



Australian Government

Department of Finance and Administration

Australian Government Information Management Office

Email Protective Marking Standard for the Australian Government

October 2005

Version: 1.0
Date: 1 October 2005
Sponsor: Australian Taxation Office
Authors: Neville Jones, Greg Colla

© Commonwealth of Australia 2005

COMPLIANCE WITH THE PSM AND ACSI 33

The Australian Government Information and Communications Technology Security Manual (ACSI 33) (September 2005) at 3.5.46 states that ‘the standard for the application of protective markings to emails will be promulgated separately once it has been finalised.’

The Implementation Guide for Email Protective Markings for Australian Government Agencies Version 1 (October 2005) and the Email Protective Marking Standard for the Australian Government Version 1 (October 2005) were developed to assist agencies in implementing protective markings. These documents can be accessed at www.agimo.gov.au.

The Defence Signals Directorate (DSD) has reviewed these documents for consistency and compliance with ACSI 33 (September 2005) and the ICT Security Policy for the Use of BlackBerry by the Australian Government (July 2005). DSD supports the use of these documents by agencies in 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 PSM and ACSI 33.

In addition, DSD also considers that such an agency implementation will assist agencies to comply with the whole-of-government policy on BlackBerry as promulgated by AGIMO.

Abstract

This Standard defines the format of protective markings that may be included in internet email message headers for messages exchanged between Australian Government agencies. A protective marking is used to convey the security classification of information in a message, as defined within the Australian Government's Protective Security Manual (PSM) [5]. The protective marking may also contain additional security information about the message that tells systems and users how to appropriately handle and protect the information contained in the message.

Disclaimer

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.

Summary

Attribute	Subject Line (count)	Internet Message Header Extension (count)	Content format	Defined	Basis / Reference
VER	0	1	Fixed	2.5.4.2.13	This standard
NS	0	1	Fixed	2.5.4.2.12	PSM[5]
SEC	1	1	Fixed set	2.5.4.2.4	PSM[5], MTEE [17]
category	0..1	0..1	Fixed set & free text	2.5.4.2.5	PSM[5]
CAVEAT	0..n	0..n	Fixed set & free text	2.5.4.2.8	PSM[5], MTEE [17]
EXPIRES	0..1	0..1	Fixed format	2.5.4.2.9	PSM[5]
DOWNTO			Fixed set		
NOTE	0	0..1	Free text	2.5.4.2.10	PSM[5]
ORIGIN	0	1	Fixed format	2.5.4.2.11	PSM[5]

Table of Contents

1	Introduction.....	5
1.1	Status of this Document.....	5
1.2	Document Terminology and Conventions.....	5
1.3	Audience.....	6
1.4	Pre- and co-requisite reading.....	6
1.5	Assumptions.....	6
1.6	Why the need for this Standard?.....	7
1.7	Security Considerations.....	7
1.8	Future Directions of Standard.....	8
1.9	Change Log.....	8
1.10	Conventions used in this document.....	11
1.11	Definition of Terms.....	11
1.12	Model.....	13
2	The Standard.....	14
2.1	Scope.....	14
2.2	Out of Scope.....	14
2.3	Version.....	15
2.4	Namespace.....	15
2.5	Syntax of the Protective Mark.....	15
2.6	Implementation.....	27
3	References.....	28
4	Appendix.....	30
4.1	Registration of Message Header with IANA.....	30
4.2	Examples.....	31

1 Introduction

Official information generated by the Australian Government must be protected from compromise. Part C of the Protective Security Manual (PSM) describes how to classify material so that the security requirements of the official information are conveyed to all those who handle it. The security classification of a piece of official information is captured in a protective marking applied to the material.

No formal standard currently exists that defines how such marks are to be formatted to inter-agency email messages.

With the growing use of email for inter-agency communications there is a strong case for a standardised and machine readable marking scheme. Such a scheme would allow systems like an agency's email gateway to control the flow of security classified information into and out of the agency. It also means the message recipient can appropriately handle and protect the information contained within the message.

The Standard defines two ways in which the PSM protective markings can be applied to email messages:

1. Appending the marking to Subject field using a specified syntax, and
2. Including the marking in an internet Message Header Extension using a specified syntax.

These are basic syntaxes and so should be easy to implement in sending and receiving email agents. Because of their simplicity it is envisaged that parties will be able to conform to this standard within a short amount of time.

However, due to their simple nature, these protective markings are vulnerable to security attacks. Therefore a more advanced standard is available wherein the protective marking is conveyed in a digitally signed S/MIME (Extended Security Services) Security Label [12]. The proposed standard is described in [2].

