



Australian Government

Information security management guidelines

Australian Government security classification system

Approved 1 November 2014

Version 2.0

© Commonwealth of Australia 2013

All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 3.0 AU licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.itsanhonour.gov.au).

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Commercial and Administrative Law Branch
Attorney-General's Department
3–5 National Cct
BARTON ACT 2600

Call: 02 6141 6666

Email: copyright@ag.gov.au

Document details	
Security classification	Unclassified
Dissemination limiting marking	None
Date of security classification review	Not applicable
Authority	Protective Security Policy Committee
Author	Attorney-General's Department
Document status	Version 2.0 – Approved 1 November 2014 Replaces Version 1.1 approved 18 July 2011 Amended September 2013

Contents

1. Introduction	1
1.1 Purpose	1
1.2 Audience.....	1
1.3 Scope	1
1.3.1 Use of specific terms in these guidelines.....	1
2. Background	3
2.1 Why the guidelines were developed.....	3
2.2 Relationship to other documents.....	3
2.3 How the guidelines are structured.....	3
3. Sensitive and security classified information	4
3.1 Two types of official information	4
3.2 Who is responsible for the decision to apply protective markings?	5
3.3 When to apply protective markings	5
3.4 Confirmation of protective marking.....	5
3.5 Who can alter a protective marking?	5
3.6 What to protectively mark	6
3.7 Over-classification	6
3.8 Limiting the duration of the security classification	7
3.9 Review of security classification.....	7
3.10 Agency security classification policy.....	7
3.11 How to identify national interest information	8
3.12 How to identify other information to be protectively marked	8
4. Protective markings.....	9
4.1 When to security classify information.....	9
4.1.1 PROTECTED	9
4.1.2 CONFIDENTIAL	9
4.1.3 SECRET	10
4.1.4 TOP SECRET.....	10
4.2 When to use dissemination limiting markers.....	10
4.2.1 For Official Use Only (FOUO)	11
4.2.2 Sensitive	11
4.2.3 Sensitive: Personal.....	11
4.2.4 Sensitive: Legal.....	11
4.2.5 Sensitive: Cabinet	11
4.3 How to use caveats	12
4.3.1 Codewords.....	12
4.3.2 Source codewords	12
4.3.3 Eyes Only.....	13
4.3.4 Australian Government Access Only (AGAO).....	13
4.3.5 Releasable to	13
4.3.6 Special handling caveats.....	14

4.3.7	Accountable Material	14
5	Cabinet documents.....	15
5.1	Security classifying and marking Cabinet documents	15
6	Foreign government information (FGI)	16
Annex A: Classification and marking ready-reckoner chart		17

Amendments

No.	Date	Location	Amendment
1			
2			

1. Introduction

1.1 Purpose

1. The *Australian Government information security management guidelines—Australian Government security classification system* give guidance to identify and grade the confidentiality requirements of official information.
2. These guidelines assist agencies to identify the value of information. This in turn is advised by the application of a suitable protective marking.

1.2 Audience

3. These guidelines are primarily intended for Australian Government employees and contractors.

1.3 Scope

4. These guidelines relate to information security within the Australian Government.

1.3.1 Use of specific terms in these guidelines

5. In these guidelines the terms:
 - **‘is required to’**—refer to a control:
 - to which agencies cannot give a policy exception, or
 - used in other protective security documents that set controls
 - **‘are to’** or **‘is to’**—are directions required to support compliance with the mandatory requirements of the physical security core policy
 - **‘should’** or **‘should not’**—refers to better practice; agencies are expected to apply better practice unless there is a reason based on their risk assessment to apply alternative controls
 - **‘National Interest’** - a matter which has or could have impact on Australia, including:
 - national security
 - international relations
 - law and governance, including:
 - interstate/ territory relations
 - law enforcement operations where compromise could hamper or prevent national crime prevention strategies or investigations, or endanger personal safety
 - economic wellbeing
 - heritage or culture.

6. For details on policy exceptions see the [*PSPF - Australian Government information security management protocol*](#).

2. Background

2.1 Why the guidelines were developed

7. These guidelines have been developed to provide a consistent and structured approach to the protective marking of Australian Government official information.

2.2 Relationship to other documents

8. These guidelines support the implementation of the [Protective Security Policy Framework \(PSPF\)](#).
9. In particular they support the *PSPF - [Australian Government Information security core policy](#)* and [Information security management protocol](#).
10. They are part of a suite of documents that assist agencies to meet their information security mandatory requirements.

