Requirements for the Protection of National Security Information in Federal Criminal Proceedings and Civil Proceedings[1]

National Security Information (Criminal and Civil Proceedings) Act 2004

Part 1 Introduction

1. This document sets out the requirements relating to national security information that is, or is to be, disclosed in a federal criminal proceeding or civil proceeding under the *National Security Information (Criminal and Civil Proceedings) Act 2004* (the Act). Regulations are to be made under the Act to give effect to these requirements. Appendix C explains the terms used in this document.

Part 2 Requirements for protecting national security information disclosed in a federal criminal or civil proceeding

2. This Part makes provision for:
   - the ways in which national security information that is disclosed, or to be disclosed, to the court in a federal criminal proceeding or civil proceeding must be stored, handled and destroyed; and
   - the ways in which, and places at which, such information may be accessed and documents or records relating to such information may be prepared.

   See subsections 23 (1) and 38C(1) of the Act.

Storage, handling and destruction of national security information that is disclosed, or to be disclosed, to the court

3. The tables in Part 4 set out the requirements for the storage, handling and destruction of information with a national security classification that is disclosed, or to be disclosed, to the court in a federal criminal proceeding or civil proceeding. The requirements in this document do not affect the operation of the *Archives Act 1983*. It should be noted particularly that information with a national security classification must not be created, stored or transmitted electronically unless the requirements set out in the tables are met.

4. Information with a national security classification is classified as follows:

- Restricted
- Confidential
- Secret, or
- Top Secret.

There are special requirements for some caveat or codeword information. Any special requirements are determined by the originator and will be provided to relevant court staff, the prosecution, legal teams and unrepresented parties to civil proceedings on a need to know basis.

5. Further advice on the storage, handling and destruction of information with a national security classification may be obtained from the Protective Security Coordination Centre (PSCC) of the Attorney-General's Department (telephone (02) 6250 5351 or (02) 6250 5369). The PSCC provides policy advice on protective security and delivers various security programs. The PSCC will provide security awareness training to relevant officers.

6. Further advice on the electronic transmission of information with a national security classification may be obtained from the Defence Signals Directorate (DSD) (telephone (02) 6265 0197). DSD, located within the Department of Defence, is Australia's national authority for the security of information that is processed, stored or communicated by electronic or similar means.

7. Those permitted access to information with a national security classification must be mindful of the need to know principle and of the enduring nature of their obligation to preserve the confidentiality of the information after the requirement for access to such material has ceased.

Ways in which, and places at which, national security information may be accessed and documents or records relating to such information may be prepared

Legal teams in federal criminal proceedings or civil proceedings

8. If a legal team does not have facilities that meet the requirements set out in Part 4, the information may be accessed before and during a proceeding at:
   - an office of the Australian Government Solicitor that has appropriate facilities
   - an office in the court that has appropriate facilities, or
   - another place that has appropriate facilities.

9. If documents need to be transferred to and from the court, this must be done in accordance with the requirements set out in the tables in Part 4. The documents must be returned to the place at which they are securely stored at the end of the day.

10. Any document or record prepared from a document or documents with a national security classification (source documents or copies of them) must be marked with the same classification as the most highly classified of those documents. If a defence legal team has facilities that meet the requirements set

out in Part 4, these documents or records can be kept on the legal team's premises. If a legal team does not have appropriate facilities, the documents or records prepared from the source documents must be stored on the premises where the legal team accessed the source documents.

11. If a document has no protective marking but contains national security information, it must be treated as if it were classified Top Secret unless downgraded by the Australian Government.

Unrepresented parties in civil proceedings

12. An unrepresented party in a civil proceeding may access national security information before and during a proceeding at:
    - an office of the Australian Government Solicitor that has appropriate facilities
    - an office in the court that has appropriate facilities, or
    - another place that has appropriate facilities.

13. If documents need to be transferred to and from the court, this must be done in accordance with the requirements set out in the tables in Part 4. The documents must be returned to the place at which they are stored at the end of the day. Further advice can be provided by the PSCC of the Attorney-General's Department (telephone (02) 6250 5351 or (02) 6250 5369).