1.1 Status of this Document

This document specifies a protocol for Australian Government agencies, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

This draft standard is founded on current published Australian Government policies and standards [1], [5]. These documents are expected to be revised. In turn, this standard may require revisions to reflect those modifications.

1.2 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 [9].

- ☞ These keywords are not to be interpreted as defined in ACSI 33 [1].

1.3 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.

Information security managers and policy writers in Australian Government agencies may also find the Standard of interest as they might be responsible for communicating aspects of the Standard to the public officers of the agency.

The 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 to this Standard.

1.4 Pre- and co-requisite reading

This Standard should be read in conjunction with RFC2822 [14]. 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 [10].

The Standard relies heavily upon concepts and definitions promulgated in the Protective Security Manual Part C – Information Security [5].

The Standard Metadata Tags for Electronic Email (MTEE) [17] presents a standard set of metadata for use with electronic mail (email). The set is based on the Recordkeeping Metadata Standard for Commonwealth Agencies (RkMSCA). This document defines the standard for a subset of rights management attributes from MTEE.

The Department of Finance and Administration (Australian Government Information Management Office) have developed and published implementation guidelines for email protective marking for Australian Government Agencies [3].

1.5 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 field²
- email receiving agents will not experience fatal software exceptions on receipt of a message with a 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

1.6 Why the need for this Standard?

Email has grown to be one of the main business communication tools of the modern era. Every year there is significantly more data being transferred in email messages, both intra- and inter-agency.

Associated with this explosion in use is the need for better management of official information being sent and received in emails. The email systems and users need to know the security classification of the information in order that it can be protected in transit, when stored, when archived and when being read, printed, forwarded or otherwise processed.

No formal standard currently exists that defines how such markings are to be formatted for inter-agency email messages.

For consistency across the whole of Australian Government, there is a need to standardise the way in which protective markings are applied to email messages. In this way, email systems can be automated to manage the email message according to its classification, whether created within the agency or if received from another Government agency.

1.7 Security Considerations

Users of this Standard should take the following threats into account when analysing the security of their email systems.

The methods of applying protective markings using the Subject Field Marking (Section 2.5.1) and internet Message Header Extension (Section 2.5.2) are open to tampering while in transit. This tamper could take the form of alteration, substitution or removal. Nonetheless, this Standard includes those methods as they are supplied as a simple approach for rapid adoption. Such tamper attack could lead to the degradation of the protection that the email system would apply to a message.

This threat may be managed by a combination of protective mechanisms. These mechanisms could be procedural based, such as appropriate policy and regular auditing; and technology based, such as secured networks and S/MIME v3 Security Labels, as described in [2].

Users of the Standard must be aware that the application of this Standard makes no assurance as to the validity of the Protective Markings. In addition to the threat of tampering en-route, the originator of a message may accidentally or intentionally under- or over-classify as message. Such actions may lead to the degradation of the protection that the email system would apply to a message, or increased system costs of managing the message.

This threat may be managed by a number of mechanisms, such as user policy, training and audit.

Implementers of this Standard should be aware that attackers could use this Standard in an attempt to compromise or disrupt email server and client systems and must provide defences against attack techniques such as buffer overflow, command injection and denial of service.

As some simple examples, implementers should:

- use the maximum allowable size of a protective marking when first parsing protective markings to avoid resource consumption attacks,
- validate each element of the protective marking against the defined syntaxes for the element,
- ensure that protective marking data written to files or databases for logging purposes does not contain strings that will invoke unexpected processing (for example SQL injection attacks).

1.8 Future Directions of Standard

1.8.1 Reliance on PSM and ACSI 33

Part C of the Protective Security Manual and ACSI 33 are regularly updated. This Standard has a strong dependency on the content of those documents, so any substantial changes to those could affect the nature of the protective marking for email messages. If changes in those documents cause any material change in the nature of the protective marking for email messages then an update to this Standard should be released shortly thereafter.

1.8.2 Internet standards track

This Standard has been formulated with a number of internet standards in mind, particularly those relating to email transmissions over the internet. The Standard has been written with broad application to the problem of placing protective security markings in email messages with only some parts specific to the Australian Government situation.

For these reasons, the Standard could be split into two. One standard would be generic and could be used by any entity that wished to place protective markings on internet email messages; the second would be specific to the Australian Government and would describe how it implemented the global standard in its local context. The first standard would be tabled to the Internet Engineering Task Force and ratified in that forum; the latter would be owned by the Australian Government. The authors of this Standard recommend such a strategy.

- If part of this Standard does go to Internet Engineering Task Force then it is worth noting that the internet community would possibly only specify use of the internet Message Header Extension form of the protective mark and not the Subject line form, as they would not regard the Subject line as a suitable place to carry such information.

