Australian Government

Department of Home Affairs
Protective Security Policy Framework

Australian Government Email Protective Marking Standard

Release 2025

Contents

1. Purpose

The Australian Government Email Protective Marking Standard details the requirements for marking the protective marking or security classification on emails exchanged in and between Australian Government entities. This standard supports processes and systems, such as an entity's email gateway, to control the flow of information into, and out, of the entity.

Applying a standard format for protective markings supports processes and systems, such as an entity's email gateway, to control the flow of information into and out of the entity. For message recipients it also identifies what handling protections are needed to safeguard the information.

Requirement 0067 | INFO | All entities | 31 October 2024

The Australian Government Email Protective Marking Standard is applied to protect OFFICIAL and security classified information exchanged by email in and between Australian Government entities, including other authorised parties.

Requirement 0061 | INFO | All entities | 31 October 2024

Security classified information is clearly marked with the applicable security classification, and when relevant, security caveat, by using text-based markings, unless impractical for operational reasons.

2. Assumptions

This standard assumes:

- the email message format used by the communicating parties is based on the Internet Engineering Taskforce RFCs 3339 (time), 5322[1, 2] (message format) and 5234 (syntax)
- email receiving agents will not experience fatal software exceptions on receipt of a message with an arbitrarily long (but no greater than 998 characters) subject field[3], and
- email receiving agents will not experience fatal software exceptions on receipt of a message with an internet message header extension field.

3. Version Control

This document is maintained by the Department of Home Affairs and forms part of the Australian Government Protective Security Policy Framework (PSPF). The version number for this definition of the Standard is:

2025.1

The version number will only be updated to accommodate changes in the syntax structures, regular expressions, or security caveats/protective markings. The version number will not be updated to enact administrative changes to this document, due to the significant impact on entities of updating to new version numbers.

3.1. Change Log

No.	Description	Date
2024.1	Initial release under PSPF Release 2024	01/11/24
2025.1	Syntax change: GSC agreed to retire NATIONAL CABINET caveat. Corrections to the modified regular expression syntax.	01/07/25

1 This does not mean the email was necessarily transmitted over the internet, only that it uses the RFC5322 formatting standard.
2 The guidance uses RFC5322, which obsoletes RFC2822. The text relating to the subject field is the same.
3 Agents may not be able to display arbitrarily long subject fields, but long subject fields will not cause a software exception.

4. Scope

This standard applies the Australian Government protective markings and security classifications for electronic email (i.e. email). The Australian Signals Directorate's Information Security Manual (ISM) supplements this standard and includes guidelines for emails.

This standard does not address:

- how an email agent behaves when creating or receiving an email message (see the ISM)
- the protective measures applied to an email based on its sensitivity or classification protective marking defines relevant protective measures
- the format of a sensitivity or classification protective marking when the marking is a digitally signed attribute of the message
- the format of a sensitivity or classification protective marking when the marking is part of the body of an email message
- differentiation between protective markings for whole messages or different parts/components of messages (including attachments and paragraphs). The protective marking is used to indicate the highest protection requirements of any part or component of the email message, and
- arrangements for receiving emails from other sources, including government entities that are not required to adhere to the PSPF protective markings and classifications (for example, state and territory agencies and corporate Commonwealth entities) and non-government organisations.

5. Recordkeeping Metadata Properties

The PSPF recognises a link between security classification of information and other access restrictions based on the sensitivity of subject content. Entities must apply the Australian Government Recordkeeping Metadata Standard (AGRkMS) as follows:

- for security classified information, apply the AGRkMS' 'Security Classification' property (and, where relevant, the 'Security Caveat' property), and
- where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.

Requirement 0068 | INFO | All entities | 01 July 2025

The Australian Government Recordkeeping Metadata Standard's 'Security Classification' sub-property (and where relevant, the 'Caveat Text' property and 'Caveat Type' sub-property) is applied to protectively mark information on technology systems that store, process or communicate security classified information.

Requirement 0069 | INFO | All entities | 31 October 2024

Apply the Australian Government Recordkeeping Metadata Standard's 'Rights' property where the entity wishes to categorise information content by the type of restrictions on access.

6. Namespace

The syntaxes defined in this standard contain elements to convey the gov.au namespace.

The namespace for this standard is:

gov.au

- This namespace does not necessarily reflect the email domain of the sending and receiving parties.

- State or territory governments may use the Australian Government (gov.au) namespace. If the state or territory wishes to use its own namespace and rules, it may do so provided it uses a different namespace value from the Australian Government.