14. Any document or record prepared from a document or documents with a national security classification (source documents or copies of them) must be marked with the same classification as the most highly classified of those documents. The documents or records prepared from the source documents must be stored on the premises where the unrepresented party to a civil proceeding accessed the source documents outlined in Part 2, section 12.

15. If a document has no protective marking but contains national security information, it must be treated as if it were classified Top Secret unless downgraded by the Australian Government.

Return of classified material at the end of a proceeding

Legal teams in federal criminal proceedings or civil proceedings

16. Provided a legal team has appropriate facilities, the legal team may keep information with a national security classification until the end of the period in which they are representing a party to the proceeding, or the end of the proceeding including any appeal, whichever occurs first. The information must continue to be stored and handled in accordance with the requirements set out in Part 4.

17. At the end of the proceeding including any appeal, the legal representatives acting for the parties involved must return any source documents in their possession to the originator. Copies of the source documents and any documents or records prepared from them, or copies of those documents, must be destroyed in accordance with the requirements set out in Part 4. An Australian Government official will oversee the destruction of relevant documents.

18. If a party's legal representatives cease acting for the party, source documents, copies of source documents, documents or records prepared from those documents and the classified document register (CDR) must be placed in a sealed tamper-evident container and delivered to the Attorney-General's Department, by a **prescribed method as detailed in the tables in Part 4**. The Department will store the container unopened until the new legal team has been appointed. The new legal team may then access the container.

19. At the end of a federal criminal proceeding including any appeal, the DPP will store and dispose of all documents or records containing national security information in accordance with the *Archives Act 1983* and the policy applicable to such material.

20. At the end of a civil proceeding, including any appeal, the Attorney-General's Department will store and dispose of all documents or records (other than documents in the possession of the court), containing national security information in accordance with the *Archives Act 1983* and the policy applicable to such material.

21. At the end of the proceeding including any appeal, the court will store and dispose of any documents containing national security information in its possession in accordance with Part 4. (This must be done in accordance with the *Archives Act 1983* requirements for Commonwealth records.)

Unrepresented parties in civil proceedings

22. An unrepresented party to a civil proceeding may **access information** with a national security classification until the end of the proceedings including any appeal, whichever occurs first, in accordance with the requirements in sections 12 to 15 in Part 2.

23. At the end of the proceeding including any appeal, the unrepresented party to a civil proceeding, must leave all source documents in **his or her** possession where the information was accessed during the proceeding. Copies of the source document and any documents or records prepared from them, or copies of those documents, must be destroyed in accordance with the requirements set out in Part 4. An Australian Government official will oversee the destruction of relevant documents.

24. At the end of the proceeding including any appeal, the Attorney-General's Department will store and dispose of all documents or records (other than documents in the possession of the court) containing national security information in accordance with the *Archives Act 1983* and the policy applicable to such material.

25. At the end of the proceeding including any appeal, the court will store and dispose of any documents containing national security information in its possession in accordance with Part 4. (This must be done in accordance with the *Archives Act 1983* requirements for Commonwealth records).

Part 3 Requirements relating to record of closed hearing

26. This Part makes provision for:

- the ways in which, and the places at which, the record of the hearing may be accessed by a legal team to a federal criminal proceeding, civil proceeding or a party to a civil proceeding; and
- the ways in which, and places at which, documents and records in relation to the record of the hearing may be prepared by a legal team to a federal criminal proceeding, civil proceeding, or a party to the civil proceeding.

See subsections 29 (5) and 38I(9) of the Act.

Federal criminal proceedings

27. The prosecution may make an application to the judge for an order that attributes a national security classification to the record of hearing. The record of the hearing will be stored by the court in accordance with the requirements set out in the tables in Part 4.

28. The record of the hearing may be accessed in accordance with the requirements in Part 2, sections 8 to 9.

19. Documents and records in relation to the record of the hearing may be prepared by the defence legal team in accordance with the requirements in Part 2, sections 8 to 11.