1.8.3 Application to Web traffic

The language used for Web transactions, HyperText Transfer Protocol (HTTP) [11], also uses internet Message Header fields in the headers of the request and response messages. There may be an opportunity in the future to expand the scope of this Standard to include the use of protective markings in HTTP transactions.

1.9 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.

This change log shall only be present in the document while it is in draft status.

1.9.1 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

1.9.2 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

1.9.3 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 security classification after discussions with Attorney-General’s Department and Defence Signals Directorate.

Email Protective Marking Standard for the Australian Government

- 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 security 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.

1.9.4 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

1.9.5 Changes from 2005.1

- Modified Augmented BNF definition of email address specification in Section 2.5.4.2.2 (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 2.5.4.2.14 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 2.5.4.2.14 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.

1.10 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.

1.11 Definition of Terms

These definitions have been sourced from a number of IETF standards, ACSI33, the PSM and <http://www.metasignatures.org/glossary.htm>

Caveat	“a marking that indicates that the information has special requirements in addition to those indicated by the classification”. [1]
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.” [13]
Host	“a computer system attached to the internet (or, in some cases, to a private TCP/IP network) and supporting the SMTP protocol.” [13]
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/

UNCLASSIFIED

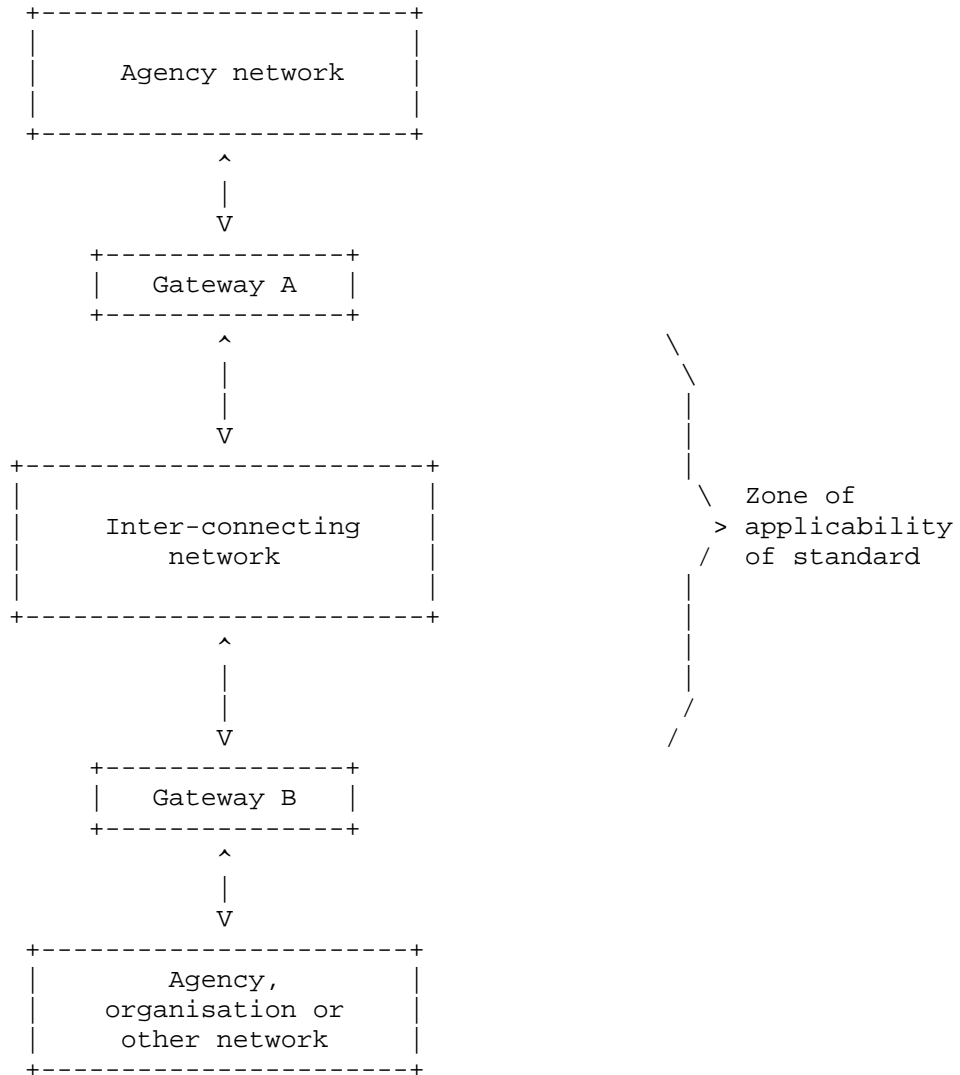
Email Protective Marking Standard for the Australian Government