2.3 How the guidelines are structured

11. These guidelines explain the purpose of protective markings and provide guidance on the security classification process, the use of dissemination limiting markers and the application of caveats.

3. Sensitive and security classified information

3.1 Two types of official information

12. There are two types of official information:
 - information that does not need increased security
 - information that needs increased security to protect its confidentiality.
13. Official information can include public sector information sanctioned for public access or circulation, such as agency publications or websites.
14. The *Freedom of Information Act 1982 (Cth)* (the FOI Act), provides the legislative basis for the release of government information. Part IV Exempt Documents, Divisions 1 to 3, describes the types of government documents that may be exempt or conditionally exempt from authorised disclosure.
15. Information which needs increased protection **is to** be either security classified and identified by a protective marking showing the level and protection required, assigned a dissemination limiting marker (DLM) or, when appropriate, a caveat. The presence or absence of a protective marking will not affect a document's status under the FOI Act.
16. Official information which does not need protection may be marked UNCLASSIFIED or left unmarked.
17. The need to know principle **is to** be applied to all official information.
18. Australian Government employees **are to** have agency authorisation to release any information to members of the public. Authorisation may be granted by the agency head or a person authorised by the agency head. When personal information is involved, any release **is to** comply with the *Privacy Act 1988 (Cth)* (the Privacy Act).
19. Even if information is intended for public release or publication it could have confidentiality requirements before release—for example, Budget papers. In this case, the point at which the information will be publicly available **is to** be marked. When this information ceases to need confidential treatment, agencies need to consider continuing availability and integrity requirements.
20. All personal information held—even if it is publicly available—**is to** be handled in accordance with the Australian Privacy Principles (APPs) in the Privacy Act.
21. Where an assessment of business impact levels suggests the compromise of official information would have adverse results, the information **should** be given extra protection. The level and type of protective measures will depend on the severity of the results.
22. Protection is given by limiting access to the information through a series of measures. The measures can be:
 - procedural—such as use, handling, transmission and access restricted to suitably cleared employees
 - physical—for example, storage and access to work area, or
 - technical—such as firewalls and encryption.

23. To reduce the risk of unauthorised disclosure, agencies **should** take all reasonable and appropriate precautions to ensure that only people with a proven need to know and the correct security clearance gain access to sensitive and security classified information.
24. People are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank or level of authorised access. For details on personnel security requirements, see the PSPF - Australian Government Personnel security protocol.
25. Sensitive and security classified information has special handling requirements, especially during electronic transmission or physical transfer. It is only to be used and stored in physical environments that provide a fitting level of protective security. For details on physical security requirements, see the PSPF - Australian Government physical security management protocol.

3.2 Who is responsible for the decision to apply protective markings?

26. The person responsible for preparing the information—or for actioning information produced outside the Australian Government—**is to** decide its protective markings. This person is called the originator.
27. Agencies **are to** advise all employees, including contractors, who use the security classification system on how to use it.

3.3 When to apply protective markings

28. When information is created, the originator **is required to** assess the consequences of damage from unauthorised compromise or misuse of the information. If adverse consequences from compromise of confidentiality could occur or the agency is legally required to protect the information it **is to** be given a protective marking.
29. If information is created outside the Australian Government the person working for the government actioning this information **is to** determine whether it needs a protective marking. Markings suggested by outside organisations or people **should not** automatically be accepted by Australian Government agencies unless there has been a prior agreement. The impact that protective marking may have on information sharing **should** also be considered.
30. Information derived directly from security classified sources **is to** carry, at a minimum, the highest security classification of any of its sources.

3.4 Confirmation of protective marking

31. As protective markings make information more expensive to handle, store and transfer, agencies are encouraged to have a procedure for confirming initial markings, especially where the protective marking is not normal or standard for that agency.

3.5 Who can alter a protective marking?

32. A fundamental principle is that only the originating agency—in other words, the agency that assigned the original protective marking—can change the markings it applies to its information.
33. Protective markings thought to be inappropriate **should** be queried with the originator or the agency now responsible. If an agency is abolished or merged, the agency assuming the former agency's responsibilities is considered the originating agency. The points of contact **should** be

the agency security adviser (ASA) and the information technology security adviser (ITSA) of the new agency.