Civil proceedings

30. The Attorney-General may make an application to the judge for an order that attributes a national security classification to the record of hearing. The record of the hearing will be stored by the court in accordance with the requirements set out in the tables in Part 4.

31. The record of the hearing may be accessed by the party's legal representative or an unrepresented party in accordance with the requirements set out in Part 2, sections 12 to 15.

32. Documents and records in relation to the record of the hearing may be prepared by the defence legal team, or the party's legal representatives or an unrepresented party in accordance with the requirements in Part 2, sections 12 to 15.

Part 4 Tables

Table 1 Requirements for national security information classified as Restricted

RESTRICTED INFORMATION	Preparation and handling	Removal and accountability
Information is classified as RESTRICTED when the compromise of the information could cause limited damage to national security	***Protective marking*** Centre of top and bottom of each page. Markings should be in capitals, bold text and a minimum of 5 mm high (preferably red). Paragraph classifications, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph.	***Removal of documents or files*** Basis of real need Court staff, legal representatives and parties to civil proceedings, should be satisfied that the person moving the document is aware of the potential risks involved and that the document is in the moving officer's personal custody at all times.
	Numbering Page and/or paragraph numbering desirable. Serial number if in series. ***Filing*** Must be filed in distinctive file cover, standard is blue or buff.	The document should be transported so that its contents cannot be viewed by unauthorised persons. A written record of the movement of material must be maintained in the CDR. Must be returned to secure storage the same day
	Registration Registration in Classified Document Register (CDR) required. A CDR must be kept to record incoming and outgoing classified information. All classified documents are accountable documents and must be registered in the CDR.	***Accounting*** Originating agencies may seek to account for their documents.

RESTRICTED INFORMATION	Preparation and handling	Removal and accountability
	Disclosure/access	
	Need to know.	
	Only in accordance with legislative requirements.	

RESTRICTED INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Copying	***Within a single physical location***	Information must not be created, stored or transmitted electronically (including by telephone, facsimile, video conference, data transmission, e-mail or computer networks) unless the electronic transmission facilities meet the requirements in ACSI 33.
Copying not permitted.	Single opaque envelope that indicates the classification of the information delivered by agency's internal mail system.	
Physical safe-keeping	May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the need to know and there is no opportunity for any unauthorised person to view the information.	
Clear desk policy.		
See Appendix B for requirements.		

RESTRICTED INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Disposal *Note Archives Act 1983* requirements for Commonwealth records, particularly section 24. *Paper waste* Documents held by the legal team or parties to civil proceedings: to be dealt with in accordance with sections 17 to 18 and 23 to 24 in Part 2. Documents held by the prosecution in federal criminal proceedings: to be dealt with in accordance with section 19 in Part 2. In all cases, if documents are to be destroyed, this must be undertaken by two officers cleared to the appropriate level who must supervise the removal of the material to the point of destruction by an approved disposal method, as prescribed in the Commonwealth Protective Security Manual (with specific reference to Class A and Class B shredders) ensure that destruction is complete, sign a destruction certificate and record the destruction in the CDR. *ICT media and equipment* Must undergo sanitisation or destruction in accordance with ACSI 33.	***Transfer within Australia*** Single opaque envelope that does not indicate the classification of the information; receipt at discretion of originator; and one of the following: • passed by hand between people who have the need to know; • delivered by SCEC-endorsed overnight courier. See Appendix A for a summary of the transmission requirements. ***Outside Australia*** No transfer outside Australia. ***Comsec material*** Must be handled in accordance with directions from DSD.	