ISO	International Standards Organization (official name is actually “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 [7]
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” [13]
Protective marking	The combined set of Security Classification, Caveats and other indicators applied to information to indicate the information has been security classified; whether it is national security or non-national security information; and the level of protective procedures that should be used over the information's lifetime. [5]
PSM	Protective Security Manual – “the principal means for disseminating Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official resources.” See http://www.ag.gov.au/
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.” [13]
RFC	Request for Comments – “the official publication channel for internet standards documents and other publications of the internet community.” [6]
Security Classification	One of a standard set of terms that indicates the sensitivity of information and how it should be handled.
SMTP	Simple Mail Transfer Protocol - internet email delivery protocol as defined in RFC2821 [13]
SMTP Client	“the sender of an email message” (a.k.a. SMTP Sender) [13]
SMTP Server	“the recipient of an email message” (a.k.a. SMTP Receiver) [13]

UNCLASSIFIED

1.12 Model

The communications model used by this Standard is such that two agency networks are interconnected via a computer network. Email message flow into, and out of, an agency network is governed by an email gateway.



2 The Standard

2.1 Scope

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

The standard SHALL apply to messages exchanged between:

- Two Australian Government agencies.

The standard MAY apply to messages exchanged between:

- An Australian Government agency and a State/Territory Government agency.
- An Australian Government agency and a Local/Municipal Government agency.
- An Australian Government agency and a business (Australian or otherwise).
- An Australian Government agency and an individual (Australian or otherwise).
- An Australian Government agency and the agency of another nation.

2.2 Out of Scope

This Standard does not prescribe how to classify a message. The Protective Security Manual [5] is the Commonwealth Government's reference document for this task.

This Standard does not prescribe which messages require a protective marking. This requirement is defined in the Defence Signals Directorate's ACSI33 [1].

This Standard does not prescribe how a sending or receiving email agent should behave when creating or receiving a classified message. This behaviour is defined in ACSI33 [1].

This Standard does not prescribe what protection should be applied to an email message based on its classification. The PSM and ACSI33 [1] define the protective measures to be taken based on the classification of the official information.

This Standard does not prescribe the format of protective markings on email messages within an agency's internal email system. It may be used for marking schemes inside an agency's computer network environment, but it is unlikely that all aspects of the Standard will be applicable because of the use of proprietary message formats in such systems.

This Standard does not prescribe the format of the protective marking when the mark is part of the body of a message.

This Standard does not prescribe the format of the protective marking when the mark is a digitally signed attribute of the message [12].

This Standard does not allow differentiation between whole message classification, different classifications on parts of message (PSM Part C "Security classifying paragraphs"), different classification for document title (PSM Part C "Security classifying titles"), or different classifications for annexes, appendices and covering document (PSM Part C "Security classifying annexes, appendices and covering documents"). The protective marking is hence used to indicate the highest classification of any part of the email message, as per PSM recommendations, and the email inherits this maximum classification for its entirety.

2.3 Version

The version number for this definition of the Standard is:

2005.6

2.4 Namespace

The protective markings described in this Standard use the security classification system defined in Part C of the Australian Government's Protective Security Manual.

The syntaxes defined in this Standard contain elements to convey this namespace. This allows receiving parties to be sure of the definition of the security classification term as carried by the protective mark.

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.

2.5 Syntax of the Protective Mark

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

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

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

2.5.1 Subject Field Marking

In this syntax the protective marking's placement is at the end 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 mark 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 mark in an automated fashion. Unfortunately, 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.

2.5.2 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 mark.

2.5.3 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.

2.5.3.1 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.

2.5.4 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 [10] as used by RFC2822.


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

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

PROTECTED
CONFIDENTIAL
HIGHLY-PROTECTED
SECRET
TOP-SECRET

- `<securityClassification>` corresponds to the PSM Part C and some additional ones introduced specifically for email transactions, and is one of:
 - PERSONAL³
 - UNCLASSIFIED
 - IN-CONFIDENCE
 - PROTECTED
 - HIGHLY-PROTECTED
 - RESTRICTED
 - CONFIDENTIAL
 - SECRET
 - TOP-SECRET

 Hyphens have been explicitly added to some of these forms in contrast to their form in the PSM. 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 to determine the security classification of the email message. See Section 2.6.