34. Protectively marked records transferred into the custody of the National Archives of Australia keep the protective markings they had when received from the originating agency and are stored and handled in accordance with those markings. The *Archives Act 1983* (the Archives Act), however, provides that where a record is made available for public access in accordance with the Act—in other words, it is in the open after 30 years period—and does not contain continuing exempt information, any protective markings cease to have effect for any purpose.
35. Agencies considering the transfer of records that carry the security classification of SECRET or above to the National Archives of Australia **should** first consult with the National Archives about the issue of declassification.

3.6 What to protectively mark

36. Government policy is to keep protectively marked information to a minimum. Information needing increased protection is identified by considering the business impact levels of its unauthorised disclosure or misuse.
37. In no case shall official information be protectively marked to:
 - hide violations of law, inefficiency, or administrative error
 - prevent embarrassment to an individual, organisation, or agency
 - restrain competition, or
 - prevent or delay the release of information that does not need protection in the National Interest.

3.7 Over-classification

38. Information **should** only be security classified when the results of compromise warrant the expense of increased protection. It is important that information not requiring protection remains unclassified. DLMs can be used for information requiring the lowest levels of protection. Inappropriate over-classification has many seriously harmful effects:
 - public access to government information becomes unnecessarily limited
 - unnecessary administrative arrangements are established that will remain in force for the life of the document—including repository arrangements for records transferred to the National Archives of Australia—imposing an unnecessary cost on the agency
 - the volume of security classified information becomes too large for an agency to protect adequately
 - security classification and associated security procedures are brought into disrepute if the security classification is unwarranted; this may lead to security classifications and protective markings in general being devalued or ignored by agency employees or receiving agencies.
39. For these reasons the Australian Government expects that agencies will only security classify information and preserve that security classification when there is a clear and justifiable need to do so.

40. To keep the volume of security classified information to a minimum, agencies **should** limit the duration of the security classification and set up review procedures.

3.8 Limiting the duration of the security classification

41. When first classifying information the originator **should** try to settle a specific date or event for declassification based on an assessment of the duration of the information's sensitivity. For example, Budget papers need high protection before the Budget's release but not once it is released publicly. Some information may need increased protection because it is under embargo until a specific public policy statement, after which it becomes public sector information. On reaching the date or event, the information **should** be automatically declassified.
42. If the originator cannot decide an earlier specific date or event for declassification, information **should** be marked for declassification 10 years from the date of the original decision. This is unless the originator otherwise determines the sensitivity of the information requires that it shall be marked for declassification for up to the stated relevant open access period as stated in the Archives Act, Section 3 (7).
43. An agency head may exempt specific information from declassification, the release of which would or could reasonably be expected to fall under the category of an exempt document under the Archives Act, Section 33, Exempt records.
44. An originator may extend the duration of security classification, change the security classification, or reclassify specific information only when the protocols and guidelines for security classifying information are followed.
45. Information marked for an indefinite duration of security classification under predecessor orders or information classified under predecessor orders that contains no declassification instructions **should** be considered for declassification in accordance with these guidelines.
46. Cabinet documents are not included in such arrangements.

3.9 Review of security classification

47. Agencies **should** review the security classification of information regularly—for example, after a project or sequence of events is completed or when a file is withdrawn from, or returned to, use.
48. All recipients of information are encouraged to contact the originator to discuss any security classification they believe is inaccurate.

3.10 Agency security classification policy

49. Failure to identify information requiring increased protection or failure to provide the protective procedures required for sensitive and security classified information would constitute an unacceptable risk to the Australian Government's protective security. It may also put at risk information sharing and consultative arrangements between agencies that are essential to the efficient operation of government.
50. It is essential that agencies respect the rule that information is protectively marked by its originator. Information received from another agency cannot have the protective markings changed without the permission of the originating agency. Agencies receiving protectively

marked information **are to** provide the minimum security protection standards required for that protective marking.

3.11 How to identify national interest information

51. National interest information is any official resource—including equipment that records official information—concerning Australia’s:
- national security:
 - protection from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia’s defence system, acts of foreign interference and the protection of Australia’s territorial and border integrity from serious threats
 - defence capability
 - international relations, significant political and economic relations with international organisations and foreign governments
 - law and governance, including:
 - interstate/ territory relations
 - law enforcement operations where compromise could hamper or make useless national crime prevention strategies or particular investigations, or endanger personal safety
 - economic, scientific or technological matters vital to Australia’s stability, integrity and wellbeing
 - heritage or culture.

