8 Sensitive and classified information

Annex G. Email protective marking standard

1. This paper provides guidance[1] for a standardised format for protective markings (and, where relevant, information management markings) on emails exchanged in and between Australian Government entities. 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.

Table 1 Allowable system usage during implementation

	1 October 2018	1 January 2019	1 October 2020
	PSPF reforms 2018 commence	New classification system Note 1 starts	Old classification system Note 2 ceases
Internal (entity) communication	**SEND:** old **or** new system **RECEIVE:** old **or** new system	**SEND:** old **or** new system **RECEIVE:** old **or** new system	**SEND: only** new system **RECEIVE: only** new system
External communication	**SEND:** ***only*** old system (***must not*** send externally under new system) **RECEIVE:** ***must*** accept old system	**SEND:** old **or** new system **RECEIVE:** ***must*** receive old and new system	**SEND: only** new system **RECEIVE:** new system Note 3

Notes:
1. New classification system is PSPF policy: Sensitive and classified information (PSPF 2018).
2. Old classification system is the Australian Government Security classification System (PSPF 2014).
3. Entity arrangements for receiving emails from sources other than non-corporate Commonwealth entities remain the same (eg emails from state and territory entities, corporate Commonwealth entities, and non-government organisations).

Scope

2. This guidance applies the protective markings for electronic email (ie email) defined in the PSPF. This guidance is subject to the PSPF and the *Australian Government Information Security Manual* (ISM).
3. This guidance paper does not address:
   a. how an email agent behaves when creating or receiving an email message (see the ISM)
   b. the protective measures applied to an email based on its sensitivity or classification protective marking (see PSPF policy: Sensitive and classified information defines relevant protective measures, with further guidance in the ISM)
   c. the format of a sensitivity or classification protective marking when the marking is a digitally signed attribute of the message
   d. the format of a sensitivity or classification protective marking when the marking is part of the body of an email message (see PSPF policy: Sensitive and classified information section Identifying sensitive and security classified information with a protective marking)

[1] Technical components of this guidance material were developed in consultation with the Digital Transformation Agency.

e. 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

f. 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.

Relevant PSPF requirements

4. The PSPF policy: Sensitive and classified information **Requirement 4** mandate entities 'clearly identify sensitive and security classified information, including emails, by using applicable protective markings'.

5. The PSPF recognises a link between security classification of information and other access restrictions based on the sensitivity of subject content. The PSPF policy: Sensitive and classified information **Requirement 5** mandates entities apply the Australian Government Recordkeeping Metadata Standard (AGRkMS) as follows:

   a. for security classified information, apply the AGRkMS' 'Security Classification' property (and, where relevant, the 'Security Caveat' property)

   b. for OFFICIAL: Sensitive information, apply the 'Dissemination Limiting Marker' property (and, where relevant, the 'Security Caveat' property)

   c. where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.

Assumptions

6. This paper assumes:

   a. the email message format used by the communicating parties is based on the Internet Engineering Taskforce RFCs 3339 (time), 5322[2, 3] (message format) and 5234 (syntax)

   b. 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[4]

   c. email receiving agents will not experience fatal software exceptions on receipt of a message with an internet message header extension field.

Namespace

7. The syntaxes defined in this paper contain elements to convey the gov.au namespace:

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

   b. 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.

Table 2: Namespace value

Namespace	gov.au

Syntax of the Protective Marking

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

   a. appending the protective marking to the Subject field using a specified syntax (Subject Field Marking)

   b. including the protective marking in an Internet Message Header Extension using a specified syntax (Internet Message Header Extension).

[2] This does not mean the email was necessarily transmitted over the internet, only that it uses the RFC5322 formatting standard.

[3] The guidance uses RFC5322, which obsoletes RFC2822. The text relating to the subject field is the same.

[4] Agents may not be able to display arbitrarily long subject fields, but long subject fields will not cause a software exception.

9. The Internet Message Header Extension marking is preferred. The PSPF policy: Sensitive and classified information states:

   For emails, entities apply an internet message header extension; it 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.

10. 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.

11. To minimise avenues of attack causing resource exhaustion, consistent with RFC5322, email protective markings are no greater than 998 ASCII characters in length.[5]

Subject Field Marking

12. 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.[6]

13. 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.

    a. Benefits of this approach are that:

       i. email gateways can translate the email's subject between internal and internet formats without any degradation

       ii. the syntax is sufficiently rich so an automated email agent can include or parse the protective marking

       iii. it is backwards compatible with internet email agents and systems.

    b. Key risks include that:

       i. overloading the 'Subject:' header with a protective marking could interfere with other subject field uses

       ii. human entry of this information is error prone and could be misinterpreted by email systems.