- `<category>` corresponds to the PSM Part C and is one of:
 - Text determined by sender, contextual for IN-CONFIDENCE exchanges which typically identifies the audience of the material; the permitted characters are limited to those defined for `<text>` ; text has maximum length of 128 characters.
 - SECURITY
 - COMMERCIAL
 - AUDIT
 - STAFF
 - MEDICAL

³ The security classification PERSONAL is not defined in the PSM. It is included in this list as ACSI 33 (paragraph 3.5.45) recommends that email not containing official information be labelled with a markings “such as” PERSONAL. It is suggested that agencies conform to the advice provided by ACSI 33, noting that a standard implementation across government is required for the effective implementation of protective markings. Server behaviour rules may be easily modified to include additional security classifications once they are standardised.

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

- CLIENT
- PERSONNEL
- CABINET-IN-CONFIDENCE

 CABINET-IN-CONFIDENCE has been designated as a category so that simpler rules can be configured at email gateways. Such rules would use the macro-level classification of either PROTECTED, HIGHLY PROTECTED, SECRET or TOP SECRET to block or allow the flow of CABINET-IN-CONFIDENCE material without needing specific rules for it. This is particularly useful for agencies that rarely deal with such material.

Categories that are conditional on the value of sensitivity are shown in this table:

Classification	Allowable Categories	Notes
IN-CONFIDENCE	<i><text></i>	Maximum 128 characters
	COMMERCIAL	
	SECURITY	
	STAFF	
	AUDIT	
	MEDICAL	
	CLIENT	
	PERSONNEL	
	<i>agencyDomainName</i>	For example, ato.gov.au for the Australian Taxation Office
PROTECTED	CABINET-IN-CONFIDENCE	By default, CABINET-IN-CONFIDENCE material is managed in almost the same way as PROTECTED information so the normal combination would be SEC=PROTECTED:CABINET-IN-CONFIDENCE. If some CABINET-IN-CONFIDENCE needs extra protection then the classification field is used to convey the equivalent level of extra care required.
HIGHLY PROTECTED		
SECRET		
TOP SECRET		

- *<caveatType>* corresponds to the PSM Part C and is one of
 - Codeword
 - SourceCodeword
 - ReleaseabilityIndicator
 - SpecialHandling

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

- 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:
 - o AUSTEO
 - o AUST/US-EO
 - o REL/*<countryCode>*
- where *<countryCode>* is a two letter country code using the ISO 3166-1-alpha-2 system [4])
- Valid *<caveatValue>*s for *<caveatType>* of SpecialHandling:
 - o ACCOUNTABLE-MATERIAL
 - o CRYPTO
 - o EXCLUSIVE-FOR *<named person>*
- where *<named person>* is the name of a person, has characters limited to those defined for *<text>* and has maximum length of 128
- *<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 [15]; 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 2004
 - *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.

UNCLASSIFIED

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

- 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 PSM Part C 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 2005.
 - 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 mark. 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 mark.
- *<comment>* is a free-text field where the sender can specify some free-form information to include additional 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.

2.5.4.2 Augmented BNF Definition

The Augmented BNF syntax is defined in RFC2234 [10] 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.

- 📖 The ABNF included herein has been validated using <http://www.apps.ietf.org/abnf.html>

UNCLASSIFIED

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

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 [15]. 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	

2.5.4.2.1 Base tokens

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

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

; by a preceding
; backslash

2.5.4.2.2 *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	

2.5.4.2.3 *Security classification literals*

protected	=	%d80.82.79.84.69.67.84.69.68	; PROTECTED
highly-protected	=	%d72.73.71.72.76.89 "_" protected	; HIGHLY ; ; PROTECTED
in-confidence	=	%d73.78 "-" %d67.79.78.70.73.68.69.78.67.69	; IN- ; CONFIDENCE
personal	=	%d80.69.82.83.79.78.65.76	; PERSONAL
unofficial	=	%d85.78.79.70.70.73.67.73.65.76	; UNOFFICIAL
unclassified	=	%d85.78 %d67.76.65.83.83.73.70.73.69.68	; UN ; CLASSIFIED
restricted	=	%d82.69.83.84.82.73.67.84.69.68	; RESTRICTED
confidential	=	%d67.79.78.70 %d73.68.69.78.84.73.65.76	; CONF ; IDENTIAL
secret	=	%d83.69.67.82.69.84	; SECRET
top-secret	=	%d84.79.80 "_" secret	; TOP ; ; SECRET

2.5.4.2.4 *Category literals*

commercial	=	%d67.79.77.77.69.82.67.73.65.76	; COMMERCIAL
security	=	%d83.69.67.85.82.73.84.89	; SECURITY
staff	=	%d83.84.65.70.70	; STAFF
audit	=	%d65.85.68.73.84	; AUDIT
medical	=	%d77.69.68.73.67.65.76	; MEDICAL
client	=	%d67.76.73.69.78.84	; CLIENT