3.12 How to identify other information to be protectively marked

52. Not all information needs to be protectively marked (assigned a security classification or DLM). Information is only to be protectively marked if its compromise could damage the National Interest, organisations or individuals, or requires protection under the Privacy Act, the Archives Act or other legislation.
53. A summary guide on identifying information requiring a protective marking is at [Annex A: Classification and marking ready-reckoner chart](#).

4. Protective markings

54. There are three types of protective markings:
- security classifications
 - dissemination limiting markers (DLMs)
 - caveats.
55. Once information has been identified as requiring some form of protection and special handling a protective marking **is to** be assigned to the information. The marking indicates:
- that the confidentiality of the information needs protection
 - the level of protective procedures that **are to** be provided during the use, storage, transmission, transfer and disposal of the information.
56. A protective marking indicates the required level of protection to all users of the information. The system, therefore, provides an assurance that information of broadly equivalent worth or value is given an appropriate and consistent level of protection.
57. Information requiring a protective marking that is held on ICT systems **is to** be identified in the same way as information held on other mediums—such as paper documents—and given an appropriate level of protection.

4.1 When to security classify information

58. There are four levels of security classification. These classifications reflect the level of damage done to the National Interest, organisations and individuals of unauthorised disclosure, or compromise of the confidentiality, of information:
- PROTECTED
 - CONFIDENTIAL
 - SECRET
 - TOP SECRET.
59. Agencies **are to** determine in which circumstances security classifications **are to** be applied to its information. Agencies **are to** develop their own classification guides to assist their personnel classify their information.

4.1.1 PROTECTED

60. The PROTECTED security classification **should** be used when the compromise of the confidentiality of information could be expected to cause damage to the National Interest, organisations or individuals.
61. Examples of types of information which could cause damage and require the use of PROTECTED are in the [Australian Government Protective security governance guidelines – Business Impact Levels](#)—Annex A: BIL 2.

4.1.2 CONFIDENTIAL

62. The CONFIDENTIAL security classification **should** be used when the compromise of the confidentiality of information could be expected to cause significant damage to the National Interest, organisations or individuals.

63. Examples of types of information which could cause significant damage and require the use of CONFIDENTIAL are in the [Australian Government Protective security governance guidelines – Business Impact Levels](#)—Annex A: BIL 3.

4.1.3 SECRET

64. The SECRET security classification **should** be used when compromise of the confidentiality of information could be expected to cause serious damage to the National Interest, organisations or individuals.
65. Examples of types of information which could cause serious damage and require the use of SECRET are in the [Australian Government Protective security governance guidelines – Business Impact Levels](#)—Annex A: BIL 4.

4.1.4 TOP SECRET

66. The TOP SECRET security classification requires the highest degree of protection as compromise of the confidentiality of information could be expected to cause exceptionally grave damage to the National Interest.
67. Examples of types of information which could cause significant damage and require the use of TOP SECRET are in the [Australian Government Protective security governance guidelines – Business Impact Levels](#)—Annex A: BIL 5.

4.2 When to use dissemination limiting markers

68. Dissemination limiting markers (DLMs) are markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling.
69. Although agencies are responsible for determining the appropriate protections to be applied to information bearing DLMs—except Sensitive: Cabinet—they **are to** ensure that the following principles of good information security practice are applied:
- information can only be released to organisations and individuals with a demonstrated need to know
 - information is stored and processed away from public access
 - the removal of information from agency premises is on the basis of identified need
 - disposal of information is by secure means
 - transmission and transfer of information is by means which deter unauthorised access—for example, external mail is sealed and electronic transmission is in accordance with the [Information Security Manual](#) (ISM) requirements.
70. The following five categories of DLM are used:
- For Official Use Only (FOUO)
 - Sensitive
 - Sensitive: Personal
 - Sensitive: Legal
 - Sensitive: Cabinet.

71. Agencies can choose whether to use DLMs—other than Sensitive: Cabinet—on a case-by-case basis.

4.2.1 For Official Use Only (FOUO)

72. **For Official Use Only (FOUO)** may be used on unclassified information only, when its compromise may cause limited damage to the National Interest, organisations or individuals.

