



Australian Security Intelligence Organisation Act 1979

No. 113, 1979

Compilation No. 80

Compilation date: 4 April 2025

Includes amendments: Act No. 100, 2024

Prepared by the Office of Parliamentary Counsel, Canberra

About this compilation

This compilation

This is a compilation of the *Australian Security Intelligence Organisation Act 1979* that shows the text of the law as amended and in force on 4 April 2025 (the *compilation date*).

The notes at the end of this compilation (the *endnotes*) include information about amending laws and the amendment history of provisions of the compiled law.

Uncommenced amendments

The effect of uncommenced amendments is not shown in the text of the compiled law. Any uncommenced amendments affecting the law are accessible on the Register (www.legislation.gov.au). The details of amendments made up to, but not commenced at, the compilation date are underlined in the endnotes. For more information on any uncommenced amendments, see the Register for the compiled law.

Application, saving and transitional provisions for provisions and amendments

If the operation of a provision or amendment of the compiled law is affected by an application, saving or transitional provision that is not included in this compilation, details are included in the endnotes.

Editorial changes

For more information about any editorial changes made in this compilation, see the endnotes.

Modifications

If the compiled law is modified by another law, the compiled law operates as modified but the modification does not amend the text of the law. Accordingly, this compilation does not show the text of the compiled law as modified. For more information on any modifications, see the Register for the compiled law.

Self-repealing provisions

If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.

Contents

Part I—Preliminary	1
1 Short title.....	1
2 Commencement	1
3 Repeal	1
4 Definitions	1
4AA References to the Attorney-General	10
4A Application of the <i>Criminal Code</i>	10
5 Extension of Act to external Territories	11
5A Copies of certain notices to be given to Inspector-General	11
5B Substitution of references to the Attorney-General	11
Part II—The Organisation and the Director-General	12
6 Continuance of Organisation	12
7 Director-General	12
8 Control of Organisation	12
8A Guidelines	13
9 Term of office of Director-General	15
10 Remuneration and allowances of Director-General.....	15
11 Leave of absence.....	15
12 Resignation	15
13 Termination of appointment	15
14 Acting Director-General	16
15 Appointment of a Judge as Director-General	17
16 Delegation.....	17
Part III—Functions and powers of Organisation	19
Division 1—General	19
17 Functions of Organisation.....	19
17AA Fees for advice and other services	20
17A Act not concerned with lawful dissent etc.	20
18 Communication of intelligence etc.	21
18A Unauthorised dealing with records	24
18B Unauthorised recording of information or matter.....	26
18C Offences against section 18, 18A or 18B—general rules	28
18D Offences against section 18, 18A or 18B—IGIS officials.....	29
19 Co-operation with other authorities in connection with performance of Organisation’s functions	29

19A	Co-operation with intelligence and law enforcement agencies etc. in connection with performance of their functions	30
20	Special responsibility of Director-General in relation to functions of Organisation.....	31
21	Leader of Opposition to be kept informed on security matters	31
21A	Voluntary assistance provided to the Organisation	32
Division 2—Special powers		35
Subdivision A—Preliminary		35
22	Interpretation.....	35
23	Requesting information or documents from operators of aircraft or vessels	38
24	Exercise of authority under warrant etc.....	39
Subdivision B—Search warrants		40
25	Search warrants.....	40
25AA	Conduct of ordinary or frisk search under search warrant.....	45
Subdivision C—Computer access warrants		45
25A	Computer access warrant	45
Subdivision D—Use of surveillance devices		50
26	Issue of surveillance device warrants	50
26A	Requirements for surveillance device warrants	52
26B	What a surveillance device warrant authorises.....	53
26C	Use etc. of listening device without warrant.....	57
26D	Use etc. of optical surveillance device without warrant	57
26E	Use etc. of tracking device without warrant or internal authorisation.....	58
26F	Director-General may determine that certain provisions do not apply to specified ASIO affiliates.....	59
Subdivision DA—Use of tracking devices under internal authorisation		60
26G	Use of tracking devices under internal authorisation.....	60
26H	Requirements for internal authorisations	61
26J	What an internal authorisation authorises.....	62
26K	Certain acts not authorised.....	63
26L	Recovery of tracking devices.....	64
26M	Exercise of authority under internal authorisations	65
26N	Variation of internal authorisations	65
26P	Discontinuance of action before expiration of internal authorisation.....	66
26Q	Register of internal authorisations	67

26R	Issue of warrants for recovery of tracking devices	68
Subdivision E—Inspection of postal and other articles		71
27	Inspection of postal articles	71
27AA	Inspection of delivery service articles	74
Subdivision F—Foreign intelligence		78
27A	Warrants for the performance of functions under paragraph 17(1)(e)	78
27B	Performance of other functions under paragraph 17(1)(e)	83
Subdivision G—Identified person warrants		84
27C	Issue of identified person warrants	84
27D	Authority under identified person warrant—search of premises and persons	86
27E	Authority under identified person warrant—computer access	88
27F	Authority under identified person warrant—surveillance devices	93
27G	Authority under identified person warrant—inspection of postal articles	94
27H	Authority under identified person warrant—inspection of delivery articles.....	96
27J	Authority under identified person warrants—general rules	97
Subdivision H—General provisions relating to warrants and authorisations		99
28	Request for warrant to specify grounds	99
29	Issue of certain warrants by Director-General in emergency	100
29A	Variation of warrants issued under this Division.....	101
30	Discontinuance of action before expiration of warrant	101
31	Certain records obtained under a warrant to be destroyed.....	102
31A	Notification requirements in relation to the use of force under warrant	102
32	Certain action in relation to requests and warrants.....	103
33	Relationship with other laws.....	104
34	Director-General to report to Attorney-General—general	105
34AAA	Director-General to report to Attorney-General— concealment of access.....	106
34AAB	Director-General to report to Attorney-General—internal authorisations to use tracking devices	107
34AAC	Evidentiary certificates	108

Subdivision J—Assistance relating to access to data	110
34AAD Person with knowledge of a computer or a data storage device to assist access to data	110
Division 3—Compulsory questioning powers	115
Subdivision A—General provisions	115
34A Definitions	115
34AA Meaning of <i>minor’s representative</i>	122
34AB Meaning of <i>questioning material</i> and <i>subject</i>	123
34AC Meaning of <i>resolved</i>	124
34AD Prescribed authorities.....	125
34AE Status of prescribed authorities.....	128
34AF Written statement of procedures	128
34AG Humane treatment of subject of questioning warrant.....	129
Subdivision B—Questioning warrants	129
34B Request for questioning warrant	129
34BA Test for issue of questioning warrant—persons who are at least 18	131
34BB Test for issue of questioning warrant—persons who are at least 14	132
34BC Warrant has no effect if person under 14.....	134
34BD What a questioning warrant authorises.....	134
34BE Other things that may be authorised in questioning warrant	136
34BF Requirements for questioning warrant.....	139
34BG Variation of questioning warrant	140
34BH Notification requirements in relation to questioning warrant.....	142
Subdivision C—Apprehension and search powers etc.	144
34C Police officer may apprehend subject of questioning warrant in certain circumstances.....	144
34CA Entering premises to apprehend subject	146
34CB Communications while apprehended.....	146
34CC Power to conduct search of apprehended subject of questioning warrant.....	147
34CD Use of force in apprehending or searching subject.....	149
34CE Power to remove, retain and copy materials etc.	149
Subdivision D—Matters relating to questioning under questioning warrants	150
34D Screening of persons.....	150
34DA Prohibition on possessing certain things during questioning.....	153
34DB Questioning under a questioning warrant	154

34DC	Prescribed authority must explain certain matters.....	154
34DD	Additional requirements for prescribed authorities in relation to minor questioning warrants	156
34DE	Directions while subject is before prescribed authority for questioning.....	157
34DF	Directions in relation to confidentiality	159
34DG	Direction that persons under 14 not be questioned.....	161
34DH	Other matters relating to the functions and powers of prescribed authorities.....	161
34DI	Complaints while appearing before prescribed authority for questioning.....	161
34DJ	Permitted questioning time	162
34DK	Extra permitted questioning time if interpreter present.....	164
34DL	Time that is not questioning time	166
34DM	Suspension of questioning etc. in response to concern of Inspector-General of Intelligence and Security	166
34DN	Interpreter provided at request of prescribed authority	167
34DO	Interpreter provided at request of subject	168
34DP	Video recording of procedures	169
Subdivision E—Particular uses or disclosures of questioning material and derivative material		169
34E	Obtaining derivative material	169
34EA	Disclosing questioning material to prosecutors of the subject	170
34EB	Disclosing derivative material to prosecutors of the subject	171
34EC	Court’s powers to order disclosure and to ensure a fair trial	172
34ED	Certain material may always be disclosed to prosecutors of the subject	173
34EE	Other matters about prosecutors and subjects.....	174
34EF	Proceeds of crime authorities and questioning under a questioning warrant.....	175
Subdivision F—Lawyers and minor’s representatives		176
34F	Person specified in warrant may contact lawyer or minor’s representative.....	176
34FA	Questioning in absence of lawyer for subject.....	177
34FB	Directions in relation to lawyers for subjects of adult questioning warrants.....	178
34FC	Directions in relation to lawyers for subjects of minor questioning warrants.....	180
34FD	Directions in relation to minor’s representatives.....	182
34FE	Lawyer may request copy of warrant	184

34FF	Involvement of lawyers	185
34FG	Conduct of minor's representatives	187
34FH	Lawyers' access to information for proceedings relating to warrant	189
34FI	Law relating to legal professional privilege not affected	189
Subdivision G—Offences		189
34G	Surrender of travel documents by person in relation to whom questioning warrant is sought	189
34GA	Person in relation to whom questioning warrant is requested must not leave Australia without permission.....	191
34GB	Surrender of travel documents by subject of questioning warrant	192
34GC	Subject of questioning warrant must not leave Australia without permission.....	193
34GD	Giving information and producing things etc.	194
34GE	Offences of contravening safeguards.....	197
34GF	Secrecy relating to warrants and questioning	199
Subdivision H—Complaints, reporting and records		205
34H	Complaints and information about contravention of procedural statement.....	205
34HA	Providing reports to the Attorney-General	206
34HB	Providing information to the Inspector-General.....	207
34HC	Destruction of certain records obtained under warrant.....	207
Subdivision I—Miscellaneous		208
34J	Discontinuance of action before cessation of warrant	208
34JA	Certain functions and powers not affected	208
34JB	IGIS official may be present at questioning or apprehension.....	208
34JC	Rules of Court about proceedings connected with warrants.....	209
34JD	Jurisdiction of State and Territory courts excluded	209
34JE	Financial assistance.....	209
34JF	Cessation of effect of Division	210
Division 4—Special intelligence operations		211
35A	Relationship to other laws and matters	211
35B	Applications for authorities to conduct special intelligence operations.....	211
35C	Granting of special intelligence operation authorities	212
35D	Contents of special intelligence operation authorities	213
35E	Commencement and duration of special intelligence operation authorities	214

35F	Variation of special intelligence operation authorities	214
35G	Cancellation of special intelligence operation authorities	216
35H	Effect of special intelligence operation authorities.....	216
35J	Defect in a special intelligence operation authority.....	217
35K	Immunity from liability for special intelligence conduct during special intelligence operations.....	217
35L	Requirements for warrants etc. not affected	218
35M	Effect of being unaware of variation or cancellation of special intelligence operation authority	218
35N	Protection from criminal responsibility for certain ancillary conduct.....	219
35P	Unauthorised disclosure of information	220
35PA	Notifications by Director-General	223
35Q	Reports by the Director-General.....	223
35R	Evidence relating to granting of special intelligence operation authority	224
Part IV—Security assessments		225
Division 1—Preliminary		225
35	Interpretation.....	225
36AA	Prescribing actions as <i>prescribed administrative action</i>	229
36	Part not to apply to certain assessments.....	230
36A	Part not to apply to security vetting and security clearance related activities	232
Division 2—Furnishing of security assessments		233
37	Security assessments.....	233
38	Person to be notified of assessment	234
39	Effect of preliminary advice by Organisation.....	235
40	Assessments and preliminary communications for State purposes	236
41	Notification of delayed security assessment.....	238
42	Protocol for dealing with delayed security assessments	239
Division 4—Review of security assessments		241
54	Applications to Tribunal	241
61	Effect of findings	241
64	Restriction on further assessments after review	241
65	Reference of certain matters to Tribunal by Attorney-General	241
81	Secrecy.....	243

Part IVA—Security vetting and security clearance related activities	244
Division 1—Preliminary	244
82 Purpose of this Part	244
82A Definitions	244
82B Simplified outline of this Part.....	246
Division 2—Security vetting and security clearance related decisions	248
82C Security vetting and security clearance related activities	248
82D Director-General’s powers, functions and duties	249
82E Communications by Organisation to another Commonwealth security vetting agency	250
82F Communications by Organisation to State security vetting agency	250
82G Statement of grounds for prejudicial security clearance suitability assessments	252
82GA Notification of delayed security clearance decision or delayed security clearance suitability assessment	253
82GB Protocol for dealing with delayed security clearance decisions and delayed security clearance suitability assessments	254
Division 3—Review of certain security clearance decisions and prejudicial security clearance suitability assessments	257
Subdivision A—Internal review of certain security clearance decisions	257
82H Internally reviewable decisions	257
82J Notification of internally reviewable decision.....	258
82K Application for internal review of decision	259
82L Decision on internal review	259
Subdivision B—Review by the Administrative Review Tribunal of certain security clearance decisions and security clearance suitability assessments	262
83 Externally reviewable decisions	262
83A Notification of prejudicial security clearance suitability assessment that is an externally reviewable decision	264
83B Applications to Administrative Review Tribunal.....	266
83C Statement of grounds for security clearance decision	266

83CA	Access to security clearance standards	268
83D	Effect of findings	269
83E	Conclusive certificates.....	269
Subdivision C—Review by an independent reviewer		270
83EA	Independently reviewable decisions	270
83EB	Application for independent review of decision.....	272
83EC	Director-General to provide information to independent reviewer	272
83ED	Independent review of decision	274
83EE	Director-General’s consideration of independent reviewer’s opinion	275
83EF	Attorney-General may engage independent reviewers	276
Division 4—Other matters relating to review by the Administrative Review Tribunal		277
83F	Reference of certain matters to Administrative Review Tribunal by Attorney-General	277
Part V—ASIO employees etc.		279
84	Employees of the Organisation.....	279
85	Consultants and contractors	279
86	Secondment of ASIO employees.....	280
87	Secondment of persons to the Organisation	280
88	Applicability of principles of the <i>Public Service Act 1999</i>	280
89	Voluntary moves to APS	281
90	Regulations relating to employment of persons	281
91	Application of Crimes Act.....	281
92	Making public the identity of ASIO employees and ASIO affiliates	282
92A	Disclosing the identity of ASIO employees and ASIO affiliates	283
92B	Cover employment for ASIO employees and ASIO affiliates	285
92C	Cover employment—determining a specified authority of the Commonwealth.....	285
92D	Protection from criminal liability—third parties	287
Part VI—Miscellaneous		289
93A	Costs in certain ART reviews	289
93	Offences	289
94	Annual report	290
95	Regulations	295

Endnotes	296
Endnote 1—About the endnotes	296
Endnote 2—Abbreviation key	298
Endnote 3—Legislation history	299
Endnote 4—Amendment history	314

An Act relating to the Australian Security Intelligence Organisation

Part I—Preliminary

1 Short title

This Act may be cited as the *Australian Security Intelligence Organisation Act 1979*.

2 Commencement

This Act shall come into operation on a date to be fixed by Proclamation.

3 Repeal

The *Australian Security Intelligence Organisation Act 1956* and the *Australian Security Intelligence Organisation Act 1976* are repealed.

4 Definitions

In this Act, unless the contrary intention appears:

activities prejudicial to security includes any activities concerning which Australia has responsibilities to a foreign country as referred to in paragraph (b) of the definition of ***security*** in this section.

acts of foreign interference means activities relating to Australia that are carried on by or on behalf of, are directed or subsidised by or are undertaken in active collaboration with, a foreign power, being activities that:

- (a) are clandestine or deceptive and:
 - (i) are carried on for intelligence purposes;

Section 4

- (ii) are carried on for the purpose of affecting political or governmental processes; or
 - (iii) are otherwise detrimental to the interests of Australia; or
- (b) involve a threat to any person.

AGO has the meaning given by the *Intelligence Services Act 2001*.

ASD has the meaning given by the *Intelligence Services Act 2001*.

ASIO affiliate means a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 and a person performing services under an agreement under section 87, but does not include the Director-General or an ASIO employee.

ASIO employee means a person employed under section 84 or 90.

ASIS has the meaning given by the *Intelligence Services Act 2001*.

attacks on Australia's defence system means activities that are intended to, and are likely to, obstruct, hinder or interfere with the performance by the Defence Force of its functions or with the carrying out of other activities by or for the Commonwealth for the purposes of the defence or safety of the Commonwealth.

Australia, when used in a geographical sense, includes the external Territories.

Australian travel document has the same meaning as in the *Australian Passports Act 2005*.

authority of a State:

- (a) in Part IV—has the meaning given by subsection 35(1); and
- (aa) in Part IVA—has the meaning given by section 82A; and
- (b) otherwise—includes:
 - (i) a Department of State of a State, or a Department of the Public Service of a State; and
 - (ii) a body, whether incorporated or not, established for public purposes by or under a law of a State; and

- (iii) a body corporate in which a State or a body referred to in subparagraph (ii) has a controlling interest.

authority of the Commonwealth includes:

- (a) a Department of State or an Agency within the meaning of the *Public Service Act 1999*;
- (aa) a Department within the meaning of the *Parliamentary Service Act 1999*;
- (b) the Defence Force;
- (c) a body, whether incorporated or not, established for public purposes by or under a law of the Commonwealth or of a Territory;
- (d) the holder of an office established for public purposes by or under a law of the Commonwealth or of a Territory;
- (e) a prescribed body established in relation to public purposes that are of concern to the Commonwealth and any State or States; and
- (f) a body corporate in which the Commonwealth or a body referred to in paragraph (c) has a controlling interest.

carriage service provider has the same meaning as in the *Telecommunications Act 1997*.

carrier has the same meaning as in the *Telecommunications Act 1997*.

certified copy means:

- (a) in relation to a warrant—a copy of the warrant that has been certified in writing by the Director-General or a Deputy Director-General to be a true copy of the warrant; or
- (b) in relation to an authorisation under section 27G—a copy of the authorisation that has been certified in writing by the Director-General or a Deputy Director-General to be a true copy of the authorisation; or
- (c) in relation to an instrument varying or revoking a warrant or an authorisation under section 27G—a copy of the instrument that has been certified in writing by the Director-General or a Deputy Director-General to be a true copy of the instrument.

Section 4

Committee on Intelligence and Security means the Parliamentary Joint Committee on Intelligence and Security established under the *Intelligence Services Act 2001*.

Commonwealth agency means a Minister or an authority of the Commonwealth.

computer means all or part of:

- (a) one or more computers; or
- (b) one or more computer systems; or
- (c) one or more computer networks; or
- (d) any combination of the above.

data storage device means a thing (for example, a disk or file server) containing (whether temporarily or permanently), or designed to contain (whether temporarily or permanently), data for use by a computer.

Defence Department means the Department of State that deals with defence and that is administered by the Minister administering section 1 of the *Defence Act 1903*.

Defence Minister means the Minister administering section 1 of the *Defence Act 1903*.

Deputy Director-General means a person who holds, or is acting in, a position known as Deputy Director-General of Security.

Director-General means the Director-General of Security holding office under this Act.

engage in conduct has the same meaning as in the *Criminal Code*.

entrusted person means:

- (a) an ASIO employee; or
- (b) an ASIO affiliate; or
- (c) a person who has entered into a contract, agreement or arrangement with ASIO (other than as an ASIO affiliate).

Foreign Affairs Minister means the Minister administering the *Diplomatic Privileges and Immunities Act 1967*.

foreign intelligence means intelligence about the capabilities, intentions or activities of people or organisations outside Australia.

foreign power means:

- (a) a foreign government;
- (b) an entity that is directed or controlled by a foreign government or governments; or
- (c) a foreign political organisation.

frisk search means:

- (a) a search of a person conducted by quickly running the hands over the person's outer garments; and
- (b) an examination of anything worn or carried by the person that is conveniently and voluntarily removed by the person.

IGIS official (short for Inspector-General of Intelligence and Security official) means:

- (a) the Inspector-General of Intelligence and Security; or
- (b) any other person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*.

intelligence or security agency means any of the following:

- (a) the Australian Secret Intelligence Service;
- (aa) the Australian Signals Directorate;
- (b) the Office of National Intelligence;
- (c) that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation;
- (d) that part of the Defence Department known as the Defence Intelligence Organisation.

intercept a communication passing over a telecommunications system has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

Judge means a Judge of a court created by the Parliament.

Section 4

law enforcement agency means an authority of the Commonwealth, or an authority of a State, that has functions relating to law enforcement.

ONI means the Office of National Intelligence.

ordinary search means a search of a person or of articles on his or her person that may include:

- (a) requiring the person to remove his or her overcoat, coat or jacket and any gloves, shoes and hat; and
- (b) an examination of those items.

Organisation means the Australian Security Intelligence Organisation.

participant in a special intelligence operation means a person who is authorised under Division 4 of Part III to engage in special intelligence conduct for the purposes of the special intelligence operation.

permanent resident means a person:

- (a) in the case of a natural person:
 - (i) who is not an Australian citizen;
 - (ii) whose normal place of residence is situated in Australia;
 - (iii) whose presence in Australia is not subject to any limitation as to time imposed by law; and
 - (iv) who is not an unlawful non-citizen within the meaning of the *Migration Act 1958*; or
- (b) in the case of a body corporate:
 - (i) which is incorporated under a law in force in a State or Territory; and
 - (ii) the activities of which are not controlled (whether directly or indirectly) by a foreign power.

politically motivated violence means:

- (a) acts or threats of violence or unlawful harm that are intended or likely to achieve a political objective, whether in Australia or elsewhere, including acts or threats carried on for the

purpose of influencing the policy or acts of a government, whether in Australia or elsewhere; or

(b) acts that:

(i) involve violence or are intended or are likely to involve or lead to violence (whether by the persons who carry on those acts or by other persons); and

(ii) are directed to overthrowing or destroying, or assisting in the overthrow or destruction of, the government or the constitutional system of government of the Commonwealth or of a State or Territory; or

(ba) acts that are offences punishable under Subdivision A of Division 72, or Part 5.3, of the *Criminal Code*; or

(c) acts that are offences punishable under Division 119 of the *Criminal Code*, the *Crimes (Hostages) Act 1989* or Division 1 of Part 2, or Part 3, of the *Crimes (Ships and Fixed Platforms) Act 1992* or under Division 1 or 4 of Part 2 of the *Crimes (Aviation) Act 1991*; or

(d) acts that:

(i) are offences punishable under the *Crimes (Internationally Protected Persons) Act 1976*; or

(ii) threaten or endanger any person or class of persons specified by the Minister for the purposes of this subparagraph by notice in writing given to the Director-General.

promotion of communal violence means activities that are directed to promoting violence between different groups of persons in the Australian community so as to endanger the peace, order or good government of the Commonwealth.

retained data has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

Section 4

security means:

- (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
 - (i) espionage;
 - (ii) sabotage;
 - (iii) politically motivated violence;
 - (iv) promotion of communal violence;
 - (v) attacks on Australia's defence system; or
 - (vi) acts of foreign interference;whether directed from, or committed within, Australia or not; and
- (aa) the protection of Australia's territorial and border integrity from serious threats; and
- (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

security clearance decision means a decision to do any of the following:

- (a) grant a security clearance to a person;
- (b) deny a security clearance in respect of a person;
- (c) impose, vary or remove conditions on a security clearance in respect of a person;
- (d) suspend a security clearance, or revoke a suspension of a security clearance, held by a person;
- (e) revoke a security clearance held by a person.