UNCLASSIFIED

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

```
personnel          = %d80.69.82.83.79.78.78.69.76          ; PERSONNEL
cabinet-in-confidence = %d67.65.66.73.78.69.84 "-"          ; CABINET-
in-confidence      ; IN-
                   ; CONFIDENCE
```

2.5.4.2.5 Category rules

```
x-in-confidence = in-confidence [ ":"
                  ( one-to-128-safe-text /
                    commercial /
                    security /
                    staff /
                    audit /
                    simple-domain /
                    medical /
                    client /
                    personnel ) ]

colon-cic       = ":" cabinet-in-confidence

p-cic          = protected colon-cic
                ; PROTECTED:CABINET-IN-CONFIDENCE

hp-cover-cic   = highly-protected colon-cic
                ; HIGHLY-PROTECTED:CABINET-IN-CONFIDENCE

s-cover-cic    = secret colon-cic
                ; SECRET:CABINET-IN-CONFIDENCE

ts-cover-cic   = top-secret colon-cic
                ; TOP-SECRET:CABINET-IN-CONFIDENCE
```

2.5.4.2.6 Security classification rules

```
classification-tag = %d83.69.67          ; SEC

classification-value = highly-protected /          ; Non-nationals
hp-cover-cic /
protected /
p-cic /
x-in-confidence /
personal /          ; shared
unofficial /
unclassified /
restricted /          ; Nationals
confidential /
secret /
s-cover-cic /
top-secret /
ts-cover-cic

classification = classification-tag "="
classification-value
                ; examples:
                ; SEC=UNCLASSIFIED
                ; SEC=IN-CONFIDENCE:STAFF
```

UNCLASSIFIED

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

2.5.4.2.7 *Caveat literals*

codeword	= %d67.111.100.101 %d119.111.114.100	; Code ; word
source-codeword	= %d83.111.117.114.99.101 codeword	; Source ; Codeword
releaseability-indicator	= %d82.101.108.101.97.115.101 %d97.98.105.108.105.116.121 %d73.110.100.105.99.97.116.111.114	; Release ; ability ; Indicator
special-handling	= %d83.112.101.99.105.97.108 %d72.97.110.100.108.105.110.103	; Special ; Handling
accountable-material	= %d65.67.67.79.85.78.84.65.66.76.69 "- " %d77.65.84.69.82.73.65.76	; ACCOUNTABLE-MATERIAL
crypto	= %d67.82.89.80.84.79	; CRYPTO
exclusive-for	= %d69.88.67.76.85.83.73.86.69 "- " %d70.79.82	; EXCLUSIVE ; -FOR
austeo	= %d65.85.83.84.69.79	; AUSTEO
aust-us-eo	= %d65.85.83.84 " / " %d85.83 "- " %d69.79	; AUST/ ; US-EO
rel	= %d82.69.76	; REL
country-code-iso-a2	= "AF" / "AX" / "AL" / "DZ" / "AS" / "AD" / "AO" / "AI" / "AQ" / "AG" / "AR" / "AM" / "AW" / "AU" / "AT" / "AZ" / "BS" / "BH" / "BD" / "BB" / "BY" / "BE" / "BZ" / "BJ" / "BM" / "BT" / "BO" / "BA" / "BW" / "BV" / "BR" / "IO" / "BN" / "BG" / "BF" / "BI" / "KH" / "CM" / "CA" / "CV" / "KY" / "CF" / "TD" / "CL" / "CN" / "CX" / "CC" / "CO" / "KM" / "CG" / "CD" / "CK" / "CR" / "CI" / "HR" / "CU" / "CY" / "CZ" / "DK" / "DJ" / "DM" / "DO" / "EC" / "EG" / "SV" / "GQ" / "ER" / "EE" / "ET" / "FK" / "FO" / "FJ" / "FI" / "FR" / "GF" / "PF" / "TF" / "GA" / "GM" / "GE" / "DE" / "GH" / "GI" / "GR" / "GL" / "GD" / "GP" / "GU" / "GT" / "GN" / "GW" / "GY" / "HT" / "HM" / "VA" / "HN" / "HK" / "HU" / "IS" / "IN" / "ID" / "IR" / "IQ" / "IE" / "IL" / "IT" / "JM" / "JP" / "JO" / "KZ" / "KE" / "KI" / "KP" / "KR" / "KW" / "KG" / "LA" / "LV" / "LB" / "LS" / "LR" / "LY" / "LI" / "LT" / "LU" / "MO" / "MK" / "MG" / "MW" / "MY" / "MV" / "ML" / "MT" / "MH" / "MQ" / "MR" / "MU" / "YT" / "MX" / "FM" / "MD" / "MC" / "MN" / "MS" / "MA" / "MZ" / "MM" / "NA" / "NR" / "NP" / "NL" / "AN" / "NC" / "NZ" / "NI" / "NE" / "NG" / "NU" / "NF" / "MP" / "NO" / "OM" / "PK" / "PW" / "PS" / "PA" / "PG" / "PY" / "PE" / "PH" / "PN" / "PL" / "PT" / "PR" / "QA" / "RE" / "RO" / "RU" / "RW" / "SH" / "KN" / "LC" / "PM" / "VC" / "WS" / "SM" / "ST" / "SA" / "SN" / "CS" / "SC" / "SL" / "SG" / "SK" / "SI" / "SB" / "SO" / "ZA" / "GS" / "ES" / "LK" / "SD" / "SR" / "SJ" / "SZ" / "SE" / "CH" / "SY" / "TW" / "TJ" / "TZ" / "TH" / "TL" / "TG" / "TK" / "TO" / "TT" / "TN" / "TR" / "TM" / "TC" / "TV" / "UG" / "UA" / "AE" / "GB"	