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

    a. position the marking at the end of the Subject field.

    b. where possible, implement mitigation strategies to minimise the risk of the marking being truncated.

       i. 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).

Internet Message Header Extension

15. 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.

[5] 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.

[6] 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.

16. 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.

Syntax Definitions

17. The syntax for each protective marking is defined using two methods:
    a. a modified regular expression syntax using a format derived from script language regular expressions
    b. a formal syntax using the Augmented Backus-Naur Form (ABNF) notation as used by RFC5234 and used by RFC5322.
18. If there are any ambiguities arising from the two syntaxes then the ABNF syntax is definitive.

Regular Expression Definition

19. The modified regular expression syntax of the protective marking, when it appears in the subject field, is outlined in **Table 3**.

Table 3: Subject Field Marking: syntax for modified regular expression

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

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

Table 4: Internet Message Header Extension Marking: syntax for modified regular expression

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

21. It is important that the elements appear in the specified order. Field names and values are case-sensitive.
22. **Table 5** describes each of terms and symbols used in the above definitions.

Table 5: 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.
<securityClassification>	Corresponds to the PSPF policy: Sensitive and classified information's classifications (PROTECTED, SECRET, TOP SECRET) and three additional markings are treated as <securityClassification> specifically for email messages (UNOFFICIAL, OFFICIAL, OFFICIAL:Sensitive). <security Classification> is one of: a. UNOFFICIAL[7] b. OFFICIAL[8] c. OFFICIAL:Sensitive[9] d. PROTECTED e. SECRET f. 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 policy: Sensitive and classified information.
<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: a. Personal-Privacy b. Legal-Privilege c. Legislative-Secrecy An email with InformationManagementMarker requires a security classification of OFFICIAL or higher (OFFICIAL: Sensitive or above recommended).
<caveatType>	Corresponds to the PSPF policy: *Sensitive and classified information*[10] and requires a security classification of PROTECTED or higher (with the exception of the NATIONAL CABINET caveat, which can appear in conjunction with either the OFFICIAL: Sensitive marking or a security classification). <caveatType> is one (or more) of: a. C, a Codeword caveat b. FG, a ForeignGovernment caveat c. SH, a SpecialHandling caveat d. RI, a ReleasabilityIndicator caveat.
<caveatValue>	<caveatValue> corresponds to the PSPF policy: Sensitive and classified information: a. A Codeword <caveatValue> is of type <text> and has maximum length of 128 characters. b. A ForeignGovernment <caveatValue> is of type <text> and has maximum length of 128 characters. c. A ReleasabilityIndicator <caveatValue> is one of: ii. AGAO iii. AUSTEO iv. REL <countryCodes> A. where <countryCodes> consist of one or more <countryCode>, separated by the '/' character B. <countryCode> is a country code as defined ISO 3166-1 alpha-3. d. A SpecialHandling <caveatValue>s is one of: i. DELICATE SOURCE ii. ORCON iii. EXCLUSIVE-FOR <named person>|<indicator> A. where <named person> is the name of a person, has characters limited to those defined for <text> and has maximum length of 128 characters B. where <indicator> is the position title or designation, has characters limited to those defined for <text> and has maximum length of 128 characters. iv. CABINET v. NATIONAL-CABINET[11]
<genDate>	Is a date of the form YYYY-MM-DD(THH:II:SS(.F)(Z|(+|-)HH:II)).[12] 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. a. YYYY is a four digit number representing the year, for example 2018 b. MM is a two digit number representing the month, for example 02 for February c. DD is a two digit number representing the day of the month, for example 31 for the last day of January d. HH is a two digit number representing the hour of the day, using a 24 hour clock (for example 13 for 1pm) e. II is a two digit number representing the minute of the hour f. SS is a two digit number representing the second of the minute g. F is a variable length number representing the fraction of the second; optional h. (Z|(+|-)HH:II) represents the time-**z**one and is an optional part of the genDate. Either set to Greenwich Mean Time (Z) or indicates variation from Greenwich Mean Time.
<event>	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: a. YYYY is a four digit number representing the year of ratification of the standard, for example 2018 b. 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 2018.4
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 **Namespace** 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.[13]
<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.

[7] In the PSPF policy: Sensitive and classified information 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.

[8] In the PSPF policy: Sensitive and classified information 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.

[9] In the PSPF policy: Sensitive and classified information OFFICIAL: Sensitive identifies sensitive but not security classified information. It is included here for simplicity in protective markings.

[10] PSPF policy: Sensitive and classified information, Caveats and accountable material section.

[11] The NATIONAL CABINET caveat commences on 1 December 2020, with implementation by all NCCEs who are required to use this caveat, required by 31 March 2021.

[12] 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).

[13] 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.

23. **Table 6** provides some examples of protective markings using Subject Field Markings.