Note: See also subsection 82L(4) in relation to a decision of an internal reviewer (within the meaning of Part IVA).

security clearance suitability assessment means a statement in writing that:

- (a) is furnished by the Organisation; and
- (b) is about a person's suitability to hold a security clearance (with or without conditions imposed in respect of the security clearance) that has been, or may be, granted by another

security vetting agency (within the meaning of Part IVA);
and

- (c) expressly states that it is a security clearance suitability assessment for the purposes of paragraph 82C(1)(d).

seizable item means anything that could present a danger to a person or that could be used to assist a person to escape from lawful custody.

senior position-holder means an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is:

- (a) equivalent to or higher than a position occupied by an SES employee; or
(b) known as Coordinator.

serious crime means conduct that, if engaged in within, or in connection with, Australia, would constitute an offence against the law of the Commonwealth, a State or a Territory punishable by imprisonment for a period exceeding 12 months.

special intelligence conduct means conduct for or in relation to which a person would, but for section 35K, be subject to civil or criminal liability under a law of the Commonwealth, a State or a Territory.

special intelligence function means a function of the Organisation under paragraph 17(1)(a), (b), (e) or (f).

special intelligence operation is an operation:

- (a) in relation to which a special intelligence operation authority has been granted; and
(b) that is carried out for a purpose relevant to the performance of one or more special intelligence functions; and
(c) that may involve an ASIO employee or an ASIO affiliate in special intelligence conduct.

special intelligence operation authority means an authority to conduct a special intelligence operation granted under section 35C.

Section 4AA

staff member of a body (however described) includes:

- (a) the head (however described) of the body, or another person who holds an office or appointment in relation to the body; and
- (b) a person who is otherwise a member of the staff of the body (whether an employee of the body, a consultant or contractor to the body, or a person who is made available by an authority of the Commonwealth, an authority of a State, or other person, to perform services for the body).

State includes the Australian Capital Territory and the Northern Territory.

strip search means a search of a person or of articles on his or her person that may include:

- (a) requiring the person to remove all of his or her garments; and
- (b) an examination of the person's body (but not of the person's body cavities) and of those garments.

Territory does not include the Australian Capital Territory or the Northern Territory.

violence includes the kidnapping or detention of a person.

4AA References to the Attorney-General

Despite subsection 19(1) of the *Acts Interpretation Act 1901*, a reference in this Act to the Attorney-General is a reference only to the Minister with that title.

Note: A reference in this Act to the Attorney-General may include a reference to a person acting as the Attorney-General: see subsection 19(4) of the *Acts Interpretation Act 1901*.

4A Application of the *Criminal Code*

Chapter 2 of the *Criminal Code* (except Part 2.5) applies to all offences against this Act.

Note: Chapter 2 of the *Criminal Code* sets out the general principles of criminal responsibility.

5 Extension of Act to external Territories

This Act extends to every external Territory.

5A Copies of certain notices to be given to Inspector-General

Where the Minister gives a notice in writing to the Director-General for the purposes of subparagraph (d)(ii) of the definition of *politically motivated violence* in section 4, the Minister shall give a copy of the notice to the Inspector-General of Intelligence and Security.

5B Substitution of references to the Attorney-General

Unless the Prime Minister is satisfied that exceptional circumstances exist, the Governor-General must not make a substituted reference order under subsection 19B(2) of the *Acts Interpretation Act 1901* that relates to a provision of this Act (other than section 34JE) that refers to the Attorney-General.

Part II—The Organisation and the Director-General

6 Continuance of Organisation

The Australian Security Intelligence Organisation, being the Organisation that was continued in existence by the Acts repealed by this Act, is continued in existence.

7 Director-General

- (1) There shall be a Director-General of Security, who shall be appointed by the Governor-General and shall hold office, subject to this Act, on such terms and conditions as the Governor-General determines.
- (2) Before a recommendation is made to the Governor-General for the appointment of a person as Director-General, the Prime Minister shall consult with the Leader of the Opposition in the House of Representatives.

8 Control of Organisation

- (1) The Organisation shall be under the control of the Director-General.
- (2) Subject to subsections (4) and (5), in the performance of the Director-General's functions under this Act, the Director-General is subject to the directions of the Minister.
- (3) If the Director-General requests that a direction of the Minister be put in writing, the Minister shall comply with the request.
- (4) The Minister is not empowered to override the opinion of the Director-General concerning the nature of the advice that should be given by the Organisation.

- (5) The Minister is not empowered to override the opinion of the Director-General:
- (a) on the question whether the collection of intelligence by the Organisation concerning a particular individual would, or would not, be justified by reason of its relevance to security; or
 - (b) on the question whether a communication of intelligence concerning a particular individual would be for a purpose relevant to security;
- except by a direction contained in an instrument in writing that sets out the Minister's reasons for overriding the opinion of the Director-General.
- (6) The Minister shall, as soon as practicable after giving a direction in writing to the Director-General, cause a copy of the direction to be given to the Inspector-General of Intelligence and Security and, if the direction relates to a question referred to in subsection (5), to the Prime Minister.
- (7) Where intelligence is collected or communicated pursuant to a direction referred to in subsection (5), the Director-General shall cause a record in writing to be kept of the intelligence so collected or communicated.

8A Guidelines

- (1) The Minister may, from time to time, by written notice given to the Director-General, give to the Director-General guidelines to be observed:
- (a) in the performance by the Organisation of its functions or the exercise of its powers; or
 - (b) in the exercise by the Director-General of his or her powers under sections 84, 85, 86 and 87.
- (1A) Before making guidelines under subsection (1), the Minister must consult with the Attorney-General.

Section 8A

- (2) The Minister shall, as soon as practicable after the commencement of this section, by notice in writing given to the Director-General, give to the Director-General guidelines to be observed in relation to the performance of that part of the Organisation's functions that relates to politically motivated violence, and may, from time to time, vary or replace guidelines so given.
- (2A) Before varying or replacing guidelines given under subsection (2), the Minister must consult with the Attorney-General.
- (3) Subject to subsection (4), the Minister shall cause a copy of any guidelines given under subsection (1) or (2) to be laid before each House of the Parliament within 15 sitting days of that House after the guidelines were given.
- (4) Where the laying of a copy of guidelines before the Parliament in accordance with subsection (3) would result in the disclosure of information that would, in the opinion of the Minister, be contrary to the public interest by reason that it would prejudice security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs or the privacy of individuals, the Minister may cause a copy of the guidelines to be laid before each House of the Parliament with such deletions as the Minister thinks necessary to avoid that result or decline to cause a copy to be laid before each House of the Parliament.
- (5) The Minister shall, in accordance with arrangements made between the Minister and the Leader of the Opposition in the House of Representatives, make available to the Leader of the Opposition a copy of any guidelines given under subsection (1) or (2), but it is the duty of the Leader of the Opposition to treat as secret any part of those guidelines that has not been laid before a House of the Parliament.
- (6) The Minister shall, as soon as practicable after guidelines under subsection (1) or (2) are given to the Director-General, give a copy of the guidelines to the Inspector-General of Intelligence and Security and, unless the Minister considers it inappropriate to do so, to the Committee on Intelligence and Security.

9 Term of office of Director-General

- (1) Subject to sections 12 and 13, the Director-General holds office for such period, not exceeding 7 years, as is specified in his or her instrument of appointment, but is eligible for re-appointment.

10 Remuneration and allowances of Director-General

- (1) The Director-General shall be paid such remuneration as is determined by the Remuneration Tribunal but, if no determination of that remuneration by the Tribunal is in operation, he or she shall be paid such remuneration as is prescribed.
- (2) The Director-General shall be paid such allowances as are prescribed.
- (3) This section has effect subject to the *Remuneration Tribunal Act 1973* and to section 15.

11 Leave of absence

- (1) The Director-General has such recreation leave entitlements as are determined by the Remuneration Tribunal.
- (2) The Minister may grant the Director-General leave of absence, other than recreation leave, on such terms and conditions as to remuneration or otherwise as the Minister determines.

12 Resignation

The Director-General may resign from office by writing signed by the Director-General and delivered to the Governor-General.

13 Termination of appointment

- (1) The Governor-General may terminate the appointment of the Director-General by reason of physical or mental incapacity, misbehaviour or failure to comply with a provision of this Act.
- (2) If the Director-General:

Section 14

- (a) is absent from duty, except with leave of absence, for 14 consecutive days or for 28 days in any 12 months; or
- (b) becomes bankrupt, applies to take the benefit of any law for the relief of bankrupt or insolvent debtors, compounds with his or her creditors or makes an assignment of his or her remuneration for their benefit;

the Governor-General shall terminate his or her appointment.

14 Acting Director-General

- (1) The Minister may appoint a person to act as Director-General:
 - (a) during a vacancy in the office of Director-General; or
 - (b) during any period, or during all periods, when the Director-General is absent from duty or from Australia or is, for any reason, unable to perform the functions of his or her office;but a person appointed to act during a vacancy shall not continue so to act for more than 12 months.
- (2) Before a recommendation is made to the Minister for the appointment of a person, under subsection (1), to act as Director-General, the Prime Minister shall consult with the Leader of the Opposition in the House of Representatives, unless it is impracticable to do so.
- (3) An appointment of a person under subsection (1) may be expressed to have effect only in such circumstances as are specified in the instrument of appointment.
- (4) The Minister may:
 - (a) determine the terms and conditions of appointment, including remuneration and allowances, of a person acting as Director-General; and
 - (b) at any time terminate such an appointment.
- (5) Where a person is acting as Director-General in accordance with paragraph (1)(b) and the office of Director-General becomes vacant while that person is so acting, that person may continue so

to act until the Minister otherwise directs, the vacancy is filled or a period of 12 months from the date on which the vacancy occurred expires, whichever first happens.

- (6) The appointment of a person to act as Director-General ceases to have effect if the person resigns the appointment by writing signed by the person and delivered to the Minister.
- (7) While a person is acting as Director-General, he or she has, and may exercise, all the powers and shall perform all the functions of the Director-General.

15 Appointment of a Judge as Director-General

- (1) The appointment of a Judge as Director-General, or service of a Judge as Director-General, does not affect the tenure of his or her office as a Judge or his or her rank, title, status, precedence, salary, annual or other allowances or other rights or privileges as the holder of his or her office as a Judge and, for all purposes, his or her service as Director-General shall be taken to be service as the holder of his or her office as a Judge.
- (2) Subject to subsection (3), if the Director-General is a Judge, he or she shall be paid salary at such rate (if any), and an annual allowance at such rate (if any), as are fixed from time to time by the Parliament.
- (3) If the Director-General is a Judge, he or she is not, while he or she receives salary or annual allowance as a Judge, entitled to salary or annual allowance, as the case may be, under this Act, except to the extent (if any) that the salary or annual allowance that would be payable to him or her under this Act apart from this subsection exceeds the salary or annual allowance payable to him or her as a Judge.

16 Delegation

- (1) Subject to subsection 92C(8), the Director-General may, by signed writing, delegate to a person any of the Director-General's powers,

Section 16

functions or duties under or for the purposes of this Act that relate to:

- (a) the management of ASIO employees or ASIO affiliates; or
- (b) the financial management of the Organisation.

Note: For further provisions relating to delegations, see sections 34AA, 34AB and 34A of the *Acts Interpretation Act 1901*.

(1A) The Director-General may, by writing, delegate any or all of the Director-General's functions or powers under section 21A to a senior position-holder.

(1B) Subject to subsection (1C), the Director-General may, by writing, delegate any or all of the Director-General's powers and functions under subsection 82D(1) to a person who is an ASIO employee or an ASIO affiliate.

Note: Subsection 82D(1) provides that the Director-General may, on behalf of the Organisation, exercise the powers or perform the functions of the Organisation under Part IVA.

(1C) The Director-General may delegate the power or function under subsection 82D(1) to:

- (a) make a security clearance decision under paragraph 82C(1)(b); or
 - (b) furnish a security clearance suitability assessment under paragraph 82C(1)(d) that is a prejudicial security clearance suitability assessment (within the meaning of Part IVA);
- only to an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than an Executive Level 1 position.

Note: The Director-General may, under subsection (1B), delegate the power or function under subsection 82D(1) to furnish a security clearance suitability assessment under paragraph 82C(1)(d) that is not a prejudicial security clearance suitability assessment.

(2) In exercising powers, performing functions or discharging duties under a delegation, the delegate must comply with any written direction given by the Director-General to the delegate.

Part III—Functions and powers of Organisation

Division 1—General

17 Functions of Organisation

- (1) The functions of the Organisation are:
- (a) to obtain, correlate and evaluate intelligence relevant to security; and
 - (b) for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes; and
 - (c) to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities; and
 - (ca) to furnish security assessments and make preliminary communications to a State or an authority of a State in accordance with paragraphs 40(1)(b) and (1A)(a); and
 - (cb) to undertake security vetting and security clearance related activities in accordance with Part IVA; and
 - (d) to advise Ministers, authorities of the Commonwealth and such other persons as the Minister, by notice in writing given to the Director-General, determines on matters relating to protective security; and
 - (e) to obtain within Australia foreign intelligence pursuant to section 27A or 27B of this Act or section 11A, 11B or 11C of the *Telecommunications (Interception and Access) Act 1979*, and to communicate any such intelligence in accordance with this Act or the *Telecommunications (Interception and Access) Act 1979*; and
 - (f) to co-operate with and assist bodies referred to in section 19A in accordance with that section.

Section 17AA

Note: The Organisation's function referred to in paragraph (cb) does not limit the capacity of any other authority of the Commonwealth to undertake the kinds of activities referred to in that paragraph.

- (2) It is not a function of the Organisation to carry out or enforce measures for security within an authority of the Commonwealth.

17AA Fees for advice and other services

- (1) The Director-General may determine in writing that fees are payable by persons for the giving of advice or the provision of services by the Organisation to the persons at their request.
- (2) Unless the Director-General determines otherwise, the Organisation may refuse to give the advice, or provide the service, to a person until the fee is paid in whole or part. If the whole or part of the fee is not paid before the advice is given or the service is provided, the amount concerned is a debt due to the Commonwealth and may be recovered by the Commonwealth in a court of competent jurisdiction.
- (3) The amount of the fee must not exceed the reasonable costs to the Organisation of giving the advice or providing the service.
- (4) The Director-General may, on application in writing by a person who is or will be required to pay a fee, if the Director-General considers it appropriate in the circumstances:
- (a) not require the person to pay any of the fee; or
 - (b) require the person to pay only a specified part of the fee.

17A Act not concerned with lawful dissent etc.

This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.

18 Communication of intelligence etc.

Who may communicate intelligence

- (1) The communication of intelligence on behalf of the Organisation shall be made only by the Director-General or by a person acting within the limits of authority conferred on the person by the Director-General.

Offence for unauthorised communication of information or matter

- (2) A person commits an offence if:
- (a) the person makes a communication of any information or matter; and
 - (b) the information or matter has come to the knowledge or into the possession of the person by reason of:
 - (i) his or her being, or having been, an ASIO employee; or
 - (ii) his or her being, or having been, an ASIO affiliate; or
 - (iii) his or her having entered into a contract, agreement or arrangement with ASIO (otherwise than as an ASIO affiliate); and
 - (c) the information or matter:
 - (i) was acquired or prepared by or on behalf of the Organisation in connection with its functions; or
 - (ii) relates to the performance by the Organisation of its functions; and
 - (d) the communication was not made to the Director-General, an ASIO employee or an ASIO affiliate:
 - (i) by an ASIO employee, in the course of the ASIO employee's duties; or
 - (ii) by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation; or
 - (iii) by a person who has entered into a contract, agreement or arrangement with ASIO (otherwise than as an ASIO

Section 18

affiliate), in accordance with the contract, agreement or arrangement; and

- (e) the communication was not made by a person acting within the limits of authority conferred on the person by the Director-General; and
- (f) the communication was not made with the approval of the Director-General or of a person having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 10 years.

Exception—information or matter lawfully available

- (2A) Subsection (2) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

Exception—IGIS officials

- (2B) Subsection (2) does not apply if the person communicates the information or matter to an IGIS official for the purpose of the IGIS official exercising a power, or performing a function or duty, as an IGIS official.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2B) (see subsection 13.3(3) of the *Criminal Code*).

Communicating information to appropriate authorities of the Commonwealth or a State

- (3) A person referred to in subsection (1) may communicate information to a person referred to in subsection (4) if:
 - (a) the information has come into the possession of the Organisation in the course of performing the Organisation's functions under section 17; and
 - (b) either:

- (i) the information relates, or appears to relate, to the commission, or intended commission, of a serious crime; or
- (ii) the Director-General, or a person authorised for the purpose by the Director-General, is satisfied that the national interest requires the communication; and
- (c) the information relates, or appears to relate, to the performance of the functions, responsibilities or duties of the person referred to in subsection (4).

Note: There are additional restrictions, in the *Telecommunications (Interception and Access) Act 1979*, on communicating telecommunications information.

- (4) The persons to whom information may be communicated under subsection (3) are the following:
 - (a) a Minister;
 - (b) a staff member of an authority of the Commonwealth;
 - (c) a staff member of an authority of a State.

Communicating information to ASIS, ASD and AGO

- (4A) A person referred to in subsection (1) may communicate information to a staff member of ASIS, ASD or AGO if:
 - (a) the information has come into the possession of the Organisation in the course of performing the Organisation's functions under section 17; and
 - (b) the information relates, or appears to relate, to the performance of ASIS, ASD or AGO's functions (as the case requires).

Communicating information in relation to emergency declarations

- (4B) A person referred to in subsection (1) may communicate information, in accordance with Part VIA of the *Privacy Act 1988*, if:
 - (a) the information has come into the possession of the Organisation in the course of performing its functions under section 17; and

Section 18A

- (b) an emergency declaration (within the meaning of section 80G of that Act) is in force.

Communicating information to the Australian Designated Authority etc.

- (5) A person referred to in subsection (1) may communicate information to:
 - (a) the Australian Designated Authority (within the meaning of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*); or
 - (b) an APS employee in the Attorney-General's Department (within the meaning of that Schedule);for the purpose of the Australian Designated Authority exercising a power, or performing a function, under that Schedule.

18A Unauthorised dealing with records

Offence for unauthorised dealing with records

- (1) A person commits an offence if:
 - (a) the person is, or has been, an entrusted person; and
 - (b) the person has obtained a record in the person's capacity as an entrusted person; and
 - (c) the record:
 - (i) was acquired or prepared by or on behalf of the Organisation in connection with its functions; or
 - (ii) relates to the performance by the Organisation of its functions; and
 - (d) the person engages in any of the following conduct (the **relevant conduct**):
 - (i) copying the record;
 - (ii) transcribing the record;
 - (iii) retaining the record;
 - (iv) removing the record;
 - (v) dealing with the record in any other manner; and

- (e) the relevant conduct was not engaged in by the person:
- (i) as an ASIO employee in the course of the person's duties as an ASIO employee; or
 - (ii) as an ASIO affiliate in accordance with the contract, agreement or other arrangement under which the person is performing functions or services for the Organisation; or
 - (iii) in accordance with a contract, agreement or arrangement the person has entered into with ASIO (other than as an ASIO affiliate); or
 - (iv) acting within the limits of authority conferred on the person by the Director-General; or
 - (v) with the approval of the Director-General, or of a person having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—record lawfully available

- (2) Subsection (1) does not apply to a record that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Exception—IGIS officials

- (2A) Subsection (1) does not apply if the person deals with the record for the purpose of an IGIS official exercising a power, or performing a function or duty, as an IGIS official.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

Alternative verdict

- (3) Subsection (4) applies if, in a prosecution for an offence (the **prosecuted offence**) against subsection (1), the trier of fact:

Section 18B

- (a) is not satisfied that the defendant is guilty of the prosecuted offence; but
 - (b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 18B(1) (the *alternative offence*).
- (4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

Definitions

- (5) In this section:

record means a document, or any other object by which words, images, sounds or signals are recorded or stored or from which information can be obtained, and includes part of a record.

Note: For the definition of **document**, see section 2B of the *Acts Interpretation Act 1901*.

signals includes electromagnetic emissions.

18B Unauthorised recording of information or matter

- (1) A person commits an offence if:
- (a) the person is, or has been, an entrusted person; and
 - (b) information or matter has come to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and
 - (c) the information or matter:
 - (i) was acquired or prepared by or on behalf of the Organisation in connection with its functions; or
 - (ii) relates to the performance by the Organisation of its functions; and
 - (d) the person makes a record of the information or matter; and
 - (e) the record is not made by the person:

Section 18B

- (i) as an ASIO employee in the course of the person's duties as an ASIO employee; or
- (ii) as an ASIO affiliate in accordance with the contract, agreement or other arrangement under which the person is performing functions or services for the Organisation; or
- (iii) in accordance with a contract, agreement or arrangement the person has entered into with ASIO (other than as an ASIO affiliate); or
- (iv) acting within the limits of authority conferred on the person by the Director-General; or
- (v) with the approval of the Director-General, or of a person having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—information or matter lawfully available

- (2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Exception—IGIS officials

- (2A) Subsection (1) does not apply if the person makes the record for the purpose of an IGIS official exercising a power, or performing a function or duty, as an IGIS official.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

Alternative verdict

- (3) Subsection (4) applies if, in a prosecution for an offence (the **prosecuted offence**) against subsection (1), the trier of fact:

Section 18C

- (a) is not satisfied that the defendant is guilty of the prosecuted offence; but
 - (b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 18A(1) (the *alternative offence*).
- (4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

Definitions

- (5) In this section:

record has the same meaning as in section 18A.

18C Offences against section 18, 18A or 18B—general rules

Extended geographical jurisdiction

- (1) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against section 18, 18A or 18B.
- (2) Subsection (1) does not, by implication, affect the interpretation of any other provision of this Act.

Institution of prosecution

- (3) A prosecution under section 18, 18A or 18B may be instituted only by, or with the consent of, the Attorney-General or a person acting under the Attorney-General's direction.
- (4) However:
 - (a) a person charged with an offence against section 18, 18A or 18B may be arrested, or a warrant for his or her arrest may be issued and executed; and
 - (b) such a person may be remanded in custody or on bail;

even if the consent of the Attorney-General or a person acting under his or her direction has not been obtained, but no further proceedings are to be taken until that consent has been obtained.

- (5) Nothing in subsection (3) or (4) prevents the discharging of the accused if proceedings are not continued within a reasonable time.

18D Offences against section 18, 18A or 18B—IGIS officials

- (1) A person does not commit an offence against subsection 18(2), 18A(1) or 18B(1) if:
- (a) the person is an IGIS official; and
 - (b) the relevant conduct is engaged in by the person for the purposes of exercising powers, or performing functions or duties, as an IGIS official.
- (2) In a prosecution for an offence against subsection 18(2), 18A(1) or 18B(1), the defendant does not bear an evidential burden in relation to the matter in subsection (1) of this section, despite subsection 13.3(3) of the *Criminal Code*.

19 Co-operation with other authorities in connection with performance of Organisation's functions

- (1) So far as necessary for, or conducive to, the performance of the Organisation's functions, the Organisation may, subject to any arrangements made or directions given by the Minister, co-operate with:
- (a) authorities of the Commonwealth; and
 - (b) Departments, Police Forces and authorities of the States; and
 - (c) authorities of other countries approved by the Minister as being capable of assisting the Organisation in the performance of its functions; and
 - (d) any other person or body whether within or outside Australia.
- (2) A person referred to in subsection 18(1) may, where the Organisation is co-operating with an authority of another country in accordance with paragraph (1)(c), communicate to an officer of

Section 19A

that authority information that has come into the possession of the Organisation in the course of performing its functions under section 17, being information that is relevant to the security of that other country and that could not, apart from this subsection, be communicated to that officer.