7. Syntax of the Protective Marking

There are two ways Australian Government protective markings can be applied to email messages:

- appending the protective marking to the Subject field using a specified syntax (Subject Field Marking)
- including the protective marking in an Internet Message Header Extension using a specified syntax (Internet Message Header Extension).

The Internet Message Header Extension marking is the preferred approach for Australian Government entities. An internet message header extension is designed for construction and parsing by email agents (gateways and servers) allowing for handling based on the protective marking.

Where an internet message header extension is not possible, protective markings are placed in the subject field of an email. When printed an email is considered a physical document, as such a visual presentation of the protective marking (such as a separate line in the email) is also important.

Both techniques may be used in a single email message so long as the protective marking is consistent across both. When a message contains both forms of the protective marking, information in the Internet Message Header Extension takes precedence over the Subject Field Marking.

To minimise avenues of attack causing resource exhaustion, consistent with RFC5322, email protective markings are no greater than 998 ASCII characters in length.[4]

7.1. Subject Field Marking

In this syntax, the protective marking is placed in the subject field of the message (RFC5322 'Subject'). As per RFC5322, an Internet email message can have at most one subject field. Allowing for no more than one email protective marking in the subject line minimises confusion and potential conflict.[5]

A Subject Field Marking is less sophisticated than an Internet Message Header Extension as it is possible to manipulate an email's subject during message generation or transport. However, it is easy to apply as a human user can construct (and interpret) the protective marking without the need for additional tools.

Benefits of this approach are that:

- email gateways can translate the email's subject between internal and internet formats without any degradation
- the syntax is sufficiently rich so an automated email agent can include or parse the protective marking, and
- it is backwards compatible with internet email agents and systems.

Key risks include that:

- overloading the 'Subject:' header with a protective marking could interfere with other subject field uses
- human entry of this information is error prone and could be misinterpreted by email systems.

For a standardised approach to Subject Field Marking across government, it is recommended that entities:

---

[4] RFC5322 sets the maximum length of the subject field for compatibility across email clients. In principle, a smaller maximum length also offers a security advantage. A protective marking may contain a number of caveats. This could provide a means for attackers to cause resource exhaustion on receiving agents. In practice, the length of protective marking will be bounded to some reasonable size which accommodates all current and future possible values. The size constraint given here accommodates such values and thus minimise avenues of attack.

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

- position the marking at the end of the Subject field, and
- where possible, implement mitigation strategies to minimise the risk of the marking being truncated.

RFC5322 section 2.1.1 states: there are two limits that this standard places on the number of characters in a line. Each line of characters MUST be no more than 998 characters, and SHOULD be no more than 78 characters, excluding the carriage return/line feed (CRLF).

7.2. Internet Message Header Extension

In this syntax, the protective marking is carried as a custom Internet Message Header Extension 'X-Protective-Marking'. Allowing for no more than one 'X-Protective-Marking' field minimises confusion and potential conflict.

Using an Internet Message Header Extension is more sophisticated than a Subject Field Marking. 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.

8. 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
- a formal syntax using the Augmented Backus-Naur Form (ABNF) notation as used by RFC5234 and used by RFC5322.

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

8.1. Regular Expression Definition

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

```
[(SEC=<securityClassification>)(, CAVEAT=<caveatType>:<caveatValue>)*(,
ACCESS=<InformationManagementMarker>)*(, 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=<caveatType>:<caveatValue>)*(, ACCESS=< InformationManagementMarker>)*(,
EXPIRES=(<genDate>|<event>), DOWNTO=<securityClassification>)?(, NOTE=<comment>)?, ORIGIN=<authorEmail>
```

It is important that the elements appear in the specified order. Field names and values are case-sensitive.

Table 1: Symbols used in regular expression definition

Symbol	Definition
( )?	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 '\'; and the following characters 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.