Table 6: 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. Bye, 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. Bye, 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. Bye, Neville
A message containing sensitive information prepared for National Cabinet or its subcommittees	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, CAVEAT=SH:NATIONAL-CABINET] This is an example message body. Bye, 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. Bye, Neville
A message containing SECRET information, that is, ACCOUNTABLE	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <421132133124434324567435@entity.gov.au> MIME-Version: 1.0

Message type	Example
MATERIAL and which can only be released to AUSTEO members	Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit Subject: This is an example subject line [SEC=SECRET, CAVEAT=SH:ACCOUNTABLE-MATERIAL, CAVEAT=RI:AUSTEO] This is an example message body. Bye, Neville

Augmented BNF Definition

24. The ABNF syntax is defined in RFC5234[14] 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 7: 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

[14] 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 8: ABNF Definition: Email address specification[15]

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 9: 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[16]
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 10: ABNF Definition: Security classification rules

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

Table 11: 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	=	%65.71.65.79	; 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 eg AUS
country-codes	=	country-code *("/" country-code)	

Table 12: 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 17 for email system design guidance

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

[16] For protective marking OFFICIAL: Sensitive, ABNF has no space between colon and S, therefore subject line shows as SEC=OFFICIAL:Sensitive. If a protective marking is also applied in the body of the email, that marking should read OFFICIAL: Sensitive (ie with space) in line with PSPF policy 8, Requirement 4.

handling-caveat	=	special-handling ":" (NATIONAL-CABINET / 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 13: ABNF Definition: InformationManagementMarker 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 14: ABNF Definition: InformationManagementMarker rules

Rule name		Production	Comment
InformationManagement Marker-tag	=	%d65.67.67.69.83.83	ACCESS
InformationManagement Marker-value	=	personal-privacy / legal-privilege / legislative-secrecy	
InformationManagement Marker	=	InformationManagementMarker-tag “=” InformationManagementMarker-value	

Table 15: 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 18
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	

Table 16: 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 17: 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 18: Namespace rules

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

[17] 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).

[18] When implementing, check for a valid expires-date token (date and time information) else assume the field is a description.

namespace	=	namespace-tag "=" namespace-value	; NS=gov.au

Table 19: 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=2018.4

Table 20: 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	

25. **Table 21** provides examples of protective markings using Internet Message Header Extension Markings.

Table 21: 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=2018.4, NS=gov.au, 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=2018.4, 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. Bye, Neville

Message type	Example
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 X-Protective-Marking: VER=2018.4, 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. Bye, Neville
A message containing sensitive information prepared for National Cabinet or its subcommittees	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 X-Protective-Marking: VER=2018.4, NS=gov.au, SEC=OFFICIAL:Sensitive, CAVEAT=SH:NATIONAL-CABINET, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Bye, 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: <422344643637289089437325@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2018.4, 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. Bye, 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: <422424344364274828965885585@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2018.4, 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. Bye,

Message type	Example
	Neville

Change log

Table 22: Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	This is the first version of the standard under the new PSPF. This version aligns with 2018 PSPF classification reforms agreed by the Government Security Committee (GSC) in December 2017 for commencement from 1 October 2018 (with entity transition through to October 2020): a. Rename UNCLASSIFIED to OFFICIAL b. Consolidate DLMs to a single security marking, OFFICIAL: Sensitive c. Remove CONFIDENTIAL classification d. Add CABINET special handling caveat e. Introduce link to information management markers metadata This version also aligns to caveat reforms, as agreed by the GSC's National Intelligence and Security Subcommittee in March 2018: a. Remove EO caveat b. Include Foreign Government markings in caveat hierarchy.
V2018.2	Nov 2019	Table 1	Note added to Table 1 clarifying that existing arrangements for receiving emails from sources other than non-corporate Commonwealth entities remain the same.
V2018.3	Dec 2019	Relevant PSPF requirements	PSPF policy 9: Access to information Requirement 5 moved to policy 8: Sensitive and classified information Requirement 5. Paragraph 5 updated to reflect change.
		Version references	References to previous versions replaced with current version reference, v2018.3.
	May 2020	Tables 6, 9 and 21	Changes not substantive. Version remains the same. Minor amendment to examples in Tables 6 and 21 to show correct application for the protective marking OFFICIAL: Sensitive in the subject line, which is [SEC=OFFICIAL:Sensitive]. Clarification footnote added to Table 9.
V2018.4	September 2020		This version aligns to changes to the Security Caveat Guidelines, approved by the National Intelligence Security Sub-Committee on 18 August 2020, to create a NATIONAL CABINET caveat for use with OFFICIAL: Sensitive and above. Correction to foreign-caveat ABNF definition in Table 12.

26. For further information and guidance, contact the PSPF Team at Attorney-General's Department via email PSPF@ag.gov.au.