Table 2 Requirements for national security information classified as Confidential

CONFIDENTIAL INFORMATION	Preparation and handling	Removal and accountability
Information is classified as CONFIDENTIAL when the compromise of the information could cause damage to national security	***Protective marking*** Centre of top and bottom of each page. Markings should be in capitals, bold text and a minimum of 5 mm high (preferably red). Paragraph classifications, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph. ***Numbering*** Page and/or paragraph numbering desirable. Serial number if in series. ***Filing*** Must be filed in distinctive file cover, standard is green. ***Registration*** Registration in Classified Document Register (CDR) required. A CDR must be kept to record incoming and outgoing classified information. All classified documents are accountable documents and must be registered in the CDR. ***Disclosure/access*** Need to know. Only in accordance with legislative requirements.	***Removal of documents or files*** Basis of real need Must be in personal custody of individual and kept in a SCEC-endorsed container (eg a briefcase) Removal must be authorised by the Court officer, legal representatives or party to civil proceedings, responsible for the resource. A written record of the movement of material must be maintained in the CDR. Must be returned to secure storage the same day. ***Accounting*** Originating agencies may seek to account for their documents.

CONFIDENTIAL INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Copying Copying not permitted. ***Physical safe-keeping*** Clear desk policy. See Appendix B for requirements.	***Within a single physical location*** Single opaque envelope that indicates the classification, receipt at discretion of originator, and either: • passed by hand between people who have the appropriate need to know, or • placed in a SCEC-endorsed container (eg a briefcase) and delivered direct, by hand, by an authorised messenger. May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate need to know and there is no opportunity for any unauthorised person to view the information.	Information must not be created, stored or transmitted electronically (including by telephone, facsimile, video conference, data transmission, e-mail or computer networks) unless the electronic transmission facilities meet the requirements in ACSI 33.

CONFIDENTIAL INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Disposal *Note* Archives Act requirements for Commonwealth records, particularly section 24. *Paper waste* Documents held by legal teams or parties to civil proceedings: to be dealt with in accordance with sections 17 to 18 and 23 to 24 in Part 2. Documents held by the prosecution in federal criminal proceedings: to be dealt with in accordance with section 19 in Part 2. In all cases, if documents are to be destroyed, this must be undertaken by two officers cleared to the appropriate level who must supervise the removal of the material to the point of destruction, ensure that destruction is complete, sign a destruction certificate and record the destruction in the CDR. Destruction must occur using only appropriate SCEC-endorsed or ASIO-approved equipment and systems. *ICT media and equipment* Must undergo sanitisation or destruction in accordance with ACSI 33.	***Transfer within Australia*** Either: • single opaque envelope that does not give any indication of the classification and placed in a SCEC-endorsed container (eg a briefcase) and delivered direct, by hand, by an authorised messenger and receipt required, or • double enveloping and receipt required and delivered either by SCEC-endorsed overnight courier or by an alternative approved by ASIO. See Appendix A for a summary of the transmission requirements. ***Outside Australia*** No transfer outside Australia. ***Comsec material*** Must be handled in accordance with directions from DSD.	

Table 3 Requirements for national security information classified as Secret

SECRET INFORMATION	Preparation and handling	Removal and accountability
Information is classified as SECRET when the compromise of the information could cause serious damage to national security	***Protective marking*** Centre of top and bottom of each page. Markings should be in capitals, bold text and a minimum of 5 mm high (preferably red). Paragraph classifications, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph. ***Numbering*** Page numbering essential. Serial number if in series. ***Filing*** Must be filed in distinctive file cover, standard is salmon pink. ***Registration*** Registration in Classified Document Register (CDR) required. A CDR must be kept to record incoming and outgoing classified information. All classified documents are accountable documents and must be registered in the CDR. All incoming documents must be placed without delay in an appropriate file cover. Each incoming document must have both a reference and copy number.	***Removal of documents or files*** Basis of real need Must be in personal custody of individual and kept in a SCEC-endorsed container (eg a briefcase) Removal must be authorised by the Court officer, party to civil proceeding or legal representative responsible for the resource. A written record of the movement of material must be maintained in the CDR. Must be returned to secure storage the same day. ***Accounting*** Originating agencies may seek to account for their documents.

SECRET INFORMATION	Preparation and handling	Removal and accountability
	Disclosure/access Need to know. Only in accordance with legislative requirements.	