Symbol	Definition
<securityClassification>	Corresponds to the PSPF classifications (OFFICIAL: Sensitive, PROTECTED, SECRET, TOP SECRET) and additional markings are treated as <securityClassification> specifically for email messages (UNOFFICIAL and OFFICIAL). <security Classification> is one of: • UNOFFICIAL[6] • OFFICIAL[7] • OFFICIAL:Sensitive • PROTECTED • SECRET • TOP-SECRET The security classification value used with the DOWNTO tag is less than that of the SEC tag. The hierarchy of security classifications is outlined in the PSPF.
<InformationManagementMarker>	Is based on the Australian Government Recordkeeping Metadata Standard's 'Rights' property. While categorising information content by non-security sensitives is not mandated as a security requirement, the 'Rights' property provides an optional set of terms ensuring common understanding, consistency and interoperability across systems and government entities. If used, <InformationManagementMarker> is one (or more) of: • Personal-Privacy • Legal-Privilege • Legislative-Secrecy An email with Information Management Marker requires a security classification of OFFICIAL: Sensitive or higher.
<caveatType>	Corresponds to the PSPF classification and caveat section and requires a security classification <caveatType> is one (or more) of: • C, a Codeword caveat • FG, a ForeignGovernment caveat • SH, a SpecialHandling caveat • RI, a ReleasabilityIndicator caveat. .

<caveatValue>	<caveatValue> corresponds to the PSPF:
	• A Codeword <caveatValue> is of type <text> and has maximum length of 128 characters.
	• A ForeignGovernment <caveatValue> is of type <text> and has maximum length of 128 characters.
	• A ReleasabilityIndicator <caveatValue> is one of:
	  ○ AGAO
	  ○ AUSTEO
	  ○ REL <countryCodes>
	  ▪ where <countryCodes> consist of one or more <countryCode>, separated by the '/' character
	  ▪ <countryCode> is a country code as defined ISO 3166-1 alpha-3.
	• A SpecialHandling <caveatValue>s is one of:
	  ○ DELICATE-SOURCE
	  ○ ORCON
	  ○ EXCLUSIVE-FOR <named person>|<indicator>

[6] In the PSPF UNOFFICIAL is not a security classification. It is included as a marking here to allow those entities that choose to use it a way of distinguishing non work-related email on their systems.

[7] In the PSPF OFFICIAL is not a security classification, rather it describes routine information created or processed by the public sector with a low business impact. It is included here in order to allow those entities that choose to use it a way to recognise work-related emails that do not carry a security classification or other protective marking.

Symbol	Definition
	▪ 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 the position title or designation, has characters limited to those defined for <text> and has maximum length of 128 characters. o CABINET o
<genDate>	Is a date of the form YYYY-MM-DD(THH:II:SS(.F)(Z|(+|-)HH:II)).[8] This is a minor variation of the date and time specification presented in RFC3339; as the time component is optional – if missing the time is assumed to be T00:00:00Z. Midnight is represented by HH:II:SS = 00:00:00. • YYYY is a four digit number representing the year, for example 2025 • 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, using a 24 hour clock (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 Universal Time Coordinated (Z) or indicates variation from Universal Time Coordinated.
<event>	Is a free-text field; the permitted characters are limited to those defined for *<text>* and has maximum length of 128 characters.
<ver>	The version number 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 2025 • 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 1. For this *Email protective marking standard*, the version value is **2025.1**. Refer to Section 3 – Version Control for details on version control.
NS	In the Internet Message Header Extension this is used to convey the namespace of the terms used in the protective marking. For Australian Government entities it has the value 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.[9]
<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 RFC5322 From field.

[8] Example: 1996-12-19T16:39:57-08:00 represents 57 seconds after 4:39pm on 19 December 1996 with an offset of -08:00 from UTC (Pacific Standard Time).

[9] This technique therefore cannot be used when a sender from an Australian Government entity 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.

Table 2: Examples of Protective Markings using Subject Field Markings

Message Type	Example
A message containing official information that is not classified	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <421132133124434324567435@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit Subject: This is an example subject line [SEC=OFFICIAL] This is an example message body. Regards, Neville
A message containing sensitive information	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <421132133124434324567435@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit Subject: This is an example subject line [SEC=OFFICIAL:Sensitive] This is an example message body. Regards, Neville
A message containing sensitive information that is legally privileged (where the entity wishes to categorise information content)	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <421132133124434324567435@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit Subject: This is an example subject line [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege] This is an example message body. Regards, Neville
A message containing PROTECTED information, but which, on 1 July 2019, is no longer classified	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <421132133124434324567435@entity.gov.au> 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=2019-07-01, DOWNTO=OFFICIAL] This is an example message body. Regards, Neville
A message containing SECRET information, that is, ACCOUNTABLE MATERIAL and which can only be released to AUSTEO members	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <421132133124434324567435@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit Subject: This is an example subject line [SEC=SECRET, CAVEAT=SH:ACCOUNTABLE-MATERIAL, CAVEAT=RI:AUSTEO] This is an example message body. Regards, Neville

9. Augmented Backus-Naur Form Definition

The Augmented Backus-Naur Form (ABNF) syntax is defined in RFC5234[10] and is used in RFC5322 to define the syntax for Internet Message Headers. The same language defines 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).