Note: There are additional restrictions, in the *Telecommunications (Interception and Access) Act 1979*, on communicating telecommunications information.

19A Co-operation with intelligence and law enforcement agencies etc. in connection with performance of their functions

- (1) The Organisation may co-operate with and assist the following bodies in the performance of their functions:
 - (a) ASIS;
 - (b) ASD;
 - (c) AGO;
 - (ca) ONI;
 - (d) a law enforcement agency;
 - (e) an authority of the Commonwealth, or an authority of a State, that is prescribed by the regulations for the purposes of this paragraph.
- (2) However, the Organisation may only do so:
 - (a) subject to any arrangements made or directions given by the Minister; and
 - (b) on request by the head (however described) of the body referred to in subsection (1).
- (3) Without limiting subsection (1), in co-operating with and assisting a body in accordance with this section, the Organisation may make the services of ASIO employees and ASIO affiliates, and other resources of the Organisation, available to the body.

Communicating information

- (4) A person referred to in subsection 18(1) may communicate information to a staff member of a body referred to in paragraph (1)(d) or (e) if:
- (a) the information has come into the possession of the Organisation in the course of performing the Organisation's functions under section 17; and
 - (b) the information is communicated for the purposes of co-operating with or assisting the body under this section.

Note 1: For communication of information to ASIS, ASD and AGO, see subsection 18(4A).

Note 2: There are additional restrictions, in the *Telecommunications (Interception and Access) Act 1979*, on communicating telecommunications information.

20 Special responsibility of Director-General in relation to functions of Organisation

The Director-General shall take all reasonable steps to ensure that:

- (a) the work of the Organisation is limited to what is necessary for the purposes of the discharge of its functions; and
- (b) the Organisation is kept free from any influences or considerations not relevant to its functions and nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions.

21 Leader of Opposition to be kept informed on security matters

The Director-General shall consult regularly with the Leader of the Opposition in the House of Representatives for the purpose of keeping him or her informed on matters relating to security.

Section 21A

21A Voluntary assistance provided to the Organisation

Assistance provided in accordance with a request by the Director-General

- (1) If:
- (a) the Director-General requests a person or body to engage in conduct; and
 - (b) the Director-General is satisfied, on reasonable grounds, that the conduct is likely to assist the Organisation in the performance of its functions; and
 - (c) the person engages in the conduct in accordance with the request; and
 - (d) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and
 - (e) the conduct does not result in significant loss of, or serious damage to, property;
- the person or body is not subject to any civil liability for, or in relation to, the conduct.
- (2) A request under paragraph (1)(a) may be made orally if:
- (a) the Director-General is satisfied that the request should be made as a matter of urgency; or
 - (b) the Director-General is satisfied that making the request in writing would be prejudicial to security; or
 - (c) the Director-General is satisfied that making the request in writing would be prejudicial to the operational security of the Organisation.
- (2A) If subsection (2) does not apply to a request under paragraph (1)(a), the request must be made in writing.
- (3) If a request under paragraph (1)(a) is made orally, the Director-General must:
- (a) make a written record of the request; and
 - (b) do so within 48 hours after the request was made.

- (3A) If a request is made under paragraph (1)(a), the Director-General must, within 7 days after the request is made, notify the Inspector-General of Intelligence and Security that the request has been made.
- (4) The Director-General may enter into a contract, agreement or arrangement with a person or body in relation to conduct engaged in by the person or body in accordance with a request under paragraph (1)(a).

Unsolicited disclosure of information etc.

- (5) If:
- (a) a person or body engages in conduct that consists of, or is connected with:
 - (i) giving information to the Organisation; or
 - (ii) giving or producing a document to the Organisation; or
 - (iii) making one or more copies of a document and giving those copies to the Organisation; and
 - (b) the person reasonably believes that the conduct is likely to assist the Organisation in the performance of its functions; and
 - (c) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and
 - (d) the conduct does not result in significant loss of, or serious damage to, property; and
 - (e) subsection (1) does not apply to the conduct;
- the person or body is not subject to any civil liability for, or in relation to, the conduct.

Copies of, or extracts from, documents

- (6) The Organisation may make and retain copies of, or take and retain extracts from, a document given or produced to the Organisation:
- (a) in accordance with a request under paragraph (1)(a); or
 - (b) under paragraph (5)(a).

Section 21A

Subsections (1) and (5) have effect despite other laws

- (7) Subsections (1) and (5) have effect despite anything in a law of the Commonwealth, a State or a Territory (whether passed or made before or after the commencement of this section) unless the law expressly provides otherwise.

Certificate

- (8) The Director-General may give a certificate in writing certifying one or more facts relevant to the question of whether the Director-General was satisfied, on reasonable grounds, that particular conduct was likely to assist the Organisation in the performance of its functions.
- (9) In any proceedings that involve determining whether subsection (1) or (5) applies to particular conduct, a certificate given under subsection (8) is prima facie evidence of the facts certified.

Compensation for acquisition of property

- (10) If the operation of this section would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from a person otherwise than on just terms (within the meaning of that paragraph), the Commonwealth is liable to pay a reasonable amount of compensation to the person.
- (11) If the Commonwealth and the person do not agree on the amount of the compensation, the person may institute proceedings in the Federal Court of Australia for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

Division 2—Special powers

Subdivision A—Preliminary

22 Interpretation

In this Division, unless the contrary intention appears:

authorising officer means:

- (a) the Director-General; or
- (b) an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.

carrier means:

- (a) a carrier within the meaning of the *Telecommunications Act 1997*; or
- (b) a carriage service provider within the meaning of that Act.

communicate includes cause to be communicated.

communication in transit means a communication (within the meaning of the *Telecommunications Act 1997*) passing over a telecommunications network (within the meaning of that Act).

data includes information, a computer program or part of a computer program.

device includes instrument, apparatus, equipment and any other thing (whether tangible or intangible).

enhancement equipment, in relation to a surveillance device, means equipment capable of enhancing a signal, image or other information obtained by the use of the surveillance device.

examination includes any act or process for the purpose of producing sounds, images or information from a record, and ***examine*** has a corresponding meaning.

Section 22

identified person warrant means a warrant issued under section 27C.

install includes attach and apply.

internal authorisation means an authorisation given under section 26G.

listening device means any device capable of being used, whether alone or in conjunction with any other device, to overhear, record, monitor or listen to sounds, signals or a conversation, or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome that impairment and permit that person to hear only sounds ordinarily audible to the human ear.

maintain, in relation to a surveillance device, includes adjust, improve, relocate, repair, service and replace the device.

object means:

- (a) a vehicle, aircraft, vessel or other means of transportation; or
- (b) clothing or any other thing worn; or
- (c) any other thing.

optical surveillance device means any device capable of being used, whether alone or in conjunction with any other device, to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

prejudicial activities of a person means activities prejudicial to security that the person is engaged in, or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in.

premises includes any land, place, vehicle, vessel or aircraft.

record when used as a noun, means:

- (a) a document (including any written or printed material); or

- (b) an object (including a sound recording, magnetic tape or disc, microform, photograph or film) by which words, images, sounds or signals are recorded or stored or from which information can be obtained.

signals includes electromagnetic emissions.

surveillance device means:

- (a) a listening device, an optical surveillance device or a tracking device; or
- (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a) or (c); or
- (c) a device of a kind prescribed by regulation for the purposes of this paragraph.

surveillance device warrant means a warrant issued under section 26.

telecommunications facility means a facility within the meaning of section 7 of the *Telecommunications Act 1997*.

track a person or an object means determine or monitor:

- (a) the location of the person or object; or
- (b) the status of the object.

tracking device means any device capable of being used (whether alone or in conjunction with any other device) to track a person or an object.

use of a surveillance device includes use of the device:

- (a) to listen to, record, observe or monitor the words, sounds or signals communicated to or by a person, or the activities of a person; or
- (b) to track an object or person.

Section 23

23 Requesting information or documents from operators of aircraft or vessels

- (1) For the purposes of carrying out the Organisation's functions, the Director-General or an authorised person may:
 - (a) ask an operator of an aircraft or vessel questions relating to the aircraft or vessel, or its cargo, crew, passengers, stores or voyage; or
 - (b) request an operator of an aircraft or vessel to produce documents relating to the aircraft or vessel, or its cargo, crew, passengers, stores or voyage, that are in the possession or under the control of the operator.
- (2) A person who is asked a question or requested to produce a document under subsection (1) must answer the question or produce the document as soon as practicable.

Offence

- (3) A person commits an offence if:
 - (a) the person is an operator of an aircraft or vessel; and
 - (b) the person is asked a question or requested to produce a document under subsection (1); and
 - (c) the person fails to answer the question or produce the document.

Penalty: 60 penalty units.

- (4) Subsection (3) is an offence of strict liability.

Note: For strict liability, see section 6.1 of the *Criminal Code*.

- (5) It is a defence to a prosecution for an offence against subsection (3) if the person charged had a reasonable excuse for:
 - (a) failing to answer the question; or
 - (b) failing to produce the document.
- (6) The Director-General, or a person appointed under subsection (6A), may authorise, in writing, a person, or a class of persons, for the purposes of this section.

(6A) The Director-General may, in writing, appoint a senior position-holder, or a class of senior position-holders, for the purposes of subsection (6).

(7) In this section:

authorised person means a person who is authorised under subsection (6) for the purposes of this section.

operator has the meaning given by section 4 of the *Customs Act 1901*.

24 Exercise of authority under warrant etc.

Who may exercise authority under warrant etc.

- (1) The authority conferred by a relevant warrant or relevant device recovery provision may be exercised on behalf of the Organisation only by:
- (a) the Director-General; or
 - (b) a person approved under subsection (2); or
 - (c) a person included in a class of persons approved under subsection (2).

Approval of persons authorised to exercise authority under warrant etc.

- (2) The Director-General or a person appointed under subsection (3) may, in writing, approve a person, or a class of persons, as people authorised to exercise, on behalf of the Organisation, the authority conferred by relevant warrants or relevant device recovery provisions.
- (2A) To avoid doubt, and without limiting subsection (2), if approval is given to a person or class of persons holding, occupying or performing the duties of an office or position, then the approval extends to such an office or position that comes into existence after the approval is given.

Section 25

- (2B) Subsection (2A) does not, by implication, affect the interpretation of any other provision of this Act.
- (3) The Director-General may, in writing, appoint a senior position-holder, or a class of senior position-holders, for the purposes of subsection (2).

Records of persons who exercise the authority

- (3A) The Director-General must, as soon as practicable after the authority conferred by a relevant warrant or relevant device recovery provision is exercised on behalf of the Organisation, cause one or more written records to be made that identify each person who exercised that authority.

Definitions

- (4) In this section:

relevant device recovery provision means subsection 25A(8), 26B(5) or (6), 27A(3A), (3B) or (3C), 27E(6) or 27F(5).

relevant warrant means a warrant issued under this Division or under Division 3.

Subdivision B—Search warrants

25 Search warrants

Issue of search warrant

- (1) If the Director-General requests the Attorney-General to do so, and the Attorney-General is satisfied as mentioned in subsection (2), the Attorney-General may issue a warrant in accordance with this section.

Test for issue of warrant

- (2) The Attorney-General is only to issue the warrant if he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to records or other things on particular premises (the **subject premises**) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the **security matter**) that is important in relation to security.

Authorisation in warrant

- (3) The warrant must be signed by the Attorney-General and must authorise the Organisation to do specified things, subject to any restrictions or conditions specified in the warrant, in relation to the subject premises, which must also be specified in the warrant.

Things that may be specified in warrant

- (4) The things that may be specified are any of the following that the Attorney-General considers appropriate in the circumstances:
- (a) entering the subject premises;
 - (aa) entering any premises for the purposes of gaining entry to or exiting the subject premises;
 - (b) searching the subject premises for the purpose of finding records or other things relevant to the security matter and, for that purpose, opening any safe, box, drawer, parcel, envelope or other container in which there is reasonable cause to believe that any such records or other things may be found;
 - (c) inspecting or otherwise examining any records or other things so found, and making copies or transcripts of any such record or other thing that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;
 - (d) removing and retaining any record or other thing so found, for the purposes of:
 - (i) inspecting or examining it; and
 - (ii) in the case of a record—making copies or transcripts of it, in accordance with the warrant;

Section 25

- (e) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
- (f) any other thing reasonably incidental to any of the above.

Personal searches may be specified

- (4A) The Attorney-General may also specify any of the following things if he or she considers it appropriate in the circumstances:
- (a) conducting an ordinary search or a frisk search of a person if:
 - (i) the person is at or near the subject premises when the warrant is executed; and
 - (ii) there is reasonable cause to believe that the person has on his or her person records or other things relevant to the security matter;
 - (b) inspecting or otherwise examining any records or other things so found, and making copies or transcripts of any such record or other thing that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;
 - (c) removing and retaining any record or other thing so found, for the purposes of:
 - (i) inspecting or examining it; and
 - (ii) in the case of a record—making copies or transcripts of it, in accordance with the warrant.

Certain personal searches not authorised

- (4B) Subsection (4A) does not authorise a strip search or a search of a person's body cavities.

Time period for retaining records and other things

- (4C) A record or other thing retained as mentioned in paragraph (4)(d) or (4A)(c) may be retained:
- (a) if returning the record or thing would be prejudicial to security—only until returning the record or thing would no longer be prejudicial to security; and

- (b) otherwise—for only such time as is reasonable.

Other things that may be specified

- (5) The Attorney-General may also specify any of the following things if he or she considers it appropriate in the circumstances:
- (a) where there is reasonable cause to believe that data relevant to the security matter may be accessible by using a computer or other electronic equipment, or a data storage device, brought to or found on the subject premises—using the computer, equipment or device for the purpose of obtaining access to any such data and, if necessary to achieve that purpose, adding, copying, deleting or altering other data in the computer, equipment or device;
 - (b) using the computer, equipment or device to do any of the following:
 - (i) inspecting and examining any data to which access has been obtained;
 - (ii) converting any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, into documentary form and removing any such document;
 - (iii) copying any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, to any data storage device and removing the device;
 - (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
 - (d) any other thing reasonably incidental to any of the above.

Certain acts not authorised

- (6) Subsection (5) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

Section 25

- (a) materially interfere with, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified under subsection (5); or
- (b) cause any other material loss or damage to other persons lawfully using the computer, equipment or device.

Warrant must provide for certain matters

- (7) The warrant must:
 - (a) authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant; and
 - (b) state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

Statement about warrant coming into force

- (8) The warrant may state that it comes into force on a specified day (after the day of issue) or when a specified event happens. The day must not begin nor the event happen more than 28 days after the end of the day on which the warrant is issued.

When warrant comes into force

- (9) If the warrant includes such a statement, it comes into force at the beginning of the specified day or when the specified event happens. Otherwise, it comes into force when it is issued.

Duration of warrant

- (10) The warrant must specify the period during which it is to be in force. The period must not be more than 90 days, although the Attorney-General may revoke the warrant before the period has expired.

Issue of further warrants not prevented

- (11) Subsection (10) does not prevent the issue of any further warrant.

25AA Conduct of ordinary or frisk search under search warrant

An ordinary search or frisk search of a person that is authorised under paragraph 25(4A)(a) must, if practicable, be conducted by a person of the same sex as the person being searched.

Subdivision C—Computer access warrants

25A Computer access warrant

Issue of computer access warrant

- (1) If the Director-General requests the Attorney-General to do so, and the Attorney-General is satisfied as mentioned in subsection (2), the Attorney-General may issue a warrant in accordance with this section.

Test for issue of warrant

- (2) The Attorney-General is only to issue the warrant if he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a computer (the **target computer**) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the **security matter**) that is important in relation to security.

Note: See section 4 for the definition of **computer**.

- (3) The target computer may be any one or more of the following:
- (a) a particular computer;
 - (b) a computer on particular premises;
 - (c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

Section 25A

Authorisation in warrant

- (3A) The warrant must:
- (a) be signed by the Attorney-General; and
 - (b) authorise the Organisation to do specified things, subject to any restrictions or conditions specified in the warrant, in relation to the target computer; and
 - (c) if the target computer is or includes a particular computer—specify the computer; and
 - (d) if the target computer is or includes a computer on particular premises—specify the premises; and
 - (e) if the target computer is or includes a computer associated with, used by or likely to be used by, a person—specify the person (whether by name or otherwise).

Things that may be authorised in warrant

- (4) The things that may be specified are any of the following that the Attorney-General considers appropriate in the circumstances:
- (aa) entering specified premises for the purposes of doing the things mentioned in this subsection;
 - (aaa) entering any premises for the purposes of gaining entry to or exiting the specified premises;
 - (a) using:
 - (i) the target computer; or
 - (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
 - (iii) any other electronic equipment; or
 - (iv) a data storage device;for the purpose of obtaining access to data (the *relevant data*) that is relevant to the security matter and is held in the target computer at any time while the warrant is in force and, if necessary to achieve that purpose, adding, copying, deleting or altering other data in the target computer;

- (ab) if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) using any other computer or a communication in transit to access the relevant data; and
 - (ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;
- (ac) removing a computer or other thing from premises for the purposes of doing any thing specified in the warrant in accordance with this subsection, and returning the computer or other thing to the premises;
- (b) copying any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;
- (ba) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing specified in the warrant in accordance with this subsection;
- (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
- (d) any other thing reasonably incidental to any of the above.

Note: As a result of the warrant, a person who, by means of a telecommunications facility, obtains access to data stored in a computer etc. will not commit an offence under Part 10-7 of the *Criminal Code* or equivalent State or Territory laws (provided that the person acts within the authority of the warrant).

(4A) If:

- (a) the warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph (4)(ac); and
- (b) a computer or thing is removed from the premises in accordance with the warrant;

the computer or thing must be returned to the premises:

- (c) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or

Section 25A

(d) otherwise—within a reasonable period.

Certain acts not authorised

- (5) Subsection (4) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:
- (a) materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or
 - (b) cause any other material loss or damage to other persons lawfully using a computer.

Warrant must provide for certain matters

- (5A) The warrant must:
- (a) authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant; and
 - (b) if the warrant authorises entering premises—state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

Duration of warrant

- (6) The warrant must specify the period during which it is to remain in force. The period must not be more than 6 months, although the Attorney-General may revoke the warrant before the period has expired.

Issue of further warrants not prevented

- (7) Subsection (6) does not prevent the issue of any further warrant.

Concealment of access etc.

- (8) If any thing has been done in relation to a computer under:
- (a) the warrant; or

- (b) this subsection;
- the Organisation is authorised to do any of the following:
- (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;
 - (d) enter any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);
 - (e) enter any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);
 - (f) remove the computer or another thing from any place where it is situated for the purposes of doing the things mentioned in paragraph (c), and returning the computer or other thing to that place;
 - (g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) use any other computer or a communication in transit to do those things; and
 - (ii) if necessary to achieve that purpose—add, copy, delete or alter other data in the computer or the communication in transit;
 - (h) intercept a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing mentioned in this subsection;
 - (i) any other thing reasonably incidental to any of the above;
- at the following time:
- (j) at any time while the warrant is in force or within 28 days after it ceases to be in force;
 - (k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).
- (9) Subsection (8) does not authorise the doing of a thing that is likely to:

Section 26

- (a) materially interfere with, interrupt or obstruct:
 - (i) a communication in transit; or
 - (ii) the lawful use by other persons of a computer; unless the doing of the thing is necessary to do one or more of the things specified in subsection (8); or
 - (b) cause any other material loss or damage to other persons lawfully using a computer.
- (10) If a computer or another thing is removed from a place in accordance with paragraph (8)(f), the computer or thing must be returned to that place:
- (a) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
 - (b) otherwise—within a reasonable period.

Subdivision D—Use of surveillance devices

26 Issue of surveillance device warrants

Issue of surveillance device warrant

- (1) If the Director-General requests the Attorney-General to do so, and the Attorney-General is satisfied as mentioned in subsection (3), the Attorney-General may issue a warrant in accordance with this section.
- (2) The warrant may be issued:
 - (a) in relation to one or more of the following:
 - (i) a particular person;
 - (ii) particular premises;
 - (iii) an object or class of object; and
 - (b) in respect of more than one kind of surveillance device; and
 - (c) in respect of more than one surveillance device of any particular kind.

Test for issue of warrant

- (3) The Attorney-General is only to issue the warrant if he or she is satisfied that:
- (a) if the warrant is requested in relation to a particular person:
 - (i) the person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (ii) the use by the Organisation of a surveillance device in relation to that person will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security; and
 - (b) if the warrant is requested in relation to particular premises:
 - (i) those premises are used, likely to be used or frequented by a person engaged in or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (ii) the use on behalf of the Organisation of a surveillance device in or on those premises will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security; and
 - (c) if the warrant is requested in relation to an object or class of object:
 - (i) that object, or an object of that class, is used or worn, or likely to be used or worn by a person engaged in or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (ii) the use by the Organisation of a surveillance device in or on that object, or an object of that class, will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security.
- (4) To avoid doubt, the identity of the person referred to in paragraph (3)(a) or subparagraph (3)(b)(i) or (c)(i) need not be known.

Section 26A

Warrant may be subject to restrictions or conditions

- (5) The warrant is subject to any restrictions or conditions specified in it.

26A Requirements for surveillance device warrants

- (1) A surveillance device warrant must:
- (a) be signed by the Attorney-General; and
 - (b) specify:
 - (i) the kind of surveillance device, or kinds of surveillance devices, authorised to be used; and
 - (ii) the date the warrant is issued; and
 - (iii) if the warrant is issued in relation to a particular person—the name of the person (if known) or the fact that the person’s identity is unknown; and
 - (iv) if the warrant is issued in relation to particular premises—the premises; and
 - (v) if the warrant is issued in relation to an object or class of object—the object or class of object; and
 - (c) authorise the use of any force against persons and things that is necessary and reasonable to do the things authorised by the warrant; and
 - (d) state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.
- (2) If a surveillance device warrant is issued in relation to particular premises that are vehicles, the warrant need only specify the class of vehicle in relation to which the use of the surveillance device is authorised.
- (3) The surveillance device warrant must specify the period during which it is to remain in force. The period must not be more than 6 months, although the Attorney-General may revoke the warrant before the period has expired.
- (4) Subsection (3) does not prevent the issue of any further warrant.

26B What a surveillance device warrant authorises

Authorisation in warrant—particular person

- (1) If a surveillance device warrant is issued in relation to a particular person, the warrant authorises the following:
 - (a) the installation, use and maintenance of a surveillance device of the kind specified in the warrant to:
 - (i) listen to, record, observe or monitor the words, sounds or signals communicated to or by the person, or the activities of the person; or
 - (ii) track the person;
 - (b) the installation, use and maintenance of a surveillance device of the kind specified in the warrant:
 - (i) in or on premises where the person is reasonably believed to be or likely to be; or
 - (ii) in or on any other premises specified in the warrant from which the activities of that person, or the words, sounds or signals communicated by or to that person, can be listened to, recorded, observed or monitored;
 - (c) entering the premises referred to in paragraph (b) for any of the purposes referred to in paragraph (a) or (b) or in subsection (4) or (5);
 - (d) the installation, use and maintenance of a surveillance device of the kind specified in the warrant in or on any object used or worn, or likely to be used or worn, by the person;
 - (e) the entry into or onto, or the alteration of, the object referred to in paragraph (d);
 - (f) entering any premises in which the object referred to in paragraph (d) is or is likely to be found, for any of the purposes referred to in that paragraph or in subsection (4) or (5);
 - (g) entering any other premises, for the purposes of gaining entry to or exiting premises referred in to paragraph (b) or (f);
 - (h) any other thing reasonably incidental to any of the above.