SECRET INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Copying Copying not permitted. ***Physical safe-keeping*** Clear desk policy. See Appendix B for requirements.	***Within a single physical location*** Single opaque envelope that indicates the classification, receipt at discretion of originator, and either: • passed by hand between people who have the appropriate need to know, or • placed in a SCEC-endorsed container (eg a briefcase) and delivered direct, by hand, by an authorised messenger. May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate need to know and there is no opportunity for any unauthorised person to view the information.	Information must not be created, stored or transmitted electronically (including by telephone, facsimile, video conference, data transmission, e-mail or computer networks) unless the electronic transmission facilities meet the requirements in ACSI 33.

SECRET INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Disposal *Note Archives Act* requirements for Commonwealth records, particularly section 24. *Paper waste* Documents held by the legal teams or parties to civil proceedings: to be dealt with in accordance with sections 17 to 18 and 23 to 24 in Part 2. Documents held by the prosecution in federal criminal proceedings: to be dealt with in accordance with section 19 in Part 2. In all cases, if documents are to be destroyed, this must be undertaken by two officers cleared to the appropriate level who must supervise the removal of the material to the point of destruction, ensure that destruction is complete, sign a destruction certificate and record the destruction in the CDR. Destruction must occur using only appropriate SCEC-endorsed or ASIO-approved equipment and systems specifically Class A shredders. *ICT media and equipment* Must undergo sanitisation or destruction in accordance with ACSI 33.	***Transfer within Australia*** Double-enveloping required and receipt required and one of the following: • placed in a SCEC-endorsed container (eg a briefcase) and delivered direct by an authorised messenger; • delivered by SCEC-endorsed overnight courier; • delivered by an alternative approved by ASIO. See Appendix A for a summary of the transmission requirements. ***Outside Australia*** No transfer outside Australia. ***Comsec material*** Must be handled in accordance with directions from DSD.	

Table 4 Requirements for national security information classified as Top Secret

TOP SECRET INFORMATION	Preparation and handling	Removal and accountability
Information is classified as TOP SECRET when the compromise of the information could cause exceptionally grave damage to national security	***Protective marking*** Centre of top and bottom of each page. Markings should be in capitals, bold text and a minimum of 5 mm high (preferably red). Paragraph classifications, where adopted, should appear in a consistent position such as in the left margin adjacent to the first letter of the paragraph. ***Numbering*** Page numbering essential. Serial number if in series. Copy number essential. ***Filing*** Must be filed in distinctive file cover, standard is post office red. ***Registration*** Top Secret material must be maintained in a separate Classified Document Register (CDR), controlled only by persons authorised to handle such material. All classified documents are accountable documents and must be registered in the CDR. All incoming documents must be placed without delay in an appropriate file cover. Each incoming document must have both a reference and copy number.	***Removal of documents or files*** Basis of real need Must be in personal custody of individual and kept in a SCEC-endorsed container (eg a briefcase) Removal must be authorised by the Court officer, party to civil proceeding or legal representative responsible for the resource. A written record of the movement of TOP SECRET material must be maintained in the CDR. Must be returned to secure storage the same day. ***Accounting*** Originating agencies may seek to account for their documents.

TOP SECRET INFORMATION	Preparation and handling	Removal and accountability
	Disclosure/access Need to know. Only in accordance with legislative requirements.	

TOP SECRET INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Copying Copying not permitted. ***Physical safe-keeping*** Clear desk policy. See Appendix B for requirements.	***Within a single physical location*** Single opaque envelope that indicates the classification of the information and receipt required, and either: • passed by hand between people who have the appropriate need to know, or • placed in a SCEC-endorsed container (eg a briefcase) and delivered direct, by hand, by an authorised messenger. May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between people with the appropriate need to know and there is no opportunity for any unauthorised person to view the information.	Information must not be created, stored or transmitted electronically (including by telephone, facsimile, video conference, data transmission, e-mail or computer networks) unless the electronic transmission facilities meet the requirements in ACSI 33.