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

```
/ "US" / "UM" / "UY" / "UZ" / "VU" / "VE" / "VN" / "VG" / "VI" / "WF" / "EH" / "YE" / "ZM" / "ZW"
```

```
country-code = country-code-iso-a2 /  
; as per ISO 3166-1-alpha-2 codes
```

2.5.4.2.8 *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 = releaseability-indicator ":"  
( austeo /  
aust-us-eo /  
rel "/" country-code  
)  
  
handling-caveat = special-handling ":"  
( accountable-material /  
crypto /  
exclusive-for FWS one-to-128-safe-text  
)  
  
caveat-pair = codeword-caveat /  
source-caveat /  
release-caveat /  
handling-caveat /  
  
caveat = caveat-tag "=" caveat-pair
```

2.5.4.2.9 *Expiry rules*

```
expires-tag = %d69.88.80.73.82.69.83 ; EXPIRES  
  
expires-date = full-date ["T" full-time] ; RFC3339 [15]  
  
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
```

2.5.4.2.10 *Note rules*

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

2.5.4.2.11 *Origin rules*

UNCLASSIFIED

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

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

2.5.4.2.12 Namespace rules

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

2.5.4.2.13 Version rules

```
version-tag = %d86.69.82 ; VER
major-version = date-fullyear ; RFC3339 [15]
minor-version = 1*DIGIT
version-value = major-version "." minor-version
version = version-tag "=" version-value ; example
; VER=2005.6
```

2.5.4.2.14 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
```

2.6 Implementation

This section provides implementation requirements for the transmission and interpretation of protective markings according to this Standard. For implementation specifics on the use of protective markings in an agency email system refer to ACSIS3 [1].

2.6.1 Gateways sending email to other domains

Sending gateways SHALL transmit messages that include a protective marking using the syntax and semantics defined in this Standard.

2.6.2 Gateways receiving email from other domains

Receiving gateways SHALL interpret protective markings according to the syntax and semantics defined in this Standard.

Receiving gateways MUST be capable of interpreting both forms of the protective marking.

Receiving gateways SHOULD interpret protective markings that include additional FWSs as lexically equivalent to the protective markings as defined in this standard.

- ☞ MTAs and MUAs may interpret and reformat a message on its route from sender to recipient. For example, long lines may be folded because of line length limitations in some systems. This process may result in artefacts such as extra spaces being inserted into fields in the protective marking. For example, a message sent with “IN-CONFIDENCE” in a protective marking field, may be received as “IN-CONF I DENCE”

3 References

Key	Reference
[1]	ACSI33, <i>Australian Government Information Technology Security Manual</i> , March 2005 http://www.dsd.gov.au/library/infosec/acsi33.html
[2]	Commonwealth of Australia, <i>Advanced Standard for Applying Australian Government Protective Markings to Internet Email Messages</i> (not yet published)
[3]	<i>Implementation Guide for Email Protective Markings for Australian Government</i> , August 2005, Department of Finance and Administration, AGIMO
[4]	ISO 3166 Code lists http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html
[5]	PSM, <i>Australian Government Protective Security Manual</i> , 2005 http://www.ag.gov.au/
[6]	RFC2026, <i>The internet Standards Process -- Revision 3</i> , October 1996 http://www.ietf.org/rfc/rfc2026.txt
[7]	RFC2045, <i>Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies</i> , November 1996 http://www.ietf.org/rfc/rfc2045.txt