Section 26B

Authorisation in warrant—particular premises

- (2) If a surveillance device warrant is issued in relation to particular premises (the **subject premises**), the warrant authorises the following:
- (a) the installation, use and maintenance of a surveillance device of the kind specified in the warrant:
 - (i) in or on the subject premises; or
 - (ii) in or on any other premises specified in the warrant from which the activities of a person, or the words, sounds or signals communicated by or to a person, can be listened to, recorded, observed or monitored while the person is in or on the subject premises;
 - (b) entering the subject premises, or any other premises specified in the warrant, for any of the purposes referred to in paragraph (a) or subsection (4) or (5);
 - (c) entering any other premises, for the purposes of gaining entry to or exiting the subject premises or any other premises specified in the warrant;
 - (d) any other thing reasonably incidental to any of the above.

Authorisation in warrant—object or class of object

- (3) If a surveillance device warrant is issued in relation to an object, or class of object, the warrant authorises the following:
- (a) the installation, use and maintenance of a surveillance device of the kind specified in the warrant in or on the specified object, or an object of the specified class;
 - (b) the entry into or onto, or alteration of, the specified object, or an object of the specified class;
 - (c) entering any premises where the object, or an object of the class, is reasonably believed to be or is likely to be for any of the purposes referred to in paragraph (a) or (b) or subsection (4) or (5);
 - (d) entering any other premises, for the purposes of gaining entry to or exiting premises referred to in paragraph (c);
 - (e) any other thing reasonably incidental to any of the above.

Authorisation in warrant—general

- (4) A surveillance device warrant also authorises the following:
- (a) the installation, use and maintenance of enhancement equipment in relation to the surveillance device;
 - (b) the temporary removal of an object from premises for the installation or maintenance of the surveillance device or enhancement equipment and the return of the object to the premises;
 - (c) the replacement of an object with an equivalent object for the purposes of the installation or maintenance of the surveillance device or enhancement equipment;
 - (d) the breaking open of any thing for the installation or maintenance of the surveillance device or enhancement equipment;
 - (e) the connection of the surveillance device or enhancement equipment to any source of electricity and the use of electricity from that source to operate the device or equipment;
 - (f) the connection of the surveillance device or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the device or equipment;
 - (g) the doing of any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
 - (h) any other thing reasonably incidental to any of the above.

Recovery of surveillance devices

- (5) If a surveillance device is installed or used under a surveillance device warrant, the Organisation is authorised to do any of the following:
- (a) recover the surveillance device or any enhancement equipment in relation to the device;

Section 26B

- (b) enter any premises where the surveillance device is reasonably believed to be, for the purpose of recovering the device or the equipment;
 - (c) enter any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (b);
 - (d) enter into or onto, or alter, an object for the purpose of recovering the device or the equipment;
 - (e) replace an object with an equivalent object for the purposes of recovering the device or the equipment;
 - (f) break open any thing for the purpose of recovering the device or the equipment;
 - (g) if the device or equipment is installed in or on an object—temporarily remove the object from any place where it is situated for the purpose of recovering the device or the equipment and returning the object to that place;
 - (h) use a nominal amount of electricity from any source to power the device or equipment;
 - (i) any thing reasonably necessary to conceal the fact that any thing has been done under this subsection;
 - (j) use any force against persons and things that is necessary and reasonable to do any of the above;
 - (k) any other thing reasonably incidental to any of the above;
- at the following time:
- (l) at any time while the warrant is in force or within 28 days after it ceases to be in force;
 - (m) if the surveillance device is not recovered at a time mentioned in paragraph (l)—at the earliest time, after the 28 days mentioned in that paragraph, at which it is reasonably practicable to do the things concerned.
- (6) If, for the purposes of subsection (5):
- (a) the surveillance device is not recovered while the warrant is in force; and
 - (b) the surveillance device is a tracking device;

the Organisation is also authorised to use the surveillance device or any enhancement equipment in relation to the device solely for the purposes of the location and recovery of the device or equipment.

26C Use etc. of listening device without warrant

Either of the following (the *first person*):

- (a) an ASIO employee acting in the course of the ASIO employee's duties;
- (b) an ASIO affiliate acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation;

may install, use or maintain a listening device without warrant for any purpose involving listening to or recording words, sounds or signals being communicated by or to another person (the *second person*) if:

- (c) the first person is the communicator of the words, sounds or signals; or
- (d) the second person intends, or should reasonably expect, those words, sounds or signals to be communicated to the first person, or to a class or group of persons in which the first person is included; or
- (e) the first person does so with the implied or express consent of a person who is permitted under paragraph (c) or (d) to listen to or record the words, sounds or signals.

Note: This section does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

26D Use etc. of optical surveillance device without warrant

Either of the following:

- (a) an ASIO employee acting in the course of the ASIO employee's duties;
- (b) an ASIO affiliate acting in accordance with the contract, agreement or other arrangement under which the ASIO

Section 26E

affiliate is performing functions or services for the Organisation;

may install, use or maintain an optical surveillance device without warrant if the installation, use or maintenance of the device does not involve:

- (c) entering premises without permission from the owner or occupier of the premises; or
- (d) interference with any vehicle or thing without permission of the person having lawful possession or control of the vehicle or thing.

Note: This section does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

26E Use etc. of tracking device without warrant or internal authorisation

(1) Either of the following:

- (a) an ASIO employee acting in the course of the ASIO employee's duties;
- (b) an ASIO affiliate acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation;

may install, use or maintain a tracking device without warrant or internal authorisation for the purposes of tracking a person if the person consents to the installation, use or maintenance.

Note: This subsection does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

(2) Either of the following:

- (a) an ASIO employee acting in the course of the ASIO employee's duties;
- (b) an ASIO affiliate, acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation;

may install, use or maintain a tracking device without warrant or internal authorisation for the purposes of tracking an object if the person using the object consents to the installation, use or maintenance.

Note: This subsection does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

26F Director-General may determine that certain provisions do not apply to specified ASIO affiliates

- (1) The Director-General may, by signed writing, determine that section 26C or 26D or subsection 26E(1) or (2) does not apply to:
 - (a) a specified ASIO affiliate; or
 - (b) a specified class of ASIO affiliates.
- (2) A determination under subsection (1) has effect accordingly.
- (3) A determination under subsection (1) is not a legislative instrument.
- (4) The Director-General may, by signed writing, delegate the Director-General's power under this section to:
 - (a) a Deputy Director-General; or
 - (b) any other ASIO employee or ASIO affiliate who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee with a classification of SES Band 2.
- (5) In exercising powers under a delegation, the delegate must comply with any written direction given by the Director-General to the delegate.

Subdivision DA—Use of tracking devices under internal authorisation

26G Use of tracking devices under internal authorisation

Request for authorisation

- (1) An ASIO employee or ASIO affiliate (the *applicant*) may request an authorising officer to give an authorisation under this section in respect of a matter (the *security matter*) that is important in relation to security.

Note: An authorisation given under this section cannot authorise certain things, including the following:

- (a) entering premises or interfering with the interior of a vehicle without permission;
- (b) remotely installing a tracking device;
- (c) installing a tracking device to listen to a person;
- (d) any other thing that the Organisation would otherwise need a warrant under section 25A to do.

See section 26K.

- (2) The request must be made in relation to one or both of the following:
- (a) a particular person;
 - (b) an object or a class of object.
- (3) The request may be made:
- (a) in writing; or
 - (b) orally in person, or by telephone or other means of communication.
- (4) A request under subsection (1) must include a statement of:
- (a) the facts and other grounds on which the applicant considers it necessary that the authorisation should be given; and
 - (b) the extent to which the applicant considers that the authorisation will substantially assist the collection of intelligence in respect of the security matter; and

- (c) the period for which the applicant considers the authorisation should remain in force, which must not exceed 90 days.
- (5) If the request is made orally, a written record of the request that meets the requirements of subsection (4) must be made within 48 hours after the request is made.

Test for giving of authorisation

- (6) The authorising officer may give the authorisation only if the authorising officer is satisfied that there are reasonable grounds for believing that:
 - (a) if the authorisation is requested in relation to a particular person—the use by the Organisation of a tracking device in relation to the person will, or is likely to, substantially assist the collection of intelligence in respect of the security matter; and
 - (b) if the authorisation is requested in relation to an object or class of object—the use by the Organisation of a tracking device in or on that object, or an object of that class, will, or is likely to, substantially assist the collection of intelligence in respect of the security matter.
- (7) To avoid doubt, the identity of the person referred to in paragraph (6)(a) need not be known.

Authorisation may be subject to restrictions or conditions

- (8) The authorisation is subject to any restrictions or conditions specified in it.

26H Requirements for internal authorisations

- (1) An internal authorisation may be given:
 - (a) in writing; or
 - (b) orally in person, or by telephone or other means of communication.
- (2) The authorisation must specify:

Section 26J

- (a) the matter (the *security matter*) that is important in relation to security in respect of which the authorisation is given; and
 - (b) the day and time the authorisation is given; and
 - (c) if the authorisation is given in relation to a particular person—the name of the person (if known) or the fact that the person’s identity is unknown; and
 - (d) if the authorisation is given in relation to an object or a class of object—the object or class of object; and
 - (e) the restrictions or conditions (if any) to which the authorisation is subject.
- (3) The authorisation must also specify the period for which the authorisation is to remain in force, being a period that:
- (a) the authorising officer considers reasonable and necessary in the circumstances; and
 - (b) does not exceed 90 days;
- but the authorising officer may revoke the authorisation before the period has expired.
- (4) Subsection (3) does not prevent the giving of further internal authorisations in relation to the same security matter.
- (5) If an internal authorisation is given orally, a written record of the authorisation that meets the requirements of subsections (2) and (3) must be made within 48 hours after the authorisation is given.
- (6) The following are not legislative instruments:
- (a) an authorisation under this section;
 - (b) a written record referred to in subsection (5).

26J What an internal authorisation authorises

Things that may be authorised—particular person

- (1) If an internal authorisation is given in relation to a particular person, the authorisation may authorise the Organisation to do, without warrant, one or more of the following:

- (a) install, use or maintain one or more tracking devices to track the person;
- (b) install, use or maintain one or more tracking devices in or on any object used or worn, or likely to be used or worn, by the person;
- (c) install, use or maintain enhancement equipment in relation to the device or devices referred to in paragraph (a) or (b);
- (d) enter into or onto, or alter, the object referred to in paragraph (b);
- (e) any thing reasonably necessary to conceal the fact that any thing has been done in accordance with the authorisation;
- (f) any other thing reasonably incidental to any of the above.

Note: However, an internal authorisation cannot authorise the doing of certain things: see section 26K.

Things that may be authorised—object or class of object

- (2) If an internal authorisation is given in relation to an object or a class of object, the authorisation may authorise the Organisation to do, without warrant, one or more of the following:
 - (a) install, use or maintain one or more tracking devices in or on the specified object, or an object of the specified class;
 - (b) install, use or maintain enhancement equipment in relation to the device or devices;
 - (c) enter into or onto, or alter, the specified object, or an object of the specified class;
 - (d) any thing reasonably necessary to conceal the fact that any thing has been done in accordance with the authorisation;
 - (e) any other thing reasonably incidental to any of the above.

Note: However, an internal authorisation cannot authorise the doing of certain things: see section 26K.

26K Certain acts not authorised

Neither an internal authorisation nor section 26L authorises any of the following:

Section 26L

- (a) the doing of any thing that would involve either or both of the following:
 - (i) entering premises without permission from the owner or occupier of the premises;
 - (ii) interference with the interior of a vehicle without permission of the person having lawful possession or control of the vehicle;
- (b) the remote installation of a tracking device or enhancement equipment in relation to the device;
- (c) the installation, use or maintenance of a tracking device, or enhancement equipment in relation to the device, to listen to, record, observe or monitor the words, sounds or signals communicated to or by a person;
- (d) the doing of any thing by the Organisation if, apart from section 26G, the Organisation could not do the thing without it being authorised by a warrant issued under section 25A.

Note: Section 26L deals with the recovery of tracking devices.

26L Recovery of tracking devices

- (1) If a tracking device is installed, used or maintained under an internal authorisation, the Organisation is also authorised to do any of the following:
 - (a) recover the tracking device or any enhancement equipment in relation to the device;
 - (b) any thing reasonably necessary to conceal the fact that any thing has been done under this subsection;
 - (c) any other thing reasonably incidental to any of the above;at the following time:
 - (d) at any time while the authorisation is in force or within 28 days after it ceases to be in force;
 - (e) if the device or equipment is not recovered at a time mentioned in paragraph (d)—at the earliest time, after the 28 days mentioned in that paragraph, at which it is reasonably practicable to do the things concerned.

- (2) If, for the purposes of subsection (1), a tracking device or enhancement equipment in relation to the device is not recovered while the authorisation is in force, the Organisation is also authorised to use the device or equipment solely for the purposes of the location and recovery of the device or equipment.

Note: However, subsections (1) and (2) do not authorise the doing of a thing that would involve a thing specified in section 26K.

26M Exercise of authority under internal authorisations

The authority conferred by an internal authorisation or by section 26L may be exercised on behalf of the Organisation by:

- (a) an ASIO employee; or
- (b) an ASIO affiliate.

26N Variation of internal authorisations

Request for variation

- (1) An ASIO employee or ASIO affiliate (the ***applicant***) may request an authorising officer to vary an internal authorisation.
- (2) The request may be made:
 - (a) in writing; or
 - (b) orally in person, or by telephone or other means of communication.
- (3) A request under subsection (1) must include a statement of:
 - (a) the facts and other grounds on which the applicant considers it necessary that the authorisation should be varied; and
 - (b) the extent to which the applicant considers that the authorisation, as varied, will substantially assist the collection of intelligence in respect of the matter (the ***security matter***) that is important in relation to security in respect of which the authorisation is given.

Section 26P

- (4) If the request is made orally, a written record of the request that meets the requirements of subsection (3) must be made within 48 hours after the request is made.

Giving of variation

- (5) The authorising officer may vary the authorisation only if the authorising officer is satisfied that there are reasonable grounds for believing that the authorisation, as varied, will substantially assist the collection of intelligence in respect of the security matter.
- (6) If the variation extends, or further extends, the period during which the authorisation is in force, the total period during which the authorisation is in force must not exceed 90 days.
- (7) An internal authorisation may be varied more than once under this section.

Requirements for variations

- (8) A variation under this section may be given:
- (a) in writing; or
 - (b) orally in person, or by telephone or other means of communication.
- (9) If the variation is given orally, a written record of the variation must be made within 48 hours after the variation is given.

Written variations and records not legislative instruments

- (10) The following are not legislative instruments:
- (a) a variation under this section;
 - (b) a written record referred to in subsection (9).

26P Discontinuance of action before expiration of internal authorisation

- (1) Subject to subsections (3) and (4), if an authorising officer is satisfied that the grounds on which an internal authorisation was

given have ceased to exist, the authorising officer must, as soon as practicable, take such steps as are necessary to ensure that action under the internal authorisation is discontinued.

- (2) For the purposes of subsection (1), *action under an internal authorisation* does not include the recovery of a tracking device or any enhancement equipment in relation to the device.
- (3) If:
 - (a) an internal authorisation was given in relation to more than one of the matters mentioned in subsection 26G(2); and
 - (b) the grounds on which the internal authorisation was given continue to exist for at least one of those matters;subsection (1) applies only in relation to the matters for which the grounds have ceased to exist.
- (4) Subsection (1) does not apply to an authorising officer if another authorising officer has already taken, or started to take, such steps as are necessary to ensure that action under the internal authorisation is discontinued.

26Q Register of internal authorisations

- (1) The Director-General must establish and maintain a register of requests for internal authorisations.
- (2) The register may be kept by electronic means.
- (3) The register must include, for each request for an internal authorisation:
 - (a) the name of the person who made the request; and
 - (b) the matter that is important in relation to security in respect of which the authorisation was requested; and
 - (c) the day on which the authorisation was given or refused; and
 - (d) the name of the authorising officer who gave or refused to give the authorisation; and
 - (e) if the authorisation was given:

Section 26R

- (i) the day on which the authorisation ceased to be in force; and
- (ii) whether action under the authorisation was discontinued in accordance with section 26P, and, if so, the day on which the action was discontinued; and
- (f) the location at which any record relating to the request (including the request) is kept by the Organisation.

Note: For the purposes of paragraph (f), the location may be a physical location or an electronic location.

- (4) The register is not a legislative instrument.

26R Issue of warrants for recovery of tracking devices

Request for warrant

- (1) The Director-General may request the Attorney-General to issue a warrant under this section in respect of one or more tracking devices (the **relevant devices**), or enhancement equipment in relation to the device or devices (the **relevant equipment**), if:
 - (a) the relevant devices, or relevant equipment, were:
 - (i) installed in or on an object by the Organisation; or
 - (ii) used by the Organisation; or
 - (iii) maintained by the Organisation; and
 - (b) the installation, use or maintenance was not under:
 - (i) a surveillance device warrant; or
 - (ii) a warrant issued under section 27A; or
 - (iii) an identified person warrant; and
 - (c) recovery of the device or devices or equipment may involve either or both of the following:
 - (i) entering premises without permission from the owner or occupier of the premises;
 - (ii) interference with the interior of a vehicle without permission of the person having lawful possession or control of the vehicle.

Issue of warrant

- (2) The Attorney-General may issue a warrant in respect of the relevant devices or relevant equipment if the Attorney-General is satisfied that failure to recover the relevant devices or relevant equipment would be prejudicial to security.
- (3) In determining whether the warrant should be issued, the Attorney-General must have regard to the risk that information relating to the operations, capabilities or technologies of, or methods or sources used by, the Organisation will be communicated or made available to the public without the authority of the Commonwealth if the warrant is not issued.

Requirements for warrant

- (4) A warrant issued under this section must:
 - (a) be signed by the Attorney-General; and
 - (b) specify:
 - (i) details of the relevant devices or relevant equipment; and
 - (ii) the day the warrant is issued; and
 - (iii) the period during which the warrant is in force, which must not be more than 90 days; and
 - (iv) any restrictions or conditions that the Attorney-General considers appropriate in the circumstances; and
 - (c) authorise the use of any force against persons and things that is necessary and reasonable to do the things authorised by the warrant; and
 - (d) state whether entry to premises is authorised to be made at any time of the day or night or during stated hours of the day or night.
- (5) Subparagraph (4)(b)(iii) does not prevent the issuing of further warrants in relation to the same devices or equipment.

Section 26R

Authorisation in warrant

- (6) A warrant issued under this section in respect of relevant devices or relevant equipment authorises the Organisation to:
- (a) recover the devices or equipment; and
 - (b) do any of the following:
 - (i) use the devices or equipment solely for the purposes of locating the devices or equipment;
 - (ii) enter any premises where the devices or equipment are reasonably believed to be, for the purpose of recovering the devices or equipment;
 - (iii) enter any other premises for the purpose of gaining entry to or exiting the premises referred to in subparagraph (ii);
 - (iv) enter into or onto, or alter, an object for the purpose of recovering the devices or equipment;
 - (v) replace an object with an equivalent object for the purpose of recovering the devices or equipment;
 - (vi) break open any thing for the purpose of recovering the devices or equipment;
 - (vii) if the devices or equipment are installed in or on an object—temporarily remove the object from any place where it is situated for the purpose of recovering the devices or equipment and returning the object to that place;
 - (viii) use a nominal amount of electricity from any source to power the devices or equipment;
 - (ix) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
 - (x) use any force against persons and things that is necessary and reasonable to do any of the above;
 - (xi) any other thing reasonably incidental to any of the above.

Subdivision E—Inspection of postal and other articles

27 Inspection of postal articles

- (1) It is unlawful:
- (a) for a person, being the Director-General, an ASIO employee or an ASIO affiliate acting in his or her capacity as such, to seek from the Australian Postal Corporation or from an employee or agent of that Corporation; or
 - (b) for that Corporation or an employee or agent of that Corporation to provide to such a person;

access to a postal article that is in the course of the post or information concerning the contents or cover of any postal article except in pursuance of, or for the purposes of, a warrant under this Division, and it is the duty of the Director-General to take all reasonable steps to ensure that this subsection is not contravened.

- (2) Where, upon receipt by the Attorney-General of a request by the Director-General for the issue of a warrant under this section in relation to a person, the Attorney-General is satisfied that:
- (a) that person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (b) access by the Organisation to postal articles posted by or on behalf of, addressed to or intended to be received by, that person, while the articles are in the course of the post, will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security;

the Attorney-General may, by warrant under his or her hand, authorize the Organisation to do such of the following acts and things as the Attorney-General considers appropriate in the circumstances, namely, with respect to postal articles in the course of the post that were posted by or on behalf of, or are addressed to, that person or are reasonably suspected by a person authorized to exercise the authority of the Organisation under the warrant to be intended to be received by that person, to inspect, and make copies

Section 27

of, or of the covers of, the articles, and to open the articles and inspect and make copies of the contents of any such article.

- (3) Where, upon receipt by the Attorney-General of a request by the Director-General for the issue of a warrant under this section in relation to an address, the Attorney-General is satisfied that:
- (a) some or all of the postal articles that are being, or are likely to be, sent by post to that address are or will be intended to be received by a person (whether of known identity or not) engaged in, or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (b) access by the Organisation to postal articles posted to that address and intended to be received by the person referred to in paragraph (a) will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security;

the Attorney-General may, by warrant under his or her hand, authorize the Organisation to do such of the following acts and things as the Attorney-General considers appropriate in the circumstances, namely, with respect to postal articles in the course of the post that are addressed to that address and appear on their face to be, or are reasonably suspected by a person authorized to exercise the authority of the Organisation under the warrant to be, intended to be received by the person referred to in paragraph (a), to inspect, and make copies of, or of the covers of, the articles and to open the articles and inspect and make copies of the contents of any such article.

- (4) A warrant under this section shall specify the period for which it is to remain in force, being a period not exceeding 6 months, but may be revoked by the Attorney-General at any time before the expiration of the period so specified.
- (5) Subsection (4) shall not be construed as preventing the issue of any further warrant.
- (6) Where the Director-General is informed under section 32 of the issue of a warrant under this section, the Director-General must:

- (a) cause the Australian Postal Corporation to be informed of the issue of the warrant without delay; and
 - (b) where, under section 32, the Director-General receives the warrant—cause a certified copy of the warrant to be given to the Australian Postal Corporation as soon as practicable.
- (6A) Where:
- (a) the Director-General has been informed under section 32 of the issue of a warrant under this section; and
 - (b) the Director-General is informed under that section that the warrant has been revoked;
- the Director-General must:
- (c) cause the Australian Postal Corporation to be informed of the revocation without delay; and
 - (d) where, under section 32, the Director-General receives the instrument of revocation—cause a certified copy of the instrument of revocation to be given to the Australian Postal Corporation as soon as practicable.
- (7) The Australian Postal Corporation shall give to a person acting in pursuance of a warrant under this section all reasonable assistance.
- (8) Nothing in Part VIIA of the *Crimes Act 1914* or the *Australian Postal Corporation Act 1989* shall be taken to prohibit the doing of anything in pursuance of, or for the purposes of, a warrant under this section.
- (9) Nothing in subsection (1) applies in relation to a postal article addressed to, or appearing to be intended to be received by or on behalf of, the Organisation.

- (10) In this section:

address means any premises or place (including a post office box or bag service) to which postal articles may be addressed.

agent, in relation to the Australian Postal Corporation, includes any person performing services for that Corporation otherwise than under a contract of service and an employee of such a person.