TOP SECRET INFORMATION

Copying, storage and disposal	Manual transmission	Electronic transmission
Disposal *Note* Archives Act requirements for Commonwealth records, particularly section 24. Unless required for Archival purposes, TOP SECRET material should be destroyed as soon as possible after it is no longer required for operational purposes. *Paper waste* Documents held by legal teams or parties to civil proceedings: to be dealt with in accordance with sections 17 to 18 and 23 to 24 in Part 2. Documents held by the prosecution: to be dealt with in accordance with section 19 in Part 2. In all cases, if documents are to be destroyed, this must be undertaken by two officers cleared to the appropriate level who must supervise the removal of the material to the point of destruction, ensure that destruction is complete, sign a destruction certificate and record the destruction in the CDR. Destruction must occur using only appropriate SCEC-endorsed or ASIO-approved equipment and systems. specifically Class A shredders. *ICT media and equipment* Must undergo sanitisation or destruction in accordance with ACSI 33.	***Transfer within Australia*** Double-enveloping required and receipt required and one of the following: • placed in a SCEC-endorsed container (eg a briefcase) and delivered direct, by hand, by an authorised messenger; • delivered by SCEC-endorsed same-day courier; • delivered by SCEC-endorsed safe hand courier. See Appendix A for a summary of the transmission requirements. ***Outside Australia*** No transfer outside Australia. ***Comsec material*** Must be handled in accordance with directions from DSD.	

Appendix A

Requirements for the transfer of paper-based security classified information

Classification of information	Transfer within a single physical location (eg building or complex)	Transfer within Australia
Top Secret	a + i + (either d or e)	c + i + (e, h or k)
Secret	a + j + (either d or e)	c + i + (e, f or g)
Confidential	a + j + (either d or e)	b + i + e or: c + i + (either f or g)
Restricted	a + d	b + j + (either d or f)

Legend

a single opaque envelope that indicates the classification of the information

b single opaque envelope that does not give any indication of the classification

c double enveloping required:

- inner envelope to bear classification of the information enclosed
- inner envelope to be sealed with SCEC-endorsed wafer seals
- inner envelope to be marked 'To be opened only by addressee'
- outer envelope not to bear classification of the information enclosed
- outer envelope to be marked 'safe hand' and 'To be opened only by addressee'

d passed by hand between people who have the appropriate need to know

e placed in a SCEC-endorsed container (eg a briefcase) and delivered direct, by hand, by an authorised messenger

f delivered by SCEC-endorsed overnight courier

g delivered by an alternative approved by ASIO

h delivered by SCEC-endorsed same-day courier

i receipt required

j receipt at discretion of the originator

k delivered by SCEC-endorsed safe hand courier

Note 1 Information, including highly classified information, may be passed uncovered, by hand within a discrete office environment provided that:

- the information is transferred directly between members of staff who have the appropriate need to know; and
- there is no opportunity for any unauthorised person to view the information.

If there is a risk that the information may be viewed by an unauthorised person, it must be covered.

Note 2 Information must not be transferred outside Australia.

Note 3 The transfer of Comsec material must be undertaken in accordance with directions from DSD.

Appendix B

Requirements for security containers and secure rooms for the handling and storage of security classified information within Australia

Classification of information	Secure Area	Partially Secure Area	Intruder Resistant Area
Top Secret	B	A[1]/B[2]	—
Secret	C	B	A
Confidential	C[3]	C	B
Restricted	Agency discretion	Lockable cabinet[4]	Lockable cabinet4

Notes

1. This is the minimum class of container required when guards are used during non-operational hours.
2. This is the minimum class of container required if either an ASIO-approved or SCEC-endorsed intruder alarm system is in use during non-operational hours.
3. Alternatively, a lockable cabinet with a SCEC-endorsed lock is acceptable.
4. A lockable commercial grade cabinet is the minimum requirement in this area.

Appendix C

Explanation of terms

accountable: documents/material information which has been determined by the originator as accountable, requiring both originals and copies to be recorded and accounted for.

