rfc/rfc2234.txt</a>
[5]	AGEMS, Australian Government Email Metadata Standard Version 1.0, 2005 National Archives of Australia <a href="http://www.naa.gov.au/Images/Email_Metadata_Standard_tcm2-911.pdf">http://www.naa.gov.au/Images/Email_Metadata_Standard_tcm2-911.pdf</a>
[6]	Australian Government Recordkeeping Metadata Standard (AGRkMS) Version 2.0 July 2008 <a href="http://www.naa.gov.au/Images/AGRkMS_Final%20Edit_16%2007%2008_Revised_tcm2-12630.pdf">http://www.naa.gov.au/Images/AGRkMS_Final%20Edit_16%2007%2008_Revised_tcm2-12630.pdf</a>
[7]	Email Protective Markings Implementation Guide for the Australian Government, Version 2011.1, September 2011, Department of Finance and Deregulation, AGIMO <a href="http://www.finance.gov.au/e-government/security-and-authentication/docs/Email_Protective.pdf">http://www.finance.gov.au/e-government/security-and-authentication/docs/Email_Protective.pdf</a>
[8]	ISM, Australian Government Information Security Manual, August 2011 <a href="http://www.dsd.gov.au/publications/Information_Security_Manual_2010_revisedAug11.pdf">http://www.dsd.gov.au/publications/Information_Security_Manual_2010_revisedAug11.pdf</a>
[9]	RFC3339, Date and Time on the Internet: Timestamps, July 2002 <a href="http://www.ietf.org/rfc/rfc3339.txt">http://www.ietf.org/rfc/rfc3339.txt</a>
[10]	RFC2821, Simple Mail Transfer Protocol, April 2001 <a href="http://www.ietf.org/rfc/rfc2821.txt">http://www.ietf.org/rfc/rfc2821.txt</a>
[11]	RFC2026, The internet Standards Process – Revision 3, October 1996 <a href="http://www.ietf.org/rfc/rfc2026.txt">http://www.ietf.org/rfc/rfc2026.txt</a>
[12]	RFC3864, Registration Procedures for Message Header Fields, September 2004 <a href="http://www.ietf.org/rfc/rfc3864.txt">http://www.ietf.org/rfc/rfc3864.txt</a>

## 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 the security classification. The term covers codewords, source codewords, releasability indicators, special-handing caveats and dissemination limiting markers.
Classification	One of a standard set of terms that indicates the sensitivity of information and how it should be handled.
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.
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 <a href="http://www.ietf.org/">http://www.ietf.org/</a>
ISO	International Organization for Standardization - see <a href="http://www.iso.org/">http://www.iso.org/</a>
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 <a href="http://www.itu.org/">http://www.itu.org/</a>
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 classification, 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.
SMTP	Simple Mail Transfer Protocol - Internet email delivery protocol as defined in RFC2821 10.
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 <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 release 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 DOWNT0 attribute as now the DOWNT0 has the same format as SEC.
- Added summary table to content of protective marking.
- Increased scope to include email communications with state and local governments.

#### 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 0 (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 0 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 0 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 Registration of Message Header with IANA

As described in RFC3864 [2], Internet Message Header fields are to be registered with the Internet Assigned Numbers Authority (IANA). <http://www.iana.org/assignments/message-headers/message-header-index.html>.

According to the definitions in RFC3864, the author(s) believe the Internet Message Header Extension defined in this Standard qualifies as a “Permanent Header Field” as it is based on an “Open Standard” in the sense of RFC2026 [1] Section 7.

#### PERMANENT MESSAGE HEADER FIELD REGISTRATION TEMPLATE:

Header field name:

X-Protective-Marking

Applicable protocol:

mail

Status:

Standard

Change controller:

Commonwealth of Australia

Specification document(s): This Document:

[http://www.finance.gov.au/e-government/security-and-authentication/docs/Email\\_Protective\\_Marking\\_Standard\\_2011\\_1.pdf](http://www.finance.gov.au/e-government/security-and-authentication/docs/Email_Protective_Marking_Standard_2011_1.pdf).

### 6.2 Examples

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

Four examples are:

1. A message containing unclassified information
2. A message containing sensitive but unclassified personal information
3. A message containing PROTECTED information, but which shall become unclassified on the 1<sup>st</sup> of July 2015
4. A message containing SECRET information, that is ACCOUNTABLE MATERIAL and which can only be released to AUSTEO members

#### Subject Line Examples

A message containing unclassified 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
```

```
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: <4212357542757254757242@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, CAVEAT=SENSITIVE:PERSONAL]

This is an example message body.

Bye,
Neville
```

#### A message containing PROTECTED information, but which shall become unclassified on the 1<sup>st</sup> of July 2015

```
From: neville.jones@ato.example.org
To: alice@example.org
Message-ID: <4213454645282486986586538@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: <4214543637754743747347745@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=ACCOUNTABLE-MATERIAL, CAVEAT=AUSTEO]

This is an example message body.

Bye,
Neville
```

## Internet Message Header Extension Examples

### A message containing unclassified information

```
From: neville.jones@ato.example.org
To: alice@example.org
Message-ID: <422143989890483298324098@ato.example.org>
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
X-Protective-Marking: VER=2011.1, 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: <422243245932893490823498@ato.example.org>
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
X-Protective-Marking: VER=2011.1, NS=gov.au,
    SEC=UNCLASSIFIED,
    CAVEAT=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 1<sup>st</sup> of July 2015

```
From: neville.jones@ato.example.org
To: alice@example.org
Message-ID: <422344643637289089437325@ato.example.org>
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
X-Protective-Marking: VER=2011.1, 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=2011.1, NS=gov.au,
    SEC=SECRET,
    CAVEAT=ACCOUNTABLE-MATERIAL,
    CAVEAT=AUSTEO,
    ORIGIN=neville.jones@ato.example.org
Subject: This is an example subject line

This is an example message body.

Bye,
Neville
```