27AA Inspection of delivery service articles

Unlawful access to delivery service articles

- (1) It is unlawful for:
- (a) the Director-General, an ASIO employee or an ASIO affiliate, for the purposes of the Organisation, to seek from a delivery service provider or from an employee or agent of a delivery service provider; or
 - (b) a delivery service provider or an employee or agent of a delivery service provider to give the Director-General, an ASIO employee or an ASIO affiliate, for the purposes of the Organisation;

access to:

- (c) an article that is being delivered by the delivery service provider; or
- (d) information concerning the contents or cover of any such article;

except in accordance with, or for the purposes of, a warrant under this Division. It is the duty of the Director-General to take all reasonable steps to ensure that this subsection is not contravened.

Note: ***Delivery service provider, agent*** and ***article*** are defined in subsection (12).

Issue of delivery services warrant

- (2) If the Director-General requests the Attorney-General to do so, and the Attorney-General is satisfied as mentioned in subsection (3) or (6), the Attorney-General may issue a warrant in accordance with this section.

Test 1 for issue of warrant

- (3) The Attorney-General may issue a warrant if he or she is satisfied that:
- (a) a person (the ***subject***) is engaged in or is reasonably suspected by the Director-General of being engaged in, or of

being likely to engage in, activities prejudicial to security;
and

- (b) access by the Organisation to articles sent by or on behalf of, addressed to or intended to be received by, the subject while the articles are being delivered by a delivery service provider, will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security.

Authorisation in warrant

- (4) The warrant must be signed by the Attorney-General and must authorise the Organisation to do specified things, subject to any restrictions or conditions specified in the warrant, in relation to articles that:
 - (a) are being delivered by the delivery service provider; and
 - (b) in respect of which any of the following are satisfied:
 - (i) the articles have been sent by or on behalf of the subject, who must be specified in the warrant, or addressed to the subject; or
 - (ii) the articles are reasonably suspected, by a person authorised to exercise the authority of the Organisation under the warrant, of having been so sent or addressed; or
 - (iii) the articles are intended to be received by the subject, who must be specified in the warrant, or are reasonably suspected, by a person authorised to exercise the authority of the Organisation under the warrant, of being intended to be received by the subject.

Things that may be specified for a warrant issued under subsection (3)

- (5) The things that may be specified are any of the following that the Attorney-General considers appropriate in the circumstances:
 - (a) inspecting or making copies of the articles or the covers of the articles;
 - (b) opening the articles;

Section 27AA

- (c) inspecting and making copies of the contents of the articles;
- (d) any other thing reasonably incidental to any of the above.

Test 2 for issue of warrant

- (6) The Attorney-General may issue a warrant if he or she is satisfied that:
 - (a) some or all of the articles that are being, or are likely to be, sent by a delivery service provider to an address (the **subject address**) are, or will be intended to be, received by a person (the **subject**) (whether of known identity or not) engaged in, or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (b) access by the Organisation to articles sent to, or intended to be received by, the subject while the articles are being delivered by a delivery service provider will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security.

Authorisation in warrant

- (7) The warrant must be signed by the Attorney-General and must authorise the Organisation to do specified things, subject to any restrictions or conditions specified in the warrant, in relation to articles that:
 - (a) are being delivered by the delivery service provider; and
 - (b) are addressed to the subject address, which must be specified in the warrant; and
 - (c) appear on their face to be, or are reasonably suspected by a person authorised to exercise the authority of the Organisation under the warrant to be, intended to be received by the subject.

Things that may be specified for warrant issued under subsection (6)

- (8) The things that may be specified are any of the following that the Attorney-General considers appropriate in the circumstances:
- (a) inspecting or making copies of any of the articles or the covers of the articles;
 - (b) opening any of the articles;
 - (c) inspecting and making copies of the contents of any of the articles;
 - (d) any other thing reasonably incidental to any of the above.

Duration of warrant

- (9) A warrant issued under this section must specify the period during which it is to remain in force. The period must not be more than 6 months, although the Attorney-General may revoke the warrant before the period has expired.

Issue of further warrants not prevented

- (10) Subsection (9) does not prevent the issue of any further warrant.

Definitions

- (11) To avoid doubt, the expression **deliver** an article includes any thing done by the deliverer, for the purpose of delivering the article, from the time when the article is given to the deliverer by the sender until it is given by the deliverer to the recipient.

- (12) In this section:

agent, in relation to a delivery service provider, includes:

- (a) any person performing services for the delivery service provider otherwise than under a contract of service; and
- (b) an employee of the person mentioned in paragraph (a).

article means any object reasonably capable of being sent through the post.

delivery service provider means a person whose business is or includes delivering articles.

Subdivision F—Foreign intelligence

27A Warrants for the performance of functions under paragraph 17(1)(e)

(1) Where:

- (a) the Director-General gives a notice in writing to the Attorney-General requesting the Attorney-General to issue a warrant under this section in relation to premises, a person, a computer or an object identified in the notice authorising the Organisation to do acts or things referred to in whichever of subsections 25(4) or (5), 25A(4), 26B(1), (2), (3) or (4), 27(2) or (3) or 27AA(5) or (8) is or are specified in the notice for the purpose of obtaining foreign intelligence relating to a matter specified in the notice; and
- (b) the Attorney-General is satisfied, on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, that the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being;

the Attorney-General may, by warrant under his or her hand, authorise the Organisation, subject to any conditions or restrictions that are specified in the warrant, to do such of those acts or things in relation to those premises, that person, that computer or those objects as the Attorney-General considers appropriate in the circumstances and are specified in the warrant for the purpose of obtaining that intelligence.

(2) The warrant must:

- (a) authorise the use of any force against persons and things that is necessary and reasonable to do the things mentioned in subsection (1); and

- (b) if the warrant authorises entering premises—state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.
- (3) A warrant under this section shall specify the period for which it is to remain in force, being a period not exceeding:
- (a) in a case where the warrant authorises the doing of acts or things referred to in subsection 25(4) or (5)—90 days;
 - (b) in a case where the warrant authorises the doing of acts or things referred to in subsection 25A(4), 26B(1), (2), (3) or (4), 27(2) or (3) or 27AA(5) or (8)—6 months;
- but may be revoked by the Attorney-General at any time before the end of the period so specified.
- (3A) If a surveillance device is installed or used in accordance with a warrant under this section authorising the doing of acts referred to in subsection 26B(1) (2), (3) or (4), the Organisation is authorised to do any of the following:
- (a) recover the surveillance device or any enhancement equipment in relation to the device;
 - (b) enter any premises where the surveillance device is reasonably believed to be, for the purpose of recovering the device or the equipment;
 - (c) enter any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (b);
 - (d) enter into or onto, or alter, an object for the purpose of recovering the device or the equipment;
 - (e) replace an object with an equivalent object for the purposes of recovering the device or the equipment;
 - (f) break open any thing for the purpose of recovering the device or the equipment;
 - (g) if the device or equipment is installed in or on an object—temporarily remove the object from any place where it is situated for the purpose of recovering the device or the equipment and returning the object to that place;
 - (h) use a nominal amount of electricity from any source to power the device or equipment;

Section 27A

- (i) any thing reasonably necessary to conceal the fact that any thing has been done under this subsection;
 - (j) use any force against persons and things that is necessary and reasonable to do any of the above;
 - (k) any other thing reasonably incidental to any of the above;
- at the following time:
- (l) at any time while the warrant is in force or within 28 days after it ceases to be in force;
 - (m) if the surveillance device is not recovered at a time mentioned in paragraph (l)—at the earliest time, after the 28 days mentioned in that paragraph, at which it is reasonably practicable to do the things concerned.

(3B) If, for the purposes of subsection (3A):

- (a) the surveillance device is not recovered while the warrant is in force; and
- (b) the surveillance device is a tracking device;

the Organisation is also authorised to use the surveillance device or any enhancement equipment in relation to the device solely for the purposes of the location and recovery of the device or equipment.

(3C) If any thing has been done in relation to a computer under:

- (a) a warrant under this section that authorises the Organisation to do acts or things referred to in subsection 25A(4); or
- (b) this subsection;

the Organisation is authorised to do any of the following:

- (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;
- (d) enter any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);
- (e) enter any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);
- (f) remove the computer or another thing from any place where it is situated for the purposes of doing the things mentioned

- in paragraph (c), and returning the computer or other thing to that place;
- (g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) use any other computer or a communication in transit to do those things; and
 - (ii) if necessary to achieve that purpose—add, copy, delete or alter other data in the computer or the communication in transit;
 - (h) intercept a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing mentioned in this subsection;
 - (i) any other thing reasonably incidental to any of the above;
- at the following time:
- (j) at any time while the warrant is in force or within 28 days after it ceases to be in force;
 - (k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).
- (3D) Subsection (3C) does not authorise the doing of a thing that is likely to:
- (a) materially interfere with, interrupt or obstruct:
 - (i) a communication in transit; or
 - (ii) the lawful use by other persons of a computer;unless the doing of the thing is necessary to do one or more of the things specified in subsection (3C); or
 - (b) cause any other material loss or damage to other persons lawfully using a computer.
- (3E) If a computer or another thing is removed from a place in accordance with paragraph (3C)(f), the computer or thing must be returned to that place:

Section 27A

- (a) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
 - (b) otherwise—within a reasonable period.
- (4) Subsection (3) shall not be construed as preventing the issue of any further warrant.
- (6) Where the Director-General is informed under section 32 of the issue of a warrant under this section authorising the doing of acts or things referred to in subsection 27(2) or (3), the Director-General must:
 - (a) cause the Australian Postal Corporation to be informed of the issue of the warrant without delay; and
 - (b) where, under section 32, the Director-General receives the warrant—cause a certified copy of the warrant to be given to the Australian Postal Corporation as soon as practicable.
- (6A) Where:
 - (a) the Director-General has been informed under section 32 of the issue of a warrant under this section authorising the doing of acts or things referred to in subsection 27(2) or (3); and
 - (b) the Director-General is informed under section 32 that the warrant has been revoked;the Director-General must:
 - (c) cause the Australian Postal Corporation to be informed of the revocation without delay; and
 - (d) where, under section 32, the Director-General receives the instrument of revocation—cause a certified copy of the instrument of revocation to be given to the Australian Postal Corporation as soon as practicable.
- (7) The Australian Postal Corporation shall give to a person acting pursuant to a warrant under this section authorising the doing of acts or things referred to in subsection 27(2) or (3) all reasonable assistance.

Section 27B

- (8) Nothing in Part VIIA of the *Crimes Act 1914* or the *Australian Postal Corporation Act 1989* shall be taken to prohibit the doing of anything pursuant to, or for the purposes of, a warrant under this section.
- (9) The Director-General shall not request the issue of a warrant under this section for the purpose of collecting information concerning an Australian citizen or a permanent resident, unless the Director-General reasonably suspects that the person is acting for, or on behalf of, a foreign power.
- (9A) If the Director-General of Security requests the issue of a warrant under this section for the purpose of collecting information concerning a person who is an Australian citizen or permanent resident (see subsection (9)), then:
- (a) the Director-General must include details in the request about the grounds on which the Director-General suspects that the person is acting for, or on behalf of, a foreign power; and
 - (b) the Attorney-General must not issue the warrant unless the Attorney-General is satisfied that the person is, or is reasonably suspected by the Director-General of, acting for, or on behalf of, a foreign power.
- (10) The reference in subsection (1) to conditions or restrictions includes a reference to conditions or restrictions designed to minimise the obtaining by the Organisation, pursuant to a warrant issued under that subsection, of information that is not publicly available concerning Australian citizens or permanent residents, or to minimise the retention of information of that kind.

27B Performance of other functions under paragraph 17(1)(e)

If:

- (a) the Director-General gives a notice in writing to the Attorney-General requesting the Attorney-General to authorise the Organisation to obtain foreign intelligence in relation to a matter specified in the notice; and

Section 27C

- (b) the Attorney-General is satisfied, on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, that the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being;

the Attorney-General may, by writing signed by the Attorney-General, authorise the Organisation to obtain the intelligence in relation to the matter.

Subdivision G—Identified person warrants

27C Issue of identified person warrants

Issue of warrant

- (1) If the Director-General requests the Attorney-General to do so, and the Attorney-General is satisfied as mentioned in subsection (2), the Attorney-General may issue an identified person warrant in relation to a particular person.

Test for issue of warrant

- (2) The Attorney-General is only to issue an identified person warrant in relation to the person if he or she is satisfied that:
- (a) the person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
 - (b) the issuing of the warrant in relation to the person will, or is likely to, substantially assist the collection of intelligence relevant to security.

Requirements for warrant

- (3) The identified person warrant must:
- (a) be signed by the Attorney-General; and
 - (b) identify the person:

- (i) if the name of the person is known—by specifying the person's name; or
 - (ii) otherwise—by including other details sufficient to identify the person; and
- (c) give conditional approval for the Organisation to do one or more of the following:
- (i) access records or other things in or on premises;
 - (ii) access data held in computers;
 - (iii) use one or more kinds of surveillance devices;
 - (iv) access postal articles that are in the course of the post;
 - (v) access articles that are being delivered by a delivery service provider.

Note: Conditional approval does not, of itself, authorise the Organisation to do things under an identified person warrant. Things can only be done under the warrant if the Organisation is subsequently authorised to do those things: see sections 27D to 27H.

Duration of warrant

- (4) An identified person warrant must specify the period during which it is to remain in force. The period must not be more than 6 months, although the Attorney-General may revoke the warrant before the period has expired.

Issue of further warrants not prevented

- (5) Subsection (4) does not prevent the issue of any further warrant.

Warrant may be subject to restrictions or conditions

- (6) An identified person warrant is subject to any restrictions or conditions specified in it.

27D Authority under identified person warrant—search of premises and persons

- (1) This section applies if an identified person warrant in relation to a person (the *identified person*) gives conditional approval for the Organisation to access records or other things in or on premises.

Things that may be authorised under warrant

- (2) Subject to subsection (3), the Attorney-General or the Director-General may, on request, authorise the Organisation to do one or more of the following things under the identified person warrant in relation to one or more specified premises (the *subject premises*):
- (a) enter the subject premises;
 - (b) enter any premises for the purposes of gaining entry to or exiting the subject premises;
 - (c) search the subject premises for the purpose of finding records or other things relevant to the prejudicial activities of the identified person;
 - (d) open any safe, box, drawer, parcel, envelope or other container in or on the premises in which there is reasonable cause to believe that records or other things relevant to the prejudicial activities of the identified person may be found;
 - (e) conduct an ordinary search or a frisk search of the identified person or any other person if:
 - (i) the person is at or near the subject premises when the authority given by this subsection is exercised; and
 - (ii) there is reasonable cause to believe that the person has, on his or her person, records or other things that are relevant to the prejudicial activities of the identified person;
 - (f) inspect or otherwise examine any records or other things so found, and make copies or transcripts of any such record or other thing that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;

- (g) remove and retain any record or other thing so found, for the purposes of:
 - (i) inspecting or examining it; and
 - (ii) making copies or transcripts of it;
- (h) if there is reasonable cause to believe that data relevant to the prejudicial activities of the identified person may be accessible by using a computer or other electronic equipment, or a data storage device, brought to or found on the subject premises—use the computer, equipment or device for the purpose of obtaining access to any such data and, if necessary to achieve that purpose, add, copy, delete or alter other data in the computer, equipment or device;
- (i) if paragraph (h) applies—use the computer, equipment or device to do any of the following:
 - (i) inspect and examine any data to which access has been obtained;
 - (ii) convert any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, into documentary form and removing any such document;
 - (iii) copy any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, to any data storage device and remove the device;
- (j) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
- (k) any other thing reasonably incidental to any of the above.

Test for authorisation

- (3) The Attorney-General or the Director-General is only to give an authorisation under subsection (2) if the Attorney-General or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant in relation to the subject premises will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

Section 27E

Additional rules applying to authorisations

- (4) An ordinary search or frisk search of a person that is authorised under paragraph (2)(e) must, if practicable, be conducted by a person of the same sex as the person being searched.
- (5) A record or other thing retained as mentioned in paragraph (2)(g) may be retained:
 - (a) if returning the record or thing would be prejudicial to security—only until returning the record or thing would no longer be prejudicial to security; and
 - (b) otherwise—for only such time as is reasonable.

Certain acts not authorised

- (6) Paragraph (2)(e) does not authorise a strip search or a search of a person's body cavities.
- (7) Paragraphs (2)(h) to (k) do not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:
 - (a) materially interfere with, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises unless the addition, deletion or alteration, or the doing of the thing, is necessary to do the things authorised under one or more of those paragraphs; or
 - (b) cause any other material loss or damage to other persons lawfully using the computer, equipment or device.

27E Authority under identified person warrant—computer access

- (1) This section applies if an identified person warrant in relation to a person (the *identified person*) gives conditional approval for the Organisation to access data held in computers.

Things that may be authorised under warrant

- (2) Subject to subsection (4), the Attorney-General or the Director-General may, on request, authorise the Organisation to do

Section 27E

one or more of the following things under the identified person warrant in relation to a computer (the *target computer*):

- (a) enter specified premises for the purposes of doing the things authorised under this subsection;
- (b) enter any premises for the purposes of gaining entry to or exiting the specified premises;
- (c) use:
 - (i) the target computer; or
 - (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
 - (iii) any other electronic equipment; or
 - (iv) a data storage device;for the purpose of obtaining access to data (the *relevant data*) that is relevant to the prejudicial activities of the identified person and is held in the target computer at any time while the authorisation is in force and, if necessary to achieve that purpose, add, copy, delete or alter other data in the target computer;
- (d) if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) use any other computer or a communication in transit for the purpose referred to in paragraph (c); and
 - (ii) if necessary to achieve that purpose—add, copy, delete or alter other data in the computer or the communication in transit;
- (da) remove a computer or other thing from premises for the purposes of doing any thing authorised under this subsection, and returning the computer or other thing to the premises;
- (e) copy any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;
- (ea) intercept a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing authorised under this subsection;

Section 27E

- (f) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
- (g) any other thing reasonably incidental to any of the above.

Target computer

- (3) For the purposes of subsection (2), the target computer may be any one or more of the following:
 - (a) a particular computer;
 - (b) a computer on particular premises;
 - (c) a computer associated with, used by or likely to be used by a person (whose identity may or may not be known).

Return of computer or other thing

- (3A) If:
 - (a) an authorisation under subsection (2) authorises the removal of a computer or other thing from premises as mentioned in paragraph (2)(da); and
 - (b) a computer or thing is removed from the premises in accordance with the authorisation;the computer or thing must be returned to the premises:
 - (c) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
 - (d) otherwise—within a reasonable period.

Test for authorisation

- (4) The Attorney-General or the Director-General is only to give an authorisation under subsection (2) if the Attorney-General or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant in relation to the target computer will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

Certain acts not authorised

- (5) Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:
- (a) materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things authorised under subsection (2); or
 - (b) cause any other material loss or damage to other persons lawfully using a computer.

Concealment of access etc.

- (6) If any thing has been done in relation to a computer under:
- (a) a subsection (2) authorisation; or
 - (b) under this subsection;
- the Organisation is authorised to do any of the following:
- (c) any thing reasonably necessary to conceal the fact that any thing has been done under the subsection (2) authorisation or under this subsection;
 - (d) enter any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);
 - (e) enter any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);
 - (f) remove the computer or another thing from any place where it is situated for the purposes of doing the things mentioned in paragraph (c), and returning the computer or other thing to that place;
 - (g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) use any other computer or a communication in transit to do those things; and

Section 27E

- (ii) if necessary to achieve that purpose—add, copy, delete or alter other data in the computer or the communication in transit;
 - (h) intercept a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing mentioned in this subsection;
 - (i) any other thing reasonably incidental to any of the above;at the following time:
 - (j) at any time while the authorisation is in force or within 28 days after it ceases to be in force;
 - (k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).
- (7) Subsection (6) does not authorise the doing of a thing that is likely to:
 - (a) materially interfere with, interrupt or obstruct:
 - (i) a communication in transit; or
 - (ii) the lawful use by other persons of a computer;unless the doing of the thing is necessary to do one or more of the things specified in subsection (6); or
 - (b) cause any other material loss or damage to other persons lawfully using a computer.
- (8) If a computer or another thing is removed from a place in accordance with paragraph (6)(f), the computer or thing must be returned to the place:
 - (a) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
 - (b) otherwise—within a reasonable period.

27F Authority under identified person warrant—surveillance devices

- (1) This section applies if an identified person warrant in relation to a person (the *identified person*) gives conditional approval for the Organisation to use one or more kinds of surveillance devices.

Things that may be authorised under warrant

- (2) Subject to subsection (3), the Attorney-General or the Director-General may, on request, authorise the Organisation to do one or more of the following things under the identified person warrant:
- (a) install, use and maintain surveillance devices of the kind specified in the conditional approval to:
 - (i) listen to, record, observe or monitor the words, sounds or signals communicated to or by the identified person, or the activities of the identified person; or
 - (ii) track the identified person;
 - (b) install, use and maintain surveillance devices of the kind specified in the conditional approval:
 - (i) in or on premises where the identified person is reasonably believed to be or likely to be; or
 - (ii) in or on any other specified premises from which the activities of the identified person, or the words, sounds or signals communicated by or to the identified person, can be listened to, recorded, observed or monitored;
 - (c) enter the premises referred to in paragraph (b) for any of the purposes referred to in paragraph (a) or (b) or in subsection 26B(4), (5) or (6) (as those subsections apply because of this section);
 - (d) install, use and maintain surveillance devices of the kind specified in the conditional approval in or on any object used or worn, or likely to be used or worn, by the identified person;
 - (e) enter into or onto, or alter, an object referred to in paragraph (d);

Section 27G

- (f) enter any premises in which an object referred to in paragraph (d) is or is likely to be found, for any of the purposes referred to in that paragraph or in subsection 26B(4), (5) or (6) (as those subsections apply because of this section);
- (g) enter any other premises, for the purposes of gaining entry to or exiting premises referred to in paragraph (b) or (f);
- (h) any other thing reasonably incidental to any of the above.

Test for authorisation

- (3) The Attorney-General or the Director-General is only to give an authorisation under subsection (2) if the Attorney-General or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.
- (4) If an authorisation is given under subsection (2) in relation to a surveillance device, the identified person warrant under which the authorisation is given also authorises the Organisation to do the things mentioned in subsection 26B(4) in relation to the device.
- (5) If the Organisation installs or uses a surveillance device under the identified person warrant, the Organisation is authorised to do the things mentioned in subsections 26B(5) and (6) in relation to the device.
- (6) For the purposes of subsections (4) and (5) of this section, section 26B applies as if references in that section to a surveillance device warrant were references to an identified person warrant.

27G Authority under identified person warrant—inspection of postal articles

- (1) This section applies if an identified person warrant in relation to a person (the *identified person*) gives conditional approval for the Organisation to access postal articles while the articles are in the course of the post.

Things that may be authorised under warrant

- (2) Subject to subsection (4), the Attorney-General or the Director-General may, on request, authorise the Organisation to do one or more of the things mentioned in subsection (3) under the identified person warrant in relation to any of the following:
- (a) articles posted by or on behalf of the identified person;
 - (b) articles addressed to the identified person;
 - (c) articles reasonably suspected by a person authorised to exercise the authority of the Organisation under the warrant to be intended to be received by the identified person.
- (3) The things are as follows:
- (a) inspect and make copies of the articles, or the covers of the articles;
 - (b) open the articles;
 - (c) inspect and make copies of the contents of the articles;
 - (d) any other thing reasonably incidental to any of the above.

Test for authorisation

- (4) The Attorney-General or the Director-General is only to give an authorisation under subsection (2) if the Attorney-General or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

Rules relating to the Australian Postal Corporation

- (5) If an authorisation is given under this section, the Director-General must, as soon as practicable:
- (a) inform the Australian Postal Corporation of that fact; and
 - (b) give a certified copy of the authorisation to the Australian Postal Corporation.
- (6) If either of the following is revoked:
- (a) an authorisation under this section;

Section 27H

- (b) the identified person warrant under which the authorisation is given;
- the Director-General must:
- (c) inform the Australian Postal Corporation of that fact; and
 - (d) give a certified copy of the instrument of revocation to the Australian Postal Corporation.
- (7) The Australian Postal Corporation must provide all reasonable assistance to a person acting in accordance with an authorisation under this section.