73. Examples of types of information which could cause limited damage and require the use of FOUO are in the [Australian Government Protective security governance guidelines – Business Impact Levels](#)—Annex A: BIL 1.

4.2.2 Sensitive

74. Sensitive may be used with security classified or unclassified information:

- where the secrecy provisions of enactments may apply, or
- the disclosure of which may be limited or prohibited under legislation.

4.2.3 Sensitive: Personal

75. Sensitive: Personal may be used with security classified or unclassified information that is sensitive personal information. (This aligns with the definition of sensitive information in Section 6 of the Privacy Act.)

76. For example: a ‘Sensitive: Personal’ document would protect information such as fact or opinion about an individual including their sexual preference, health status or political beliefs.

4.2.4 Sensitive: Legal

77. Sensitive: Legal may be used for any information that may be subject to legal professional privilege.

4.2.5 Sensitive: Cabinet

78. Sensitive: Cabinet **is to** be applied to:

- any document including but not limited to business lists, minutes, submissions, memoranda and matters without submission that is or has been:
 - submitted or proposed to be submitted to Cabinet, or
- official records of Cabinet
- any other information that would reveal:
 - the deliberations or decisions of Cabinet, or
 - matters submitted, or proposed to be submitted to Cabinet.

79. Any use of the DLM ‘Sensitive: Cabinet’ **is to** be accompanied by a security classification protective marker of at least PROTECTED level.

80. For more information see [Section 5 - Cabinet documents](#).

81. A summary guide on identifying information requiring a marking is at Annex A: Classification and marking ready-reckoner chart.

4.3 How to use caveats

82. Certain security classified information, most notably some information impacting on national security, may bear a caveat in addition to a security classification. The caveat is a warning that the information has special requirements in addition to those indicated by the protective marking.
83. Caveats are not classifications in their own right and **are not to** appear without the appropriate protective marking. Those people who need to know will be cleared and briefed about the significance of this type of information. Other people are not to have access to this information.
84. Information bearing agency specific caveats **are to** be re-labelled or appropriate procedures agreed before release or transmission outside of that agency.
85. The prior agreement of the originating agency—in other words, the agency that originally placed the caveat on the material—**is required to** remove a caveat. If the originating agency will not agree to the removal of the caveat then the information cannot be released. The requirement to obtain agreement of the originating agency to release the material cannot be the subject of a policy exception under any circumstances.
86. The following categories of security caveat are used:
 - codewords
 - source codewords
 - Eyes Only
 - Australian Government Access only
 - Releasable to
 - special handling caveats
 - Accountable Material.

4.3.1 Codewords

87. A codeword is a word indicating that the information it covers is in a special need to know compartment.
88. It is often necessary to take precautions beyond those normally indicated by the security classification to protect that information. These will be specified by the organisation that owns the information—for instance, those with a need to access the information will be given a special briefing first.
89. The codeword is chosen so that its ordinary meaning is unrelated to the subject of the information.

4.3.2 Source codewords

90. A source codeword is a word or set of letters used to identify the source of certain information without revealing it to those who do not have a need to know.

4.3.3 *Eyes Only*

91. The Eyes Only marking indicates that access to information is restricted to certain nationalities, for instance:
 - **AUSTEO** means Australian Eyes Only
 - **AUS/USA EO** means Australian and United States of America Eyes Only.
92. Any information marked Eyes Only cannot be passed to or accessed by nationals who are not listed in the marking.
93. Access to information marked with the AUSTEO caveat can only be passed to appropriately security cleared Australian citizens, including officers of the Australian Government, on a need to know basis.
94. Foreign nationals cannot be allowed access to AUSTEO information, even if they have the appropriate Australian security clearance. If an agency head considers that foreign nationals **should** be given information to which the caveat AUSTEO applies, the agency head is to first consult with the originating agency to see if the caveat is still required or whether it could be modified to enable release. It may be possible to have the caveat removed or to release part of the information by removing the caveat from that part.
95. The prior agreement of the originating agency—in other words, the agency that originally placed the AUSTEO caveat on the material—**is required to** remove an AUSTEO caveat. If the originating agency will not agree to the removal of the AUSTEO caveat then the information cannot be released to foreign nationals. The requirement to obtain originating agency agreement to release AUSTEO material cannot be the subject of a policy exception under any circumstances.
96. A person who has dual nationality may be given AUSTEO-marked information as long as they were born in Australia or otherwise hold Australian citizenship.
97. With the exception of AUSTEO, Eyes Only markings **are to** employ the appropriate three letter country codes from ISO 3166-1 Alpha 3 Codes for the representation of names of countries and their subdivisions.