Table 3: ABNF Definition: Base tokens

Rule Name		Production	Comment
comma-FWS	=	"," FWS	; comma folding whitespace
escaped-special	=	("\" ",") / ("\" "\")	
safe-char	=	%d32-43 / %d45-91 / %d93-126	; US-ASCII not including "," or "\"
safe-char-pair	=	safe-char safe-char	; two safe-char
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

[10] This guidance assumes familiarity with the core rules of the Augmented BNF syntax, as defined in Section 6.1 of RFC5234. This guidance includes modified rules from RFC5322 and RFC3339. In particular, the following definitions from those documents are used by this guidance:

Rule Type	Rule Name	RFC Section
Quoted characters	quoted-pair	RFC5322 – 3.2.1
Folding white space and comments	FWS ctext ccontent comment CFWS	RFC5322 – 3.2.2
Atom	atext atom dot-atom dot-atom-text	RFC5322 – 3.2.3
Quoted Strings	qtext qcontent quoted-string	RFC5322 – 3.2.4
Miscellaneous tokens	word phrase utext unstructured	RFC5322 – 3.2.5
Internet date time format	date-fullyear full-date full-time	RFC3339 – 5.6

This table shows the tokens that are to be used by email clients when generating legal messages. However, there are obsolete tokens in use from the earlier RFC2822. Consistent with RFC5322, when receiving messages, mail clients MUST honour these obsolete tokens as part of the legal syntax.

Table 4: ABNF Definition: Email address specification[11]

Rule name		Production	Comment
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	

Table 5: ABNF Definition: Security classification literals

Rule name		Production	Comment
unofficial	=	%d85.78.79.70.70.73.67.73.65.76	; UNOFFICIAL
official	=	%d79.70.70.73.67.73.65.76	; OFFICIAL
official-sensitive	=	%d79.70.70.73.67.73.65.76 ":" %d83.101.110.115.105.116.105.118.101	; OFFICIAL:Sensitive[12]
protected	=	%d80.82.79.84.69.67.84.69.68	; PROTECTED
secret	=	%d83.69.67.82.69.84	; SECRET
top-secret	=	%d84.79.80 "-" %d83.69.67.82.69.84	; TOP-SECRET

Table 6: ABNF Definition: Security classification rules

Rule name		Production	Comment
classification-tag	=	%d83.69.67	; SEC
classification-value	=	unofficial / official / official-sensitive / protected / secret / top-secret	; Unofficial emails ; Official emails ; Sensitive emails ; Classified emails
classification	=	classification-tag "=" classification-value	

Table 7: ABNF Definition: Caveat literals

Rule name		Production	Comment
codeword	=	%d67	; C
foreign-government	=	%d70.71	; FG
releasability-indicator	=	%d82.73	; RI
special-handling	=	%d83.72	; SH
delicate-source	=	%d68.69.76.73.67.65.84.69 "-" %d83.79.85.82.67.69	; DELICATE-SOURCE
orcon	=	%d79.82.67.79.78	; ORCON
exclusive-for	=	%d69.88.67.76.85.83.73.86.69 "-" %d70.79.82	; EXCLUSIVE-FOR
cabinet	=	%d67.65.66.73.78.69.84	; CABINET
national-cabinet	=	%d78.65.84.73.79.78.65.76 "-" %d67.65.66.73.78.69.84	; NATIONAL-CABINET
named-person-or-indicator	=	one-to-128-safe-text	
austeo	=	%d65.85.83.84.69.79	; AUSTEO
agao	=	%d65.71.65.79	; AGAO
rel	=	%d82.69.76	; REL
accountable-material	=	%d65.67.67.79.85.78.84.65.66.76.69 "-" %d77.65.84.69.82.73.65.76	; ACCOUNTABLE-MATERIAL
country-code	=	3*3%d65-90	; ISO 3166-1 Alpha-3 e.g. AUS
country-codes	=	country-code *("/" country-code)	

[11] Derived from RFC5322, but with fewer optional rules and no CFWS allowed in dot-atom.

[12] For security classification OFFICIAL: Sensitive, ABNF has no space between colon and S, therefore subject line shows as SEC=OFFICIAL:Sensitive. If classification is also applied in the body of the email, that marking should read OFFICIAL: Sensitive (i.e. with space) in line with PSPF policy.