Relationship with other laws

- (8) Nothing in Part VIIA of the *Crimes Act 1914* or the *Australian Postal Corporation Act 1989* prohibits the doing of anything under or for the purposes of an authorisation under this section.

27H Authority under identified person warrant—inspection of delivery articles

- (1) This section applies if an identified person warrant in relation to a person (the *identified person*) gives conditional approval for the Organisation to access articles while the articles are being delivered by a delivery service provider.

Things that may be authorised under warrant

- (2) Subject to subsection (4), the Attorney-General or the Director-General may, on request, authorise the Organisation to do one or more of the things mentioned in subsection (3) in relation to any of the following:
- (a) articles posted by or on behalf of the identified person;
 - (b) articles addressed to the identified person;
 - (c) articles reasonably suspected by a person authorised to exercise the authority of the Organisation under the warrant to be intended to be received by the identified person.
- (3) The things are as follows:

- (a) inspect and make copies of the articles, or the covers of the articles;
- (b) open the articles;
- (c) inspect and make copies of the contents of the articles;
- (d) any other thing reasonably incidental to any of the above.

Test for authorisation

- (4) The Attorney-General or the Director-General is only to give an authorisation under subsection (2) if the Attorney-General or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

Definitions

- (5) In this section:

article has the same meaning as in section 27AA.

delivery service provider has the same meaning as in section 27AA.

27J Authority under identified person warrants—general rules

Requests for authorisations

- (1) A request for an authorisation under this Subdivision may be made:
 - (a) if the request is to the Attorney-General—by the Director-General; or
 - (b) if the request is to the Director-General—by an ASIO employee or an ASIO affiliate.
- (2) The request must specify the facts and other grounds on which the person making the request considers it necessary that the authorisation should be given.

Section 27J

Requirements for authorisations

- (3) An authorisation under this Subdivision:
- (a) must be in writing; and
 - (b) must identify the identified person warrant under which the authorisation is given; and
 - (c) must specify:
 - (i) for an authorisation under section 27D (search of premises or persons)—the subject premises; and
 - (ii) for an authorisation under section 27E (computer access)—the target computer; and
 - (iii) the thing or things that are authorised to be done; and
 - (iv) the restrictions or conditions (if any) to which the authorisation is subject; and
 - (v) the period during which the authorisation is in force; and
 - (d) must authorise the use of any force against persons and things that is necessary and reasonable to do the things covered by the authorisation; and
 - (e) if the authorisation authorises entering premises—must state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.
- (4) A restriction or condition specified in an authorisation must not be inconsistent with any restrictions or conditions specified in the identified person warrant under which the authorisation is given.
- (5) For the purposes of subparagraph (3)(c)(v), the period:
- (a) in the case of an authorisation under section 27D (search of premises and persons)—must not be more than 90 days; and
 - (b) in any case—must not end after the end of the period for which the identified person warrant under which the authorisation is given is in force.

When authorisations cease to be in force

- (6) An authorisation under this Subdivision ceases to be in force at the earliest of the following times:
- (a) the time the identified person warrant under which the authorisation is given ceases to be in force;
 - (b) the time it is revoked by the Attorney-General or the Director-General;
 - (c) the time specified in the authorisation.

Other matters

- (7) To avoid doubt, for the purposes of this Act, the authority conferred by an identified person warrant includes the authority conferred by an authorisation under this Subdivision under the warrant.
- (8) To avoid doubt, nothing in this Subdivision prevents 2 or more authorisations under this Subdivision from being given under the same identified persons warrant at any time while the warrant is in force.
- (9) An authorisation under this Subdivision is not a legislative instrument.

Subdivision H—General provisions relating to warrants and authorisations

28 Request for warrant to specify grounds

A request by the Director-General for the issue of a warrant under this Division shall specify the facts and other grounds on which the Director-General considers it necessary that the warrant should be issued and (where appropriate) the grounds on which the Director-General suspects a person of being engaged in, or of being likely to engage in, activities prejudicial to security.

29 Issue of certain warrants by Director-General in emergency

- (1) Where:
- (a) the Director-General has forwarded or made a request to the Attorney-General for the issue of a warrant under section 25, 25A, 26, 26R, 27 or 27AA;
 - (b) the Attorney-General has not, to the knowledge of the Director-General, issued, or refused to issue, a warrant as a result of the request and has not, within the preceding period of 3 months, refused to issue a substantially similar warrant;
 - (c) the Director-General has not, within the preceding period of 3 months, issued a substantially similar warrant; and
 - (d) the Director-General is satisfied:
 - (i) that the facts of the case would justify the issue of a warrant by the Attorney-General; and
 - (ii) that, if the action to be authorized by the warrant does not commence before a warrant can be issued and made available by the Attorney-General, security will be, or is likely to be, seriously prejudiced;
- the Director-General may issue a warrant signed by the Director-General of the kind that could be issued by the Attorney-General in pursuance of the request.
- (2) A warrant under this section shall specify the period for which it is to remain in force, being a period that does not exceed 48 hours, but may be revoked by the Attorney-General at any time before the expiration of the period so specified.
- (3) Where the Director-General issues a warrant under this section, the Director-General shall forthwith furnish to the Attorney-General:
- (a) a copy of the warrant; and
 - (b) a statement of the grounds on which the Director-General is satisfied as to the matter referred to in subparagraph (1)(d)(ii).
- (4) The Director-General must, within 3 working days after issuing a warrant under this section, give a copy of the warrant to the Inspector-General of Intelligence and Security.
-

29A Variation of warrants issued under this Division

- (1) The Attorney-General may, on request by the Director-General, vary a warrant issued under this Division (other than under section 29).
- (2) The variation must be in writing.
- (3) If the variation extends, or further extends, the period during which the warrant is in force, the total period during which the warrant is in force must not exceed:
 - (a) for a warrant issued under section 25 or 26R—90 days; or
 - (b) for a warrant issued under section 25A, 26, 27, 27AA or 27C—6 months.
- (4) The request by the Director-General must specify:
 - (a) the facts and other grounds on which the Director-General considers it necessary that the warrant should be varied; and
 - (b) where appropriate—the grounds on which the Director-General suspects a person of being engaged in or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security.
- (5) A warrant may be varied more than once under this section.

30 Discontinuance of action before expiration of warrant

- (1) Subject to subsection (3), if the Director-General is satisfied that the grounds on which a warrant under this Division was issued have ceased to exist, the Director-General must, as soon as practicable:
 - (a) inform the Attorney-General of that fact; and
 - (b) take such steps as are necessary to ensure that action under the warrant is discontinued.
- (2) For the purposes of paragraph (1)(b), *action under a warrant*:

Section 31

- (a) if the warrant is issued under section 26R—includes the recovery of a tracking device or any enhancement equipment in relation to the device; or
 - (b) otherwise:
 - (i) includes action under an authorisation given under an identified person warrant; but
 - (ii) does not include the recovery of a surveillance device or any enhancement equipment in relation to the device.
- (3) If:
- (a) a surveillance device warrant was issued in relation to more than one of the matters mentioned in paragraph 26(2)(a); and
 - (b) the grounds on which the warrant was issued continue to exist for at least one of those matters;
- subsection (1) applies only in relation to the matters for which the grounds have ceased to exist.

31 Certain records obtained under a warrant to be destroyed

Where:

- (a) by virtue of a warrant under this Division, a record or copy has been made;
- (b) the record or copy is in the possession or custody, or under the control, of the Organisation; and
- (c) the Director-General is satisfied that the record or copy is not required for the purposes of the performance of functions or exercise of powers under this Act;

the Director-General shall cause the record or copy to be destroyed.

31A Notification requirements in relation to the use of force under warrant

- (1) This section applies if a warrant issued under this Division authorises the use of force against persons to do the things authorised by the warrant.

- (2) The Director-General must cause the Attorney-General and the Inspector-General of Intelligence and Security to be notified if such force is used against a person in the execution of the warrant.
- (3) The notification must be given:
 - (a) in writing; and
 - (b) as soon as practicable after such force is used.

32 Certain action in relation to requests and warrants

- (1) Where the Director-General makes a request, otherwise than in writing, for the issue of a warrant under this Division, the Director-General shall forthwith forward to the Attorney-General a request in writing for the issue of a warrant.
- (2) Where the Attorney-General issues or revokes a warrant under this Division, the Attorney-General shall:
 - (a) cause the Director-General to be informed forthwith of the issue of the warrant or of the revocation, as the case may be; and
 - (b) cause the warrant or the instrument of revocation, as the case may be, to be forwarded as soon as practicable to the Director-General.
- (3) The Attorney-General shall record on each request in writing for the issue of a warrant under this Division received by the Attorney-General from the Director-General the Attorney-General's decision with respect to the request and shall cause the request to be returned to the Director-General.
- (4) The Director-General shall cause to be retained in the records of the Organisation all warrants issued by the Director-General under this Division and all warrants and instruments of revocation received by the Director-General from, and all requests and other documents returned to the Director-General by, the Attorney-General under this Division.

Section 33

33 Relationship with other laws

Listening devices—relationship with the Telecommunications (Interception and Access) Act 1979

- (2) Nothing in section 26B, 27A or 27F, or in a warrant or authorisation under those sections, applies to or in relation to the use of a listening device for a purpose that would, for the purposes of the *Telecommunications (Interception and Access) Act 1979*, constitute the interception of a communication passing over a telecommunications system operated by a carrier or a carriage service provider.

Surveillance devices—interaction with other laws

- (3) Despite any other law of the Commonwealth, a State or a Territory (including the common law), a person acting on behalf of the Organisation does not act unlawfully by installing, using, maintaining or recovering a surveillance device if the person does so:
- (a) in accordance with a warrant issued under section 26, 26R, 27A or 27C; or
 - (aa) in accordance with an authorisation given under section 26G; or
 - (b) in accordance with subsection 26B(5) or (6), section 26C, 26D, or 26E, or subsection 27A(3A) or (3B) or 27F(5).
- (4) Nothing in this Division makes the use, installation, maintenance or recovery by the Organisation of a surveillance device lawful if the use, installation, maintenance or recovery would be prohibited under an applicable law of the Commonwealth, a State or a Territory (including the common law), unless the Organisation does so:
- (a) in accordance with a warrant issued under section 26, 27A or 27C; or
 - (b) in accordance with an authorisation given under section 26G; or

- (c) in accordance with subsection 26B(5) or (6), section 26C, 26D or 26E, or subsection 27A(3A) or (3B) or 27F(5).

34 Director-General to report to Attorney-General—general

- (1) The Director-General shall furnish to the Attorney-General in respect of each warrant issued under this Division a report in writing on the extent to which the action taken under the warrant has assisted the Organisation in carrying out its functions.
- (1A) If an order was made under subsection 34AAD(2) in relation to the warrant, the report must also include details of the extent to which compliance with the order has assisted the Organisation in carrying out its functions.
- (2) If:
- (a) the warrant was issued under section 25, 25A, 27A, 27C or 29; and
 - (b) a thing mentioned in subsection 25(5) or 25A(4) or (8) or 27A(3C), paragraph 27D(2)(h) to (k) or subsection 27E(2) or (6) was done under the warrant;
- the report must also include details of anything done that materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment, or a data storage device.
- (3) For the purposes of this section, any thing done under subsection 25A(8) is taken to have been done under a warrant issued under section 25A.
- (4) For the purposes of this section, any thing done under subsection 27A(3C) is taken to have been done under a warrant issued under section 27A.
- (5) For the purposes of this section, any thing done under subsection 27E(6) is taken to have been done under a warrant issued under section 27C.

**34AAA Director-General to report to Attorney-General—
concealment of access**

(1) If:

- (a) a warrant issued under this Division has ceased to be in force; and
- (b) during a prescribed post-cessation period of the warrant, a thing was done under subsection 25A(8), 27A(3C) or 27E(6) in connection with the warrant; and
- (c) the thing has not been dealt with in a report under subsection 34(1);

the Director-General must:

- (d) give the Attorney-General a written report on the extent to which doing the thing has assisted the Organisation in carrying out its functions; and
- (e) do so as soon as practicable after the end of that period.

(2) If:

- (a) a warrant issued under this Division has ceased to be in force; and
- (b) as at the end of a prescribed post-cessation period of the warrant, it is likely that a thing will be done under subsection 25A(8), 27A(3C) or 27E(6) in connection with the warrant;

the Director-General must:

- (c) give the Attorney-General a written report on the extent to which doing the thing will assist the Organisation in carrying out its functions; and
- (d) do so as soon as practicable after the end of that period.

Prescribed post-cessation period

(3) For the purposes of this section, each of the following periods is a ***prescribed post-cessation period*** of a warrant:

- (a) the 3-month period beginning immediately after the warrant ceased to be in force;
- (b) each subsequent 3-month period.

34AAB Director-General to report to Attorney-General—internal authorisations to use tracking devices

- (1) If an internal authorisation is given, the Director-General must:
 - (a) give the Attorney-General a written report that meets the requirements of subsection (2); and
 - (b) do so within 3 months of the day on which the internal authorisation ceases to be in force.
- (2) The report must state whether the authorisation was executed, and, if so:
 - (a) give details of the extent to which any thing done in accordance with the authorisation has assisted the Organisation in carrying out its functions; and
 - (b) give details of the matter (the *security matter*) that is important in relation to security in respect of which the authorisation is given; and
 - (c) state the name, if known, of any person whose location was determined by the use of a tracking device in accordance with the authorisation; and
 - (d) state the period during which a tracking device was used in accordance with the authorisation; and
 - (e) give details of:
 - (i) any object in or on which a tracking device was installed in accordance with the authorisation; and
 - (ii) the premises where the object was located when the device was installed; and
 - (f) give details of the compliance with the restrictions or conditions (if any) to which the authorisation was subject; and
 - (g) state whether the authorisation was varied, and, if so:
 - (i) the number of variations; and
 - (ii) the reasons for each variation.

34AAC Evidentiary certificates

- (1) Subject to subsection (2), the Director-General or a Deputy Director-General may issue a written certificate setting out such facts as he or she considers relevant with respect to acts or things done by, on behalf of, or in relation to, the Organisation:
 - (a) in connection with a relevant warrant; or
 - (b) in accordance with a relevant authorising provision.
- (2) A certificate may be issued with respect to acts or things done in connection with:
 - (aa) a warrant issued under section 25, but only if the warrant authorises the doing of acts or things referred to in paragraph 25(5)(a), (b), (c) or (d), and only with respect to those acts or things; or
 - (a) a warrant issued under section 27A or 29, but only if the warrant authorises the doing of acts or things referred to in subsection 25(5) or section 25A or 26B, and only with respect to those acts or things; or
 - (b) a warrant issued under section 27C, but only if acts or things are authorised under paragraphs 27D(2)(h) to (k) or section 27E or 27F under the warrant, and only with respect to those acts or things.
- (3) Without limiting subsection (1), the certificate may set out one or more of the following:
 - (a) if premises were entered under the relevant warrant or relevant authorising provision:
 - (i) details of the premises; or
 - (ii) the time of day or night the premises were entered;
 - (b) if data was accessed under the relevant warrant or relevant authorising provision—details of the computer, telecommunications facility, electronic equipment, data storage device or communication in transit used for the purpose of obtaining such access;
 - (c) if the warrant is a surveillance device warrant—the matters required to be specified under section 26A for the warrant;

Section 34AAC

- (ca) if the authorising provision is section 26G—the matters required to be specified under subsection 26H(2);
 - (cb) if the warrant is issued under section 26R—the matters required to be specified under subsection 26R(4) for the warrant;
 - (d) if one or more surveillance devices were installed, used or maintained under the relevant warrant or relevant authorising provision:
 - (i) details of the installation, use or maintenance of the surveillance device or devices; or
 - (ii) details of the installation, use or maintenance of any enhancement equipment in relation to the surveillance device; or
 - (iii) details of the processes and procedures employed to use the surveillance device or devices, or any enhancement equipment; or
 - (iv) details of acts or things done for the purposes of recovering the surveillance device or devices, or any enhancement equipment;
 - (e) details of things done under the relevant warrant or relevant authorising provision that were reasonably necessary to conceal the fact that things were done under the relevant warrant or relevant authorising provision;
 - (f) details of persons who exercised the authority given by the relevant warrant or relevant authorising provision;
 - (g) details of things done under the relevant warrant or relevant authorising provision that were reasonably incidental to any of the acts or things done by, on behalf of, or in relation to, the Organisation in connection with the relevant warrant or relevant authorising provision.
- (4) In a proceeding, a certificate under subsection (1) is prima facie evidence of the matters stated in the certificate.
- (5) In this section:

proceeding means:

Section 34AAD

- (a) a proceeding or proposed proceeding in a federal court, or in a court of a State or Territory; or
- (b) a proceeding or proposed proceeding (including a hearing or examination, or proposed hearing or examination) by or before:
 - (i) a tribunal in Australia; or
 - (ii) any other body, authority or person in Australia having power to hear or examine evidence.

relevant authorising provision means subsection 25A(8), 26B(5) or (6), section 26C, 26D, 26E or 26G or subsection 27A(3A), (3B) or (3C), 27E(6) or 27F(5).

relevant warrant means a warrant issued under section 25, 25A, 26, 26R, 27A, 27C or 29.

Subdivision J—Assistance relating to access to data

34AAD Person with knowledge of a computer or a data storage device to assist access to data

- (1) The Director-General may request the Attorney-General to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the Organisation to do one or more of the following:
 - (a) access data held in, or accessible from, a computer or data storage device that:
 - (i) is the subject of a warrant under section 25A, 26 or 27A; or
 - (ii) is the subject of an authorisation under section 27E or 27F; or
 - (iii) is on premises in relation to which a warrant under section 25, 26 or 27A is in force; or
 - (iv) is on premises in relation to which an authorisation under section 27D or 27F is in force; or

Section 34AAD

- (v) is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by a warrant under section 25 or 27A; or
 - (vi) is found in the course of an ordinary search of a person, or a frisk search of a person, authorised under section 27D; or
 - (vii) has been removed from premises under a warrant under section 25, 26 or 27A; or
 - (viii) has been removed from premises under section 27D; or
 - (ix) has been seized under subsection 34CC(5);
 - (b) copy data held in, or accessible from, a computer, or data storage device, described in paragraph (a) to another data storage device;
 - (c) convert into documentary form or another form intelligible to an ASIO employee or ASIO affiliate:
 - (i) data held in, or accessible from, a computer, or data storage device, described in paragraph (a); or
 - (ii) data held in a data storage device to which the data was copied as described in paragraph (b); or
 - (iii) data held in a computer or data storage device removed from premises under a warrant under section 25, 26 or 27A; or
 - (iv) data held in a computer or data storage device removed from premises under section 27D.
- (2) The Attorney-General may make the order if:
- (a) in a case where the computer or data storage device:
 - (i) is the subject of a warrant under section 27A; or
 - (ii) is on premises in relation to which a warrant under section 27A is in force; or
 - (iii) is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by a warrant under section 27A; or
 - (iv) has been removed from premises under a warrant under section 27A;

Section 34AAD

the Attorney-General is satisfied, on reasonable grounds, that:

- (v) access by the Organisation to data held in, or accessible from, the computer or data storage device will be for the purpose of obtaining foreign intelligence relating to a matter specified in the relevant notice under subsection 27A(1); and
 - (vi) on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being; and
- (b) in a case where paragraph (a) does not apply—the Attorney-General is satisfied that there are reasonable grounds for suspecting that access by the Organisation to data held in, or accessible from, the computer or data storage device will substantially assist the collection of intelligence in accordance with this Act in respect of a matter that is important in relation to security; and
- (c) the Attorney-General is satisfied, on reasonable grounds, that the specified person is:
- (i) reasonably suspected of being involved in activities that are prejudicial to security; or
 - (ii) the owner or lessee of the computer or device; or
 - (iii) an employee of the owner or lessee of the computer or device; or
 - (iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or
 - (v) a person who uses or has used the computer or device; or
 - (vi) a person who is or was a system administrator for the system including the computer or device; and
- (d) the Attorney-General is satisfied, on reasonable grounds, that the specified person has relevant knowledge of:

Section 34AAD

- (i) the computer or device or a computer network of which the computer or device forms or formed a part; or
 - (ii) measures applied to protect data held in, or accessible from, the computer or device.
- (3) If the computer or data storage device is not on premises in relation to which a warrant is in force, the order must:
- (a) specify the period within which the person must provide the information or assistance; and
 - (b) specify the place at which the person must provide the information or assistance; and
 - (c) specify the conditions (if any) determined by the Attorney-General as the conditions to which the requirement on the person to provide the information or assistance is subject.
- (3A) A request under subsection (1) may be made:
- (a) orally; or
 - (b) in writing.
- (3B) If a request under subsection (1) is made orally, the Director-General must:
- (a) make a written record of the request; and
 - (b) do so within 48 hours after the request was made.
- (3C) A request under subsection (1) (the *current request*) must be accompanied by a statement setting out the particulars and outcomes of all previous requests (if any) under that subsection for the making of an order relating to the person specified in the current request.
- (3D) If the Director-General is satisfied that the grounds on which an order under this section was made have ceased to exist, the Director-General must, as soon as practicable, inform the Attorney-General of that fact.
- (3E) If:
- (a) an order is in force under this section; and

Part III Functions and powers of Organisation

Division 2 Special powers

Section 34AAD

- (b) the Attorney-General is satisfied that the grounds on which the order was made have ceased to exist; the Attorney-General must revoke the order.
- (4) A person commits an offence if:
- (a) the person is subject to an order under this section; and
 - (b) the person is capable of complying with a requirement in the order; and
 - (c) the person omits to do an act; and
 - (d) the omission contravenes the requirement.

Penalty for contravention of this subsection: Imprisonment for 5 years or 300 penalty units, or both.

Division 3—Compulsory questioning powers

Subdivision A—General provisions

34A Definitions

In this Division:

adult questioning matter means a matter that relates to the protection of, and of the people of, the Commonwealth and the several States and Territories from any of the following:

- (a) espionage;
- (b) politically motivated violence;
- (c) acts of foreign interference;

whether directed from, or committed within, Australia or not.

adult questioning warrant means a warrant issued under section 34BA (including such a warrant as varied under section 34BG).

against: a confiscation proceeding is **against** a person if:

- (a) for a proceeding under the *Proceeds of Crime Act 2002*—the person is a suspect (within the meaning of that Act) for the proceeding; or
- (b) for a proceeding under a law of a State or Territory—the person is in a corresponding category for that law.

charged: a person is **charged** with an offence if a process for prosecuting the person for the offence commences.

communication device means:

- (a) a device that a person may use to communicate information to another person; or
- (b) a surveillance device (within the meaning of Division 2).

complaints agency means an Ombudsman, agency or body:

Section 34A

- (a) that is appointed or established by a law of a State or Territory; and
- (b) that is permitted or required to investigate complaints about the police force or police service of the State or Territory; other than an agency or body prescribed by the regulations for the purposes of this definition.

confiscation proceeding means a proceeding under:

- (a) the *Proceeds of Crime Act 1987* or the *Proceeds of Crime Act 2002*; or
- (b) a corresponding law within the meaning of either of those Acts;

but does not include a criminal prosecution for an offence under either of those Acts or a corresponding law.

criminal proceeding means:

- (a) a prosecution for an offence against a law of the Commonwealth or of a State or Territory; or
- (b) a confiscation proceeding.

dangerous item means:

- (a) a weapon; or
- (b) any other thing that is or could be used in a dangerous or threatening way.

derivative material means any evidence, information, record or other thing obtained directly or indirectly from questioning material.

disclose, for questioning material or derivative material, includes:

- (a) to make available; and
- (b) to disclose copies, contents or descriptions of that material.

extra permitted questioning period has the meaning given by subsection 34DK(3).

immediate appearance requirement: a questioning warrant includes an **immediate appearance requirement** if it requires the

subject of the warrant to appear before a prescribed authority for questioning under the warrant immediately after the subject is given notice of the requirement in accordance with section 34BH.

imminent:

- (a) a charge against a person is ***imminent*** if:
 - (i) the person is under arrest for an offence, but has not been charged with the offence; or
 - (ii) a person with authority to commence a process for prosecuting the person for an offence has decided to commence, but not yet commenced, the process; or
- (b) a confiscation proceeding against a person is ***imminent*** if a person with authority to commence the proceeding has decided to commence, but not yet commenced, the proceeding.