UNCLASSIFIED

Email Protective Marking Standard for the Australian Government

Key	Reference
[8]	RFC2076, <i>Common Internet Message Headers</i> , February 1997 http://www.ietf.org/rfc/rfc2076.txt
[9]	RFC2119 (BCP14), <i>Key words for use in RFCs to Indicate Requirement Levels</i> , March 1997 http://www.ietf.org/rfc/rfc2119.txt
[10]	RFC2234, <i>Augmented BNF for Syntax Specifications: ABNF</i> , November 1997 http://www.ietf.org/rfc/rfc2234.txt
[11]	RFC2616, <i>Hypertext Transfer Protocol -- HTTP/1.1</i> , June 1999 http://www.ietf.org/rfc/rfc2616.txt
[12]	RFC2634, <i>Enhanced Security Services for S/MIME</i> , June 1999 http://www.ietf.org/rfc/rfc2634.txt
[13]	RFC2821, <i>Simple Mail Transfer Protocol</i> , April 2001 http://www.ietf.org/rfc/rfc2821.txt
[14]	RFC2822, <i>Internet Message Format</i> , April 2001 http://www.ietf.org/rfc/rfc2822.txt
[15]	RFC3339, <i>Date and Time on the Internet: Timestamps</i> , July 2002 http://www.ietf.org/rfc/rfc3339.txt
[16]	RFC3864, <i>Registration Procedures for Message Header Fields</i> , September 2004 http://www.ietf.org/rfc/rfc3864.txt
[17]	SMTEE, <i>Standard Metadata Tags for Electronic Email</i> , 2005, National Archives of Australia

UNCLASSIFIED

4 Appendix

4.1 Registration of Message Header with IANA

As described in RFC3864 [16], 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 [6] Section 7.

Once this Standard is ratified, the message header is to be registered with IANA using the following registration template.

PERMANENT MESSAGE HEADER FIELD REGISTRATION TEMPLATE:

Header field name:

X-Protective-Marking

Applicable protocol:

mail

Status:

Standard

Change controller:

TBD

Commonwealth of Australia

Specification document(s):

<http://www.dsd.gov.au/>

4.2 Examples

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

At this stage of the Standard's development, we only include four examples as the syntax may still undergo slight modification and we wish to minimise the amount of maintenance of the examples. Future versions of this Standard should include more examples.

The four examples are:

1. A message containing UNCLASSIFIED information
2. A message containing COMMERCIAL-IN-CONFIDENCE information
3. A message containing PROTECTED information, but which shall become UNCLASSIFIED on the 1st of July 2005
4. A message containing SECRET information, that is ACCOUNTABLE MATERIAL and which can only be released to AUSTEO members

4.2.1 Subject Line Examples

4.2.1.1 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
```

4.2.1.2 A message containing COMMERCIAL-IN-CONFIDENCE 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=IN-CONFIDENCE:COMMERCIAL]

This is an example message body.

Bye,
Neville
```

- 4.2.1.3 A message containing PROTECTED information, but which shall become UNCLASSIFIED on the 1st of July 2005

```
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=2005-07-01, DOWNTO=UNCLASSIFIED]

This is an example message body.

Bye,
Neville
```

- 4.2.1.4 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,
    CAV=SpecialHandling:ACCOUNTABLE-MATERIAL,
    CAV=ReleasabilityIndicator:AUSTEO]

This is an example message body.

Bye,
Neville
```

4.2.2 Internet Message Header Extension Examples

- 4.2.2.1 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=2005.6, 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
```

4.2.2.2 A message containing COMMERCIAL-IN-CONFIDENCE 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=2005.6, NS=gov.au,
    SEC=IN-CONFIDENCE:COMMERCIAL,
    ORIGIN=neville.jones@ato.example.org
Subject: This is an example subject line
```

This is an example message body.

Bye,
Neville

4.2.2.3 A message containing PROTECTED information, but which shall become UNCLASSIFIED on the 1st of July 2005

```
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=2005.6, NS=gov.au,
    SEC=PROTECTED, EXPIRES=2005-07-01,
    DOWNTO=UNCLASSIFIED,
    ORIGIN=neville.jones@ato.example.org
Subject: This is an example subject line
```

This is an example message body.

Bye,
Neville

- 4.2.2.4 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=2005.6, NS=gov.au,
    SEC=SECRET,
    CAV=SpecialHandling:ACCOUNTABLE-MATERIAL,
    CAV=ReleasabilityIndicator:AUSTEO,
    ORIGIN=neville.jones@ato.example.org
Subject: This is an example subject line

This is an example message body.

Bye,
Neville
```