Table 8: ABNF Definition: Caveat rules

Rule name		Production	Comment
caveat-tag	=	%d67.65.86.69.65.84	; CAVEAT
codeword-caveat	=	codeword ":" one-to-128-safe-text	
foreign-caveat	=	foreign-government ":" one-to-128-safe-text	
release-caveat	=	releasability-indicator ":" (austeo / agao / rel "/" country-codes)	; See Footnote [13] for email system design guidance
handling-caveat	=	special-handling ":" (CABINET / orcon / delicate-source / accountable-material / exclusive-for named-person-or-indicator)	
caveat-pair	=	codeword-caveat / foreign-caveat / release-caveat / handling-caveat	
caveat	=	caveat-tag "=" caveat-pair	

Table 9: ABNF Definition: Information Management Marker literals

Rule name		Production	Comment
personal-privacy	=	%d80.101.114.115.111.110.97.108 "-" %d80. 114.105.118.97.99.121	; Personal-Privacy
legal-privilege	=	%d76.101.103.97.108 "-" %d80.114.105.118.105.108.101.103.101	; Legal-Privilege
legislative-secrecy	=	%d76.101.103.105.115.108.97.116.105.118.101 "-" %d83.101.99.114.101.99.121	; Legislative-Secrecy

Table 10: ABNF Definition: Information Management Marker rules

Rule name		Production	Comment
InformationManagementMarker-tag	=	%d65.67.67.69.83.83	; ACCESS
InformationManagementMarker-value	=	personal-privacy / legal-privilege / legislative-secrecy	
InformationManagementMarker	=	InformationManagementMarker-tag "=" InformationManagementMarker-value	

Table 11: Expiry rules

Rule name		Production	Comment
expires-tag	=	%d69.88.80.73.82.69.83	; EXPIRES
expires-date	=	full-date ["T" full-time]	; RFC3339
expires-event	=	expires-date / event-description	; See Footnote [14]
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	

[13] The email system design should consider and manage the difference between the two 'exclusive-for' cases: the restrictive AGAO and AUSTEO tags (emails distributed within the system) and the permissive REL (emails distributed to a foreign system).
[14] When implementing, check for a valid expires-date token (date and time information) else assume the field is a description.

Table 12: Note rules

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

Table 13: Origin rules

Rule name		Production	Comment
origin-tag	=	%d79.82.73.71.73.78	; ORIGIN
origin	=	origin-tag "=" simple-email	; example: ; ORIGIN=neville.jones@entity.gov.au

Table 14: Namespace rules

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

Table 15: Version rules

Rule name		Production	Comment
version-tag	=	%d86.69.82	; VER
major-version	=	date-fullyear	; RFC3339
minor-version	=	1*DIGIT	
version-value	=	major-version "." minor-version	
version	=	version-tag "=" version-value	; example VER=2025.1

Table 16: Protective marking

Rule name		Production	Comment
protective-mark-short-form	=	classification	
protective-mark-medium-form	=	protective-mark-short-form *(comma-FWS caveat) *(comma-FWS InformationManagementMarker) [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 "]" [unstructured] CRLF	
protective-marked-header	=	"X-Protective-Marking:" [FWS] protective-mark-long-form [FWS] CRLF	

Table 17: Examples of protective markings using Internet Message Header Extensions Markings

Message type	Example
A message containing official information that is not classified	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <422143989890483298324098@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2025.1, NS=gov.au,

Message type	Example
	SEC=OFFICIAL, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Bye, Neville
A message containing sensitive information	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <422243245932893490823498@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER= 2025.1, NS=gov.au, SEC=OFFICIAL:Sensitive, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Regards, Neville
A message containing sensitive information that is legally privileged (where the entity wishes to categorise information content)	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <42113213312443432456743 5@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2025.1, NS=gov.au, SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Regards, Neville
A message containing PROTECTED information, but which, on 1 July 2019, is no longer classified	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <42234464363728908943732 5@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2025.1, NS=gov.au, SEC=PROTECTED, EXPIRES=2019-07-01, DOWNTO=OFFICIAL, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Regards, Neville
A message containing SECRET information, that is, ACCOUNTABLE MATERIAL and	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <42242434436427482896588 5585@entity.gov.au> MIME-Version: 1.0

Message type	Example
which can only be released to AUSTEO members	Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2025.1, NS=gov.au, SEC=SECRET, CAVEAT=SH:ACCOUNTABLE-MATERIAL, CAVEAT=RI:AUSTEO, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Regards, Neville