Note: Subparagraph (a)(ii) applies, for example, if a person with authority to lay the charge has decided to lay, but not yet laid, the charge.

lawyer means a person who:

- (a) is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or Territory; and
- (b) holds a practising certificate granted under a law of a State or Territory.

minor questioning matter means a matter that relates to the protection of, and of the people of, the Commonwealth and the several States and Territories from politically motivated violence, whether directed from, or committed within, Australia or not.

minor questioning warrant means a warrant issued under section 34BB (including such a warrant as varied under section 34BG).

minor's representative, for the subject of a minor questioning warrant, has the meaning given by section 34AA.

permitted questioning period has the meaning given by subsection 34DJ(3).

Section 34A

police officer means any of the following:

- (a) a member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*);
- (b) a special member of the Australian Federal Police (within the meaning of that Act);
- (c) a member of the police force or police service of a State or Territory.

post-charge:

- (a) a use or disclosure of questioning material or derivative material is a ***post-charge*** use or disclosure if the use or disclosure happens at a time when:
 - (i) the subject for the material has been charged with a related offence and that charge is still to be resolved; or
 - (ii) such a charge is imminent; or
- (b) material is ***post-charge*** questioning material if the material becomes questioning material at a time when:
 - (i) the subject for the material has been charged with a related offence and that charge is still to be resolved; or
 - (ii) such a charge is imminent; or
- (c) questioning under a questioning warrant is ***post-charge*** questioning if the questioning commences at a time when:
 - (i) the subject of the warrant has been charged with a related offence and that charge is still to be resolved; or
 - (ii) such a charge is imminent; or
- (d) a questioning warrant is a ***post-charge*** questioning warrant if the warrant is issued at a time when:
 - (i) the subject of the warrant has been charged with a related offence and that charge is still to be resolved; or
 - (ii) such a charge is imminent.

post-confiscation application:

- (a) a use or disclosure of questioning material or derivative material is a ***post-confiscation application*** use or disclosure if the use or disclosure happens at a time when:

- (i) a related confiscation proceeding has commenced against the subject for the material and that proceeding is still to be resolved; or
- (ii) such a proceeding is imminent; or
- (b) material is **post-confiscation application** questioning material if the material becomes questioning material at a time when:
 - (i) a related confiscation proceeding has commenced against the subject for the material and that proceeding is still to be resolved; or
 - (ii) such a proceeding is imminent; or
- (c) questioning under a questioning warrant is **post-confiscation application** questioning if the questioning commences at a time when:
 - (i) a related confiscation proceeding has commenced against the subject of the warrant and that proceeding is still to be resolved; or
 - (ii) such a proceeding is imminent; or
- (d) a questioning warrant is a **post-confiscation application** questioning warrant if the warrant is issued at a time when:
 - (i) a related confiscation proceeding has commenced against the subject of the warrant and that proceeding is still to be resolved; or
 - (ii) such a proceeding is imminent.

pre-charge:

- (a) a use or disclosure of questioning material or derivative material is a **pre-charge** use or disclosure if the use or disclosure happens at a time when:
 - (i) the subject for the material has not been charged with a related offence, and such a charge is not imminent; or
 - (ii) all such charges have been resolved; or
- (b) material is **pre-charge** questioning material if the material becomes questioning material at a time when:
 - (i) the subject for the material has not been charged with a related offence, and such a charge is not imminent; or

Section 34A

- (ii) all such charges have been resolved; or
- (c) questioning under a questioning warrant is **pre-charge** questioning if the questioning commences at a time when:
 - (i) the subject of the warrant has not been charged with a related offence, and such a charge is not imminent; or
 - (ii) all such charges have been resolved.

pre-confiscation application:

- (a) a use or disclosure of questioning material or derivative material is a **pre-confiscation application** use or disclosure if the use or disclosure happens at a time when:
 - (i) a related confiscation proceeding has not commenced against the subject for the material, and such a proceeding is not imminent; or
 - (ii) all such proceedings have been resolved; or
- (b) material is **pre-confiscation application** questioning material if the material becomes questioning material at a time when:
 - (i) a related confiscation proceeding has not commenced against the subject for the material, and such a proceeding is not imminent; or
 - (ii) all such proceedings have been resolved; or
- (c) questioning under a questioning warrant is **pre-confiscation application** questioning if the questioning commences at a time when:
 - (i) a related confiscation proceeding has not commenced against the subject of the warrant, and such a proceeding is not imminent; or
 - (ii) all such proceedings have been resolved.

prescribed authority means a person appointed under subsection 34AD(1).

proceeds of crime authority means:

- (a) a proceeds of crime authority within the meaning of the *Proceeds of Crime Act 2002*; or

- (b) an authority of a State or Territory responsible for conducting a confiscation proceeding under a corresponding law (within the meaning of the *Proceeds of Crime Act 2002*).

prosecuting authority means an individual, or authority, authorised by or under a law of the Commonwealth or of a State or Territory to prosecute an offence.

prosecutor, of the subject of a questioning warrant, means an individual:

- (a) who is a prosecuting authority or is employed or engaged by a prosecuting authority; and
- (b) who:
- (i) makes, or is involved in the making of, a decision whether to prosecute the subject for a related offence; or
 - (ii) is one of the individuals engaging in such a prosecution of the subject.

questioning material has the meaning given by subsection 34AB(1).

questioning warrant means:

- (a) an adult questioning warrant; or
- (b) a minor questioning warrant.

record has the same meaning as in Division 2.

related confiscation proceeding, for questioning material, derivative material or the subject of a questioning warrant, means a confiscation proceeding if the subject matter of the relevant questioning relates to the subject matter of the proceeding.

related offence, for questioning material, derivative material or the subject of a questioning warrant, means an offence if the subject matter of the relevant questioning relates to the subject matter of the offence.

resolved, in relation to a charge or a confiscation proceeding, has the meaning given by section 34AC.

Section 34AA

screening equipment means a metal detector or a device for detecting objects or particular substances.

subject:

- (a) in relation to a questioning warrant—means the person specified in the warrant; or
- (b) for questioning material or derivative material—has the meaning given by subsection 34AB(3).

superior court means:

- (a) the High Court; or
- (b) the Federal Court of Australia; or
- (c) the Federal Circuit and Family Court of Australia (Division 1); or
- (d) the Supreme Court of a State or Territory; or
- (da) a State Family Court (being a court to which section 41 of the *Family Law Act 1975* applies); or
- (e) the District Court (or equivalent) of a State or Territory.

undergo a screening procedure: a person **undergoes a screening procedure** at a place if:

- (a) the person walks, or is moved, through screening equipment at the place; or
- (b) handheld screening equipment is passed over or around the person or around things that are at the place and in the person's possession or control; or
- (c) things that are at the place and in the person's possession or control are passed through screening equipment or examined by X-ray.

use, for questioning material or derivative material, includes use of copies, contents or descriptions of that material.

34AA Meaning of *minor's representative*

- (1) A person is a ***minor's representative*** for the subject of a minor questioning warrant if the person is:

- (a) a parent of the subject; or
 - (b) a guardian of the subject; or
 - (c) another person who meets the requirements in subsection (2).
- (2) A person meets the requirements of this subsection if the person:
- (a) is able to represent the subject's interests; and
 - (b) is, as far as practicable in the circumstances, acceptable to the subject and, if applicable, to the prescribed authority; and
 - (c) is not one of the following:
 - (i) a police officer;
 - (ii) the Director-General;
 - (iii) an ASIO employee or an ASIO affiliate;
 - (iv) a person approved under section 24.

Note: A lawyer for the subject of a minor questioning warrant, including a lawyer appointed under paragraph 34FC(2)(a) or (3)(b), may also be a minor's representative for the subject if the lawyer meets the requirements of this subsection.

34AB Meaning of *questioning material* and *subject*

- (1) ***Questioning material*** is:
- (a) any information given by a person while before a prescribed authority for questioning under a questioning warrant; or
 - (b) a record or other thing produced by a person while before a prescribed authority for questioning under a questioning warrant; or
 - (c) any information that might enable a person, who has appeared before a prescribed authority for questioning under a questioning warrant, to be identified; or
 - (d) the fact that a person has appeared, or is required to appear, before a prescribed authority for questioning under a questioning warrant.
- (2) To avoid doubt, information, a record or a thing is not covered by paragraph (1)(a) or (b) to the extent that it is obtained otherwise than before a prescribed authority under a questioning warrant.

Section 34AC

Example: Before a record is produced before a prescribed authority, a copy of the record is obtained when executing a search warrant. The copy obtained under the search warrant is not questioning material.

- (3) The *subject* is:
- (a) for questioning material—the person referred to in paragraph (1)(a), (b), (c) or (d); or
 - (b) for derivative material—the person who is the subject for the questioning material from which the derivative material was obtained.

34AC Meaning of *resolved*

- (1) A charge for an offence is *resolved* in relation to a person at the later of the following times:
- (a) when:
 - (i) the charge is withdrawn; or
 - (ii) the charge is dismissed; or
 - (iii) the person is not committed on the charge following a committal hearing; or
 - (iv) the person is acquitted of the offence; or
 - (v) the person is sentenced for the offence; or
 - (vi) the person is dealt with by being the subject of a court order made as a consequence of a finding of guilt; or
 - (vii) the charge is otherwise finally dealt with;
 - (b) if an appeal relating to the charge is not lodged within the period for lodging such an appeal—when that period ends;
 - (c) if an appeal relating to the charge is lodged—when the appeal lapses or is finally determined.
- Despite paragraph (b), if an appeal relating to the charge is lodged after that period ends, the charge ceases to be *resolved* until that appeal lapses or is finally determined.
- (2) A confiscation proceeding is *resolved* in relation to a person at the later of the following times:
- (a) when the proceeding is discontinued;

- (b) if an appeal relating to the proceeding is not lodged within the period for lodging such an appeal—when that period ends;
- (c) if an appeal relating to the proceeding is lodged—when the appeal lapses or is finally determined.

Despite paragraph (b), if an appeal relating to the proceeding is lodged after that period ends, the proceeding ceases to be *resolved* until that appeal lapses or is finally determined.

34AD Prescribed authorities

Appointment of prescribed authority

- (1) The Attorney-General may, in writing, appoint as a prescribed authority:
 - (a) a person who:
 - (i) has served as a judge in one or more superior courts for a period of at least 5 years; and
 - (ii) no longer holds a commission as a judge of a superior court; or
 - (b) a person who holds an appointment to the Administrative Review Tribunal as President or Deputy President; or
 - (c) a person who:
 - (i) is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or Territory; and
 - (ii) has engaged in practice as a legal practitioner for at least 10 years; and
 - (iii) holds a practising certificate granted under a law of a State or Territory; and
 - (iv) is a Senior Counsel.
- Note: *Senior Counsel* is given an extended meaning by section 2B of the *Acts Interpretation Act 1901*.
- (2) A person is not eligible for appointment under subsection (1) if the person is:
 - (a) an ASIO employee or an ASIO affiliate; or

Section 34AD

- (b) the Director-General; or
 - (c) an AGS lawyer (within the meaning of the *Judiciary Act 1903*); or
 - (d) an IGIS official; or
 - (e) a person referred to in subsection 6(1) of the *Australian Federal Police Act 1979*; or
 - (f) a staff member of a law enforcement agency (other than the Australian Federal Police); or
 - (g) a staff member of an intelligence or security agency.
- (3) The Attorney-General must not appoint a person to whom paragraph (1)(c) applies unless the Attorney-General is satisfied that the person has the knowledge or experience necessary to properly perform the duties of a prescribed authority.
- (4) The Attorney-General must not appoint a person unless:
- (a) the person has, in writing, consented to being appointed; and
 - (b) the consent is in force.
- (5) Before appointing a person as a prescribed authority, the Attorney-General must have regard to:
- (a) whether the person engages in any paid or unpaid work that conflicts, or could conflict, with the proper performance of the person's duties as a prescribed authority; and
 - (b) whether the person has any interests, pecuniary or otherwise, that conflict, or could conflict, with the proper performance of the person's duties as a prescribed authority.

Duty to disclose interests

- (6) A person who:
- (a) is appointed as a prescribed authority; and
 - (b) has a material personal interest that relates to the proper performance of the person's duties as a prescribed authority;
- must disclose that interest, in writing, to the Attorney-General.
- (7) The disclosure must include details of:

- (a) the nature and extent of the interest; and
 - (b) how the interest relates to the proper performance of the person's duties as a prescribed authority.
- (8) The person must make the disclosure:
- (a) as soon as practicable after the person becomes aware of the interest; and
 - (b) if there is a change in the nature or extent of the interest after the person has disclosed the interest under this section—as soon as practicable after the person becomes aware of that change.

Termination of appointment

- (9) The Attorney-General may terminate the appointment of a prescribed authority:
- (a) for misbehaviour; or
 - (b) if the prescribed authority is unable to perform the duties of a prescribed authority because of physical or mental incapacity; or
 - (c) if the prescribed authority becomes bankrupt; or
 - (d) if the prescribed authority fails, without reasonable excuse, to comply with subsection (6), (7) or (8); or
 - (e) if the prescribed authority engages in paid or unpaid work, or has an interest, pecuniary or otherwise, that, in the Attorney-General's opinion, conflicts or could conflict with the proper performance of the prescribed authority's duties.

Definitions

- (10) In this section:

paid work means work for financial gain or reward (whether as an employee, a self-employed person or otherwise).

unpaid work means work that is not paid work.

Section 34AE

34AE Status of prescribed authorities

A prescribed authority has, in the performance of the prescribed authority's duties under this Division, the same protection and immunity as a Justice of the High Court.

34AF Written statement of procedures

- (1) The Director-General may prepare a written statement of procedures to be followed in the exercise of authority under a questioning warrant.

Consultation

- (2) The Director-General must consult the following about the preparation of the statement:
 - (a) the Inspector-General of Intelligence and Security;
 - (b) the Commissioner of the Australian Federal Police.

Approval by Attorney-General

- (3) The Director-General must give the statement to the Attorney-General for approval.
- (4) The Attorney-General must approve or refuse to approve the statement.

Approved statement is a legislative instrument

- (5) A statement approved by the Attorney-General is a legislative instrument made by the Attorney-General on the day on which the statement is approved, but section 42 (disallowance) of the *Legislation Act 2003* does not apply to the statement.

Note: Part 4 of Chapter 3 (sunsetting) of the *Legislation Act 2003* does not apply to the statement: see regulations made for the purposes of paragraph 54(2)(b) of that Act.

Briefing of Parliamentary Joint Committee on Intelligence and Security

- (6) The Director-General must brief the Parliamentary Joint Committee on Intelligence and Security on the statement after it is approved by the Attorney-General. The briefing may be done orally or in writing.

34AG Humane treatment of subject of questioning warrant

- (1) This section applies to the subject of a questioning warrant while anything is being done in relation to the subject under:
 - (a) the warrant; or
 - (b) a direction given by a prescribed authority in relation to the warrant.
- (2) The subject must be treated with humanity and with respect for human dignity, and must not be subjected to torture or to cruel, inhuman or degrading treatment, by any person exercising authority under the warrant or implementing or enforcing the direction.

Subdivision B—Questioning warrants

34B Request for questioning warrant

Request for warrant

- (1) The Director-General may request the Attorney-General to issue, in relation to a person:
 - (a) an adult questioning warrant; or
 - (b) a minor questioning warrant.
- (2) The request may be made:
 - (a) in writing; or
 - (b) if the Director-General reasonably believes that the delay caused by making a written request may be prejudicial to

Section 34B

security—orally in person, or by telephone or other means of communication.

- (3) To avoid doubt, this section operates in relation to a request for the issue of a questioning warrant in relation to a person, even if a request (a *previous request*) for the issue of a questioning warrant has previously been made under this section in relation to the person.

Requirements for requests

- (4) A request under subsection (1) must include:
- (a) a statement of the facts and other grounds on which the Director-General considers it necessary that the warrant should be issued; and
 - (b) a statement of the particulars and outcomes of any previous requests for the issue of a questioning warrant in relation to the person; and
 - (c) if one or more warrants were issued as a result of the previous requests—a statement of:
 - (i) the period for which the person was questioned under each of those warrants; and
 - (ii) whether the person was apprehended in connection with any of those warrants; and
 - (d) whether the request is for a warrant that includes an immediate appearance requirement; and
 - (e) if the request is for a warrant that includes an immediate appearance requirement—whether the request is also for a questioning warrant that authorises the apprehension of the person; and
 - (f) if the request is for a minor questioning warrant—all information known to the Director-General, at the time of the making of the request, about the matters mentioned in subsection 34BB(3).

Additional requirements for oral requests

- (5) If a request under subsection (1) is to be made orally, the Director-General must, before or as soon as practicable after the request is made, cause the Inspector-General of Intelligence and Security to be notified that the request will be or has been made.
- (6) If a request under subsection (1) is made orally, the Director-General must:
 - (a) make a written record of the request that includes:
 - (i) the day and time the request is made; and
 - (ii) the reasons why the Director-General believes that the delay caused by making a written request may be prejudicial to security; and
 - (iii) the matters mentioned in subsection (4); and
 - (b) as soon as practicable, and no later than 48 hours after the request is made, provide the written record to:
 - (i) the Attorney-General; and
 - (ii) the Inspector-General of Intelligence and Security.

34BA Test for issue of questioning warrant—persons who are at least 18

- (1) If the Director-General requests the Attorney-General to do so, the Attorney-General may issue a warrant in relation to a person under this section if the Attorney-General is satisfied that:
 - (a) the person is at least 18 years old; and
 - (b) there are reasonable grounds for believing that the warrant will substantially assist the collection of intelligence that is important in relation to an adult questioning matter; and
 - (c) having regard to other methods (if any) of collecting the intelligence that are likely to be as effective, it is reasonable in all the circumstances for the warrant to be issued; and
 - (d) if the warrant is a post-charge, or post-confiscation application, questioning warrant—it is necessary, for the purposes of collecting the intelligence, for the warrant to be issued even though:

Section 34BB

- (i) the person has been charged or the confiscation proceeding has commenced; or
 - (ii) that charge or proceeding is imminent; and
 - (e) there is in force under section 34AF a written statement of procedures to be followed in the exercise of authority under a questioning warrant.
- (2) Without limiting its effect apart from this subsection, this Act also has the effect it would have if:
- (a) paragraph (1)(d) had not been enacted; or
 - (b) paragraph (1)(d) were, by express provision, confined to dealing with a charge against the person or such a charge that is imminent; or
 - (c) paragraph (1)(d) were, by express provision, confined to dealing with a confiscation proceeding against the person that has commenced or is imminent.

34BB Test for issue of questioning warrant—persons who are at least 14

- (1) If the Director-General requests the Attorney-General to do so, the Attorney-General may issue a warrant in relation to a person under this section if the Attorney-General is satisfied that:
- (a) the person is at least 14 years old; and
 - (b) there are reasonable grounds for believing that the person has likely engaged in, is likely engaged in, or is likely to engage in activities prejudicial to the protection of, and of the people of, the Commonwealth and the several States and Territories from politically motivated violence, whether directed from, or committed within, Australia or not; and
 - (c) there are reasonable grounds for believing that the warrant will substantially assist the collection of intelligence that is important in relation to a minor questioning matter; and
 - (d) having regard to other methods (if any) of collecting the intelligence that are likely to be as effective, it is reasonable in all the circumstances for the warrant to be issued; and

Section 34BB

- (e) if the warrant is a post-charge, or post-confiscation application, questioning warrant—it is necessary, for the purposes of collecting the intelligence, for the warrant to be issued even though:
 - (i) the person has been charged or the confiscation proceeding has commenced; or
 - (ii) that charge or proceeding is imminent; and
 - (f) there is in force under section 34AF a written statement of procedures to be followed in the exercise of authority under a questioning warrant.
- (2) In deciding whether to issue the warrant, the Attorney-General must consider the best interests of the person as a primary consideration.
- (3) In considering the best interests of a person for the purposes of subsection (2), the Attorney-General must take into account the following matters:
- (a) the age, maturity, sex and background (including lifestyle, culture and traditions) of the person;
 - (b) the physical and mental health of the person;
 - (c) the benefit to the person of having a meaningful relationship with the person's family and friends;
 - (d) the right of the person to receive an education;
 - (e) the right of the person to practise the person's religion;
 - (f) any other matter the Attorney-General considers relevant.
- (4) The Attorney-General must take into account the matters in subsection (3) only to the extent that:
- (a) the matters are known to the Attorney-General; and
 - (b) the matters are relevant.
- Note: Information about the matters in subsection (3) is provided to the Attorney-General as part of the request for the warrant: see paragraph 34B(4)(f).
- (5) Without limiting its effect apart from this subsection, this Act also has the effect it would have if:

Section 34BC

- (a) paragraph (1)(e) had not been enacted; or
- (b) paragraph (1)(e) were, by express provision, confined to dealing with a charge against the person or such a charge that is imminent; or
- (c) paragraph (1)(e) were, by express provision, confined to dealing with a confiscation proceeding against the person that has commenced or is imminent.

34BC Warrant has no effect if person under 14

A questioning warrant has no effect if the subject of the warrant is under 14 years old.

34BD What a questioning warrant authorises

- (1) A questioning warrant must, subject to any restrictions or conditions specified in the warrant:
 - (a) require the subject of the warrant to appear before a prescribed authority for questioning under the warrant either:
 - (i) if the warrant includes an immediate appearance requirement—immediately after the subject is given notice of the requirement in accordance with section 34BH; or
 - (ii) at a day and time specified in the warrant; and
 - (b) subject to subsection (2), authorise the Organisation to question the subject of the warrant before a prescribed authority by requesting the subject to:
 - (i) if the warrant is an adult questioning warrant—give information, or produce a record or other thing, that is, or may be, relevant to intelligence that is important in relation to an adult questioning matter; or
 - (ii) if the warrant is a minor questioning warrant—give information, or produce a record or other thing, that is, or may be, relevant to intelligence that is important in relation to a minor questioning matter; and

- (c) authorise the Organisation to make copies or transcripts of a record produced by the subject while before a prescribed authority for questioning under the warrant.

Additional requirements for minors

- (2) For the purposes of paragraph (1)(b), if the warrant is a minor questioning warrant, the warrant authorises the Organisation to question the subject of the warrant before a prescribed authority:
 - (a) only in the presence of a minor's representative for the subject; and
 - (b) only for continuous periods of 2 hours or less, separated by breaks directed by the prescribed authority.

Note 1: Also, the subject of a minor questioning warrant may be questioned only in the presence of a lawyer for the subject: see subsection 34FA(1).

Note 2: The prescribed authority may set the breaks between periods of questioning by giving appropriate directions under paragraph 34DE(1)(e) for the subject's further appearance before the prescribed authority for questioning.

- (3) To avoid doubt, subsection (2) does not affect the operation of section 34DJ (permitted questioning time) or 34DK (extra permitted questioning time if interpreter present).

Matters in relation to which the Organisation may request information etc.