ACSI 33: Australian Government Information Technology Security Manual issued by DSD on 31 March 2006. The unclassified version of ACSI 33 covers the protection of Restricted information on ICT systems and is accessible at http://www.dsd.gov.au/library/infosec/acsi33.html. The classified version of ACSI 33 covers the protection of Confidential, Secret and Top Secret information on ICT systems and is available to relevant officers once a need to know has been confirmed.

approved disposal method: consult the PSCC for advice on these methods.

ASIO: Australian Security Intelligence Organisation which obtains, correlates, evaluates and disseminates intelligence about national security. Among other things, it also provides protective security advice and assistance.

Authorised: authorised by the Australian Government.

Caveat: a warning that the information has special requirements in addition to those indicated by the protective marking.

Class A secure room or security container: a secure room or security container that meets ASIO's specifications for a class A room/container. For further information, contact the PSCC.

Class B secure room or security container: a secure room or security container that meets ASIO's specifications for a class B room/container. For further information, contact the PSCC.

Class C secure room or security container: a secure room or security container that meets ASIO's specifications for a class C room/container. For further information, contact the PSCC.

classified document register (CDR): a register that includes details of all documents received with a national security classification and all copies of those documents that have been made. The CDR also records the movement and disposal of those documents. For further information on establishing a classified document register, contact the PSCC.

clear desk policy: a policy that dictates that people must ensure that classified information is secured appropriately when they are absent from the workplace.

Codeword: a word that indicates that the information it covers is in a special need to know category.

Comsec material: material that relates to communications security.

CDPP: Commonwealth Director of Public Prosecutions.

DSD: Defence Signals Directorate, within the Department of Defence.

defence legal team: legal representative(s) of the defendant and any person(s) assisting a legal representative of the defendant.

destruction certificate: instrument certifying that a document has been destroyed in the manner specified in the instrument. For further information, contact the PSCC.

double enveloping: the use of two new opaque envelopes (an inner and an outer envelope) to help protect classified information in transit from unauthorised access and, in the event of unauthorised access, provide evidence of this to the recipient.

ICT: information and communications technology.

intruder resistant area: an area secured so that it is suitable for handling and storing classified information up to and including Secret information. For further information, contact the PSCC.

need to know: the principle that the availability of official information should be limited to those who need to use or access the information to do their work.

originator (of information): the person or agency responsible for preparing or creating official information or for actioning information generated outside the Australian Government. This person or agency is also responsible for deciding whether, and at what level, to security classify that information.

partially secure area: an area that ASIO has certified is suitable for handling and storing classified information up to and including Top Secret information and storing such information in a secure room or security container as set out in Appendix B. For further information, contact the PSCC.

protective marking: an administrative label assigned to security classified information that shows the value of the information, tells users that the information has been security classified and the level of protection that must be provided during use, storage, transmission, transfer and disposal. The protective marking must be in capital letters, bold text, and of a minimum height of 5 mm.

PSCC: Protective Security Coordination Centre, in the Attorney-General's Department.

safe hand: a method of transferring an article in such a way that the article is in the care of an authorised officer or succession of authorised officers who are responsible for its carriage and safekeeping. The purpose of sending an article via safe hand is to establish an audit trail that allows the sender to receive confirmation that the addressee received the information.

Sanitisation: the process of removing certain elements of information that will allow the protective marking that indicates the level of protection required for security classified information to be removed or reduced. This can refer to both electronic media and hard copy information.

SCEC: Security Construction and Equipment Committee chaired by ASIO. SCEC evaluates and endorses security products for use in the protective security environment.

secure area: an area that ASIO has certified is suitable for handling and storing classified information up to and including Top Secret information. For further information, contact the PSCC.

source documents: includes originals of documents and electronic media, with a national security classification, obtained or produced during a federal criminal proceeding.

Note

1. Issued by the Attorney-General's Department on 28 July 2006. This document is available from the Attorney-General's Department or at www.nationalsecurity.gov.au - select the link to the Legislation page, and then select the National Security Information (Criminal and Civil Proceedings) Act 2004 hyperlink.