4.3.4 *Australian Government Access Only (AGAO)*

98. In limited circumstances AGAO is used by the Department of Defence and ASIO. It means these agencies may pass information marked with the AGAO caveat to appropriately cleared representatives of foreign governments on exchange or long-term posting or attachment to the Australian Government. AGAO material received in other agencies **is to** be handled as if it were marked AUSTEO.

4.3.5 *Releasable to*

99. The caveat RELEASABLE TO identifies information that has been released or is releasable to the indicated foreign countries only—for example, **REL GBR, NZL** means that the information may be passed to the United Kingdom and New Zealand only.
100. RELEASABLE TO markings **are to** employ the appropriate three letter country codes from the ISO 3166-1 Alpha 3 Codes for the representation of names of countries and their subdivisions.

4.3.6 Special handling caveats

101. A special-handling caveat is a collection of various indicators such as operation codewords, instructions to use particular communications channels and EXCLUSIVE FOR (named person). This caveat is usually used only within particular need to know compartments.
102. There are special requirements for some caveat or codeword information. These are determined by the agency controlling the compartment and provided on a need to know basis.

4.3.7 Accountable Material

103. If strict control over access to, and movement of, particularly sensitive information is required, originators can make this information Accountable Material. What constitutes Accountable Material will vary from agency to agency, but could include Budget papers, tender documents and sensitive ministerial briefing documents.
104. Accountable Material is subject to the following conditions:
 - the marking 'Accountable Material' can be in bold print on the front cover of the material—not necessary for Cabinet documents, TOP SECRET information and codeword material
 - it **is to** carry a reference and individual copy number—agencies could also consider making each page accountable by numbering (for example, page 3 of 10), and placing the document copy number on each page
 - it **is to** carry a warning such as: not to be copied without the prior approval of the originator
 - it **is to** only be passed by hand or safe hand—if it is passed to another person, a receipt is to be obtained
 - a central register **is to** be maintained of all persons having access to each accountable document—this central register is separate from the movement record which forms part of the document or file.

5 Cabinet documents

105. Documents used by Cabinet to formulate policy and make decisions require special protective measures.
106. This is because Cabinet documents, unlike other official information, belong to the particular governments that create them. They are integral to the process by which governments make decisions and they constitute the record of those decisions.
107. Any unauthorised disclosure damages the openness and frankness of discussions in Cabinet and thereby impedes the process of good government. For further information on Cabinet documents see the [Cabinet Handbook](#).

5.1 Security classifying and marking Cabinet documents

108. All documents prepared for consideration by Cabinet, including those in preparation are, as a minimum, to be marked 'Sensitive: Cabinet' and carry the security classification protective marker PROTECTED, regardless of any other security consideration, for example:

PROTECTED
Sensitive: Cabinet

109. Cabinet documents can require a higher level of protection depending on whether their subject matter is considered to have a higher impact on the National Interest. In this case the Cabinet document is to show, immediately before the dissemination limiting marker Sensitive: Cabinet, one of the higher protective markings, for example:

SECRET
Sensitive: Cabinet

110. For more information see Section [4.2.5 Sensitive: Cabinet](#).

6 Foreign government information (FGI)

111. Where information is provided in accordance with a bilateral security instrument for the reciprocal protection of exchanged classified information, it is to be given the equivalent Australian protective security marking.
112. The appropriate classification will assure protection equivalent to, but not less than, that required by the government providing the information.
113. Foreign government information cannot be released to third parties without the prior written approval of the foreign government.
114. Where security classified information is received from another country with which Australia does not have a bilateral security instrument, the Australian security classification to be applied will need to be determined on a case-by-case basis.
115. The Diplomatic Security and Services Branch of the Department of Foreign Affairs and Trade, or the Department of Defence's Defence Security Authority may be consulted for assistance when determining the correct level of protection.
116. Further implementation guidance can be found in the [Australian Government Protective security governance guidelines—safeguarding foreign government information](#).

Annex A: Classification and marking ready-reckoner chart