- (4) For the purposes of paragraph (1)(b), the matters in relation to which the Organisation may request the subject to give information, or produce records or things, may include:
 - (a) the subject matter of any charge, or imminent charge, against the subject; and
 - (b) the subject matter of any confiscation proceeding, or imminent confiscation proceeding, against the subject.

Section 34BE

Severability

- (5) Without limiting its effect apart from this subsection, this Act also has the effect it would have if:
- (a) subsection (4) had not been enacted; or
 - (b) subsection (4) were, by express provision, confined to dealing with a charge against the subject or such a charge that is imminent; or
 - (c) subsection (4) were, by express provision, confined to dealing with a confiscation proceeding against the subject that has commenced or is imminent.

34BE Other things that may be authorised in questioning warrant

Warrant may require immediate appearance

- (1) A questioning warrant may include an immediate appearance requirement if the Attorney-General is satisfied that it is reasonable and necessary in the circumstances.

Note: For the definition of *immediate appearance requirement*, see section 34A.

Warrant may authorise apprehension

- (2) If:
- (a) a questioning warrant is to include an immediate appearance requirement under subsection (1); and
 - (b) the Attorney-General is satisfied that there are reasonable grounds for believing that, if the subject of the warrant is not apprehended, the subject is likely to:
 - (i) alert a person involved in an activity prejudicial to security that the activity is being investigated; or
 - (ii) not appear before the prescribed authority; or
 - (iii) destroy, damage or alter, or cause another person to destroy, damage or alter, a record or other thing the subject has been or may be requested under the warrant to produce;

Section 34BE

the warrant may also authorise the apprehension of the subject by a police officer in order to immediately bring the subject before the prescribed authority for questioning under the warrant.

Note: A police officer may also apprehend the subject of a questioning warrant if the subject makes certain representations: see subsection 34C(2).

Warrant may authorise seizure of certain records or other things found during search

- (3) If the Attorney-General is satisfied that it is reasonable and necessary in the circumstances, a questioning warrant may provide that if:
- (a) a police officer conducts a search of the subject of the warrant under section 34CC; and
 - (b) a record or other thing is found during the search that the officer reasonably believes is relevant to the collection of intelligence that is important in relation to:
 - (i) if the warrant is an adult questioning warrant—an adult questioning matter; or
 - (ii) if the warrant is a minor questioning warrant—a minor questioning matter;

the officer is authorised to seize the record or other thing.

Note: A police officer may only conduct a search of the subject of a questioning warrant under section 34CC if the subject is apprehended in connection with the warrant.

Warrant may request production of records or things

- (4) A questioning warrant may request the subject of the warrant to produce, before a prescribed authority:
- (a) a specified record or other thing; or
 - (b) a specified class of record or other thing;
- if the Attorney-General is satisfied that the record or thing, or class of record or thing, is, or may be, relevant to intelligence that is important in relation to:

Section 34BE

- (c) if the warrant is an adult questioning warrant—an adult questioning matter; or
- (d) if the warrant is a minor questioning warrant—a minor questioning matter.

Warrant may require immediate further appearance etc.

- (5) If:
- (a) a questioning warrant is in force; and
 - (b) the subject of the warrant has appeared before a prescribed authority for questioning under the warrant; and
 - (c) the subject has not been questioned under the warrant for longer than the permitted questioning period or, if applicable, the extra permitted questioning period; and
 - (d) the Attorney-General is satisfied that it is reasonable and necessary in the circumstances;
- the warrant may, despite any direction given under subsection 34DE(1) to the contrary:
- (e) require the subject's further appearance before a prescribed authority for questioning under the warrant; and
 - (f) include an immediate appearance requirement under subsection (1) in relation to the further appearance.

Note: This subsection only applies if a questioning warrant that is in force is varied under section 34BG.

- (6) If:
- (a) a questioning warrant is to include the requirements mentioned in paragraphs (5)(e) and (f); and
 - (b) the Attorney-General is satisfied that there are reasonable grounds for believing that, if the subject of the warrant is not apprehended:
 - (i) the subject is likely to alert a person involved in an activity prejudicial to security that the activity is being investigated; or
 - (ii) the subject is likely to not comply with the requirements mentioned in paragraphs (5)(e) and (f); or

- (iii) the subject is likely to destroy, damage or alter, or cause another person to destroy, damage or alter, a record or other thing the subject has been or may be requested under the warrant to produce;

the warrant may also authorise the apprehension of the subject by a police officer in order to immediately bring the subject before the prescribed authority for further questioning under the warrant.

34BF Requirements for questioning warrant

- (1) A questioning warrant may be issued:
 - (a) by means of a written document signed by the Attorney-General; or
 - (b) if the Attorney-General is satisfied that there are reasonable grounds on which to believe that the delay caused by issuing a written warrant may be prejudicial to security—orally in person, or by telephone or other means of communication.

Requirements for written warrants

- (2) If a questioning warrant is issued by means of a written document, the warrant must specify:
 - (a) that the warrant authorises the things mentioned in subsection 34BD(1); and
 - (b) which of the things mentioned in section 34BE are authorised by the warrant (if any); and
 - (c) the period during which the warrant is to be in force.

Requirements for oral warrants

- (3) If a questioning warrant is issued orally, the Director-General must cause a written record of the warrant, that includes the matters mentioned in subsection (2), to be made as soon as practicable, and no later than 48 hours after the warrant is issued.

Section 34BG

Duration of warrant

- (4) A questioning warrant may remain in force for a period of no more than 28 days, although the Attorney-General may revoke the warrant before the period has expired.

Issue of further warrants not prevented

- (5) Subsection (4) does not prevent the issue of any further warrant.

Written warrants and records not legislative instruments

- (6) The following are not legislative instruments:
- (a) a document referred to in paragraph (1)(a);
 - (b) a written record referred to in subsection (3).

34BG Variation of questioning warrant

Request for variation

- (1) The Attorney-General may, on request by the Director-General, vary a questioning warrant.
- (2) The request may be made:
- (a) in writing; or
 - (b) if the Director-General reasonably believes that the delay caused by making a written request may be prejudicial to security—orally in person, or by telephone or other means of communication.
- (3) The request must include the facts and other grounds on which the Director-General considers it necessary that the warrant should be varied.

Requirements for oral requests

- (4) If a request under subsection (1) is to be made orally, the Director-General must, before or as soon as practicable after the

request is made, notify the Inspector-General of Intelligence and Security that the request will be or has been made.

- (5) If a request under subsection (1) is made orally, the Director-General must:
- (a) make a written record of the request that includes:
 - (i) the day and time the request is made; and
 - (ii) the reasons why the Director-General believes that the delay caused by making a written request may be prejudicial to security; and
 - (iii) the matter mentioned in subsection (3); and
 - (iv) whether the request is to vary the warrant to include an immediate appearance requirement; and
 - (v) whether the request is to vary the warrant to authorise the apprehension of the subject of the warrant; and
 - (vi) any other matter the Director-General considers relevant; and
 - (b) as soon as practicable, and no later than 48 hours after the request is made, provide the written record to:
 - (i) the Attorney-General; and
 - (ii) the Inspector-General of Intelligence and Security.

Issue of variation

- (6) The variation may be issued:
- (a) by means of a written document signed by the Attorney-General; or
 - (b) if the Attorney-General is satisfied that there are reasonable grounds on which to believe that the delay caused by issuing a written variation may be prejudicial to security—orally in person, or by telephone or other means of communication.
- (7) If the variation is issued orally, the Director-General must cause a written record of the variation to be made as soon as practicable, and no later than 48 hours after the variation is issued.

Section 34BH

Limits on variation

- (8) If the variation extends, or further extends, the period during which the warrant is in force, the total period during which the warrant is in force must not exceed 28 days.

Warrant may be varied more than once

- (9) A questioning warrant may be varied more than once under this section.

Written variations and records not legislative instruments

- (10) The following are not legislative instruments:
- (a) a document referred to in paragraph (6)(a);
 - (b) a written record referred to in subsection (7).

34BH Notification requirements in relation to questioning warrant

- (1) This section applies if the Attorney-General issues a questioning warrant.
- (2) The Director-General must cause the subject of the warrant to be given written notice of:
- (a) the warrant; and
 - (b) the place where the subject is required to appear before a prescribed authority for questioning under the warrant; and
 - (c) either:
 - (i) if the warrant includes an immediate appearance requirement—the fact that the subject must appear before the prescribed authority for questioning under the warrant immediately after the subject is given notice of the requirement under this section; or
 - (ii) otherwise—the day and time when the subject is required to appear before the prescribed authority for questioning under the warrant; and
 - (d) the fact that the subject is able to contact a lawyer in accordance with section 34F; and

- (e) if the warrant is a minor questioning warrant—the fact that:
 - (i) the subject may request that a minor’s representative for the subject be present during the questioning; and
 - (ii) the subject may be questioned only in the presence of a minor’s representative for the subject; and
 - (f) the subject’s obligations under sections 34GD and 34GF; and
 - (g) the subject’s right to make a complaint orally or in writing to:
 - (i) in relation to the Organisation—the Inspector-General of Intelligence and Security under the *Inspector-General of Intelligence and Security Act 1986*; or
 - (ii) in relation to the Australian Federal Police—the Ombudsman under the *Ombudsman Act 1976*; or
 - (iii) in relation to the police force or police service of a State or Territory—a complaints agency of the State or Territory concerned; and
 - (h) the fact that the subject may seek from a federal court a remedy relating to the warrant or the treatment of the subject in connection with the warrant.
- (3) If the warrant is varied before the subject is given notice of the warrant in accordance with this section, the Director-General must cause the subject to be given written notice of:
- (a) the warrant as varied; and
 - (b) the matters mentioned in paragraphs (2)(b) to (h).
- (4) If:
- (a) the warrant is varied after the subject is given notice of the warrant in accordance with this section; and
 - (b) the variation may affect the subject’s obligations under the warrant or the information provided in the notice;
- the Director-General must, as soon as practicable, cause the subject to be given written notice of:
- (c) the variation; and
 - (d) the effect of the variation on the subject’s obligations under the warrant.

Section 34C

Note: For example, if the warrant is varied to include an immediate appearance requirement, the Director-General must cause the subject to be given written notice of the fact that the subject must appear before the prescribed authority immediately after the notice is given.

- (5) If the warrant is revoked after the subject is given notice of the warrant in accordance with this section, the Director-General must, as soon as practicable, cause the subject to be given written notice of:
- (a) the revocation; and
 - (b) the fact that the subject is no longer required to appear before a prescribed authority for questioning under the warrant; and
 - (c) the effect of section 34GF; and
 - (d) the subject's right to contact a lawyer in relation to the warrant at any time.

Subdivision C—Apprehension and search powers etc.

34C Police officer may apprehend subject of questioning warrant in certain circumstances

Apprehension where authorised by warrant

- (1) If a questioning warrant authorises the apprehension of the subject of the warrant, a police officer may apprehend the subject in order to immediately bring the subject before a prescribed authority for questioning under the warrant.

Note 1: The Attorney-General may only issue a questioning warrant that authorises the apprehension of the subject of the warrant if:

- (a) the warrant includes an immediate appearance requirement; and
- (b) the Attorney-General is satisfied of certain matters.

See subsection 34BE(2).

Note 2: A police officer's power to apprehend the subject of a questioning warrant under this subsection ends when the subject appears before a prescribed authority for questioning under the warrant.

Apprehension where certain representations made

- (2) If:
-

Section 34C

- (a) a questioning warrant includes an immediate appearance requirement; and
- (b) the warrant does not authorise the apprehension of the subject of the warrant; and
- (c) at the time the subject is given notice of the requirement in accordance with section 34BH, the subject makes a representation that the subject intends to:
 - (i) alert a person involved in an activity prejudicial to security that the activity is being investigated; or
 - (ii) not appear before the prescribed authority; or
 - (iii) destroy, damage or alter, or cause another person to destroy, damage or alter, a record or other thing the subject has been or may be requested in accordance with the warrant to produce;

a police officer may apprehend the subject in order to immediately bring the subject before a prescribed authority for questioning under the warrant.

Note: A police officer's power to apprehend the subject of a questioning warrant under this subsection ends when the subject appears before a prescribed authority for questioning under the warrant.

Apprehension where subject fails to appear

- (3) If the subject of a questioning warrant fails to appear before a prescribed authority as required by:
 - (a) the warrant; or
 - (b) a direction given by the prescribed authority under subsection 34DE(1);

a police officer may apprehend the subject in order to immediately bring the subject before the prescribed authority for questioning under the warrant.

Note: A police officer's power to apprehend the subject of a questioning warrant under this subsection ends when the subject appears before a prescribed authority for questioning under the warrant.

Section 34CA

Definitions

- (4) In this section, **representation** includes:
- (a) an express or implied representation (whether oral or in writing); and
 - (b) a representation that could be inferred from conduct; and
 - (c) a representation not intended by its maker to be communicated to or seen by another person; and
 - (d) a representation that for any reason is not communicated.

34CA Entering premises to apprehend subject

If:

- (a) a police officer is authorised under section 34C to apprehend the subject of a questioning warrant; and
- (b) the officer believes on reasonable grounds that the subject is on particular premises;

the officer may enter the premises, using such force as is necessary and reasonable in the circumstances, at any time of the day or night, for the purpose of searching the premises for the subject or apprehending the subject.

34CB Communications while apprehended

- (1) The subject of a questioning warrant who is apprehended under this Division is not permitted to contact, and may be prevented from contacting, any person at any time during the period:
- (a) beginning when the subject is apprehended; and
 - (b) ending when the subject appears before a prescribed authority for questioning under the warrant.
- (2) However:
- (a) the subject may contact any or all of the following:
 - (i) a lawyer;
 - (ii) if the warrant is a minor questioning warrant—a minor's representative for the subject;

Section 34CC

- (iii) any other person the subject is permitted to contact by the warrant, or by a direction given under paragraph 34DE(1)(b); and
- (b) subsection (1) does not affect the following:
 - (i) the operation of the *Inspector-General of Intelligence and Security Act 1986* in relation to contact between the subject and the Inspector-General of Intelligence and Security;
 - (ii) the operation of section 7 of the *Ombudsman Act 1976* in relation to contact between the subject and the Ombudsman in respect of a complaint, or proposed complaint, about the Australian Federal Police;
 - (iii) the subject's right to make a complaint to a complaints agency in relation to the police force or police service of the State or Territory concerned; and
- (c) any person apprehending the subject under this Division must, if requested by the subject, give the subject facilities for the following:
 - (i) contacting a person mentioned in paragraph (a);
 - (ii) contacting the Inspector-General of Intelligence and Security;
 - (iii) contacting the Ombudsman to make a complaint under section 7 of the *Ombudsman Act 1976*;
 - (iv) contacting the Commissioner of the Australian Federal Police to give information under section 40SA of the *Australian Federal Police Act 1979*;
 - (v) contacting a complaints agency to make a complaint of the kind mentioned in subparagraph (b)(iii).

Note: For the purposes of paragraph (a), section 34F provides for the subject of a questioning warrant to contact a lawyer for the purpose of obtaining legal advice in relation to the warrant and, if the warrant is a minor questioning warrant, to also contact a minor's representative.

34CC Power to conduct search of apprehended subject of questioning warrant

- (1) This section applies if:
-

Section 34CC

- (a) a questioning warrant is in force; and
- (b) the subject of the warrant is apprehended under this Division in connection with the warrant.

Power to conduct search

- (2) A police officer may conduct an ordinary search or a frisk search of the subject at any time during the period:
 - (a) beginning when the subject is apprehended; and
 - (b) ending when the subject appears before a prescribed authority for questioning under the warrant.
- (3) An ordinary search or a frisk search of the subject must, if practicable, be conducted by a police officer of the same sex as the subject.

Records or other things found during search

- (4) If:
 - (a) a record or other thing is found during a search of the subject of a questioning warrant under this section; and
 - (b) the record or other thing is:
 - (i) a seizable item; or
 - (ii) a communication device;the record or other thing may be seized under this subsection by the police officer conducting the search.
- (5) If:
 - (a) a record or other thing is found during a search of the subject of a questioning warrant under this section; and
 - (b) the police officer conducting the search reasonably believes that the record or other thing is relevant to the collection of intelligence that is important in relation to:
 - (i) if the warrant is an adult questioning warrant—an adult questioning matter; or
 - (ii) if the warrant is a minor questioning warrant—a minor questioning matter; and

- (c) the warrant authorises the seizure of such a record or other thing;
the record or other thing may be seized under this subsection by the officer.
- (6) Despite subsection (4), a seizable item or a communication device is taken to have been seized under subsection (5) if:
- (a) the item or device is found during a search of the subject of a questioning warrant under this section; and
 - (b) the item or device is seized by the police officer conducting the search; and
 - (c) the requirements of paragraphs (5)(b) and (c) are met in relation to the item or device.

34CD Use of force in apprehending or searching subject

A police officer may use such force as is necessary and reasonable in:

- (a) apprehending the subject of a questioning warrant in accordance with section 34C, or preventing the escape of the subject from such apprehension; or
- (b) conducting an ordinary search or a frisk search of the subject of a questioning warrant under subsection 34CC(2).

34CE Power to remove, retain and copy materials etc.

Powers of the Organisation

- (1) In addition to the things that the Organisation is authorised to do that are specified in a questioning warrant, the Organisation is also authorised:
- (a) to remove and retain any record or other thing produced by the subject of the warrant while before a prescribed authority for questioning under the warrant, or to retain any record or other thing seized under subsection 34CC(5), for the purposes of:
 - (i) inspecting or examining the record or thing; and

Section 34D

- (ii) in the case of a record—making copies or transcripts of the record; and
- (b) to do any other thing reasonably incidental to:
 - (i) the things mentioned in paragraph (a); or
 - (ii) any of the things that the Organisation is authorised to do that are specified in the warrant.
- (2) A record or other thing retained as mentioned in paragraph (1)(a) may be retained:
 - (a) if returning the record or other thing would be prejudicial to security—only until returning the record or other thing would no longer be prejudicial to security; and
 - (b) otherwise—for only such time as is reasonable.

Powers of police officers

- (3) A seizable item seized by a police officer under subsection 34CC(4) may be retained for such time as is reasonable.
- (4) A communication device seized by a police officer under subsection 34CC(4) may be retained:
 - (a) if returning the device would be prejudicial to security—only until returning the device would no longer be prejudicial to security; and
 - (b) otherwise—for only such time as the prescribed authority before whom the subject is appearing for questioning under the warrant considers reasonable.

Subdivision D—Matters relating to questioning under questioning warrants

34D Screening of persons

- (1) This section applies in relation to a person who is seeking to enter a place (the *questioning place*) where the subject of a questioning warrant is appearing, or is due to appear, before a prescribed authority for questioning under the warrant.

Section 34D

Note: This section applies in relation to any person who is seeking to enter a questioning place, including the subject.

Persons may be screened or searched

- (2) A police officer may request the person to do any of the following:
- (a) undergo a screening procedure at a place;
 - (b) produce a thing in the person's possession for inspection or examination, including anything worn or carried by the person that can be conveniently removed by the person;
 - (c) undergo an ordinary search or a frisk search, if the officer suspects on reasonable grounds that it is prudent to conduct an ordinary search or a frisk search of the person in order to ascertain whether the person is carrying a dangerous item or a communication device.
- (3) An ordinary search or a frisk search under paragraph (2)(c) must, if practicable, be conducted by a police officer of the same sex as the person.
- (4) A police officer may, for the purposes of subsection (2), request the person to remove a thing in the person's possession, including anything worn or carried by the person that can be conveniently removed by the person.

Certain items may be retained

- (5) A police officer may request the person to give a dangerous item or a communication device to the officer for safekeeping while the questioning is being conducted.
- (6) A dangerous item given to a police officer under subsection (5) may be retained by the officer for such time as is reasonable.
- (7) A communication device given to a police officer under subsection (5) by the subject may be retained by the officer:
- (a) if returning the device would be prejudicial to security—only until returning the device would no longer be prejudicial to security; and

Section 34D

- (b) otherwise—for only such time as the prescribed authority before whom the subject is appearing for questioning under the warrant considers reasonable.
- (8) A communication device given to a police officer under subsection (5) by a person other than the subject must be returned to the person if:
- (a) the person requests the officer to return the device; and
 - (b) at the time of the request, the person has left the questioning place.

Person may be requested to answer questions about certain things

- (9) If a thing is:
- (a) in the possession or control of a person while the person undergoes a screening procedure in accordance with paragraph (2)(a); or
 - (b) produced by a person for inspection or examination in accordance with paragraph (2)(b); or
 - (c) removed by a person in accordance with subsection (4); or
 - (d) given by a person to a police officer for safekeeping in accordance with subsection (5);

a police officer may request the person to answer reasonable questions about the thing.

Power to refuse entry

- (10) A police officer may refuse a person (other than an IGIS official) entry to a questioning place if:
- (a) a police officer makes a request of the person under this section; and
 - (b) the person does not comply with the request.

Note: If:

- (a) a person is the subject of a questioning warrant; and
- (b) the person is refused entry under this subsection to the questioning place;

the person will be taken to have failed to appear for questioning under the warrant: see subsection 34GD(2).

Exceptions

- (11) This section does not apply in relation to:
- (a) a communication device that is in the possession of, or being used lawfully by:
 - (i) an ASIO employee; or
 - (ii) an ASIO affiliate; or
 - (iii) an IGIS official; or
 - (iv) a police officer; or
 - (b) a dangerous item that is in the lawful possession of a police officer.

34DA Prohibition on possessing certain things during questioning

- (1) This section applies in relation to a person who is at a place where the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant.

Note: This section applies in relation to any person who is at the place, including the subject.

- (2) The person must not possess either of the following while the subject is appearing for questioning:
- (a) a communication device;
 - (b) a dangerous item.
- (3) However, this section does not apply in relation to:
- (a) a communication device that is in the possession of:
 - (i) an ASIO employee; or
 - (ii) an ASIO affiliate; or
 - (iii) an IGIS official; or
 - (iv) a police officer; or
 - (b) a dangerous item that is in the lawful possession of a police officer; or

Section 34DB

- (c) a communication device or a dangerous item that is in the possession of the subject, if:
 - (i) the device or item is seized under section 34CC, or retained under section 34CE or 34D; and
 - (ii) the device or item is returned to the subject for the purpose of complying with a request made by the Organisation in accordance with the warrant; and
 - (iii) the possession is solely for that purpose.

34DB Questioning under a questioning warrant

- (1) The questioning of a person under a questioning warrant may be:
 - (a) pre-charge questioning or post-charge questioning; or
 - (b) pre-confiscation application questioning or post-confiscation application questioning.
- (2) Without limiting its effect apart from this subsection, this Act also has the effect it would have if:
 - (a) paragraph (1)(a) were, by express provision, confined to pre-charge questioning; or
 - (b) paragraph (1)(b) were, by express provision, confined to pre-confiscation application questioning.

34DC Prescribed authority must explain certain matters

- (1) When the subject of a questioning warrant first appears before a prescribed authority for questioning under the warrant, the prescribed authority must inform the subject of the following:
 - (a) what the warrant authorises the Organisation to do;
 - (b) the period for which the warrant is in force;
 - (c) the circumstances in which the subject may be apprehended during the period in which the warrant is in force;
 - (d) the role of the prescribed authority, and in particular that the role includes:
 - (i) supervising the questioning of the subject; and
 - (ii) giving appropriate directions in relation to the subject;

Section 34DC

- (e) that the subject is able to contact a lawyer in accordance with section 34F;
- (f) the effect of section 34GD (including the fact that the section creates offences);
- (g) the effect of section 34GF (including the fact that the section creates offences and allows the prescribed authority to permit certain disclosures to be made);
- (h) the subject's right to apply to the Attorney-General for the provision of financial assistance under section 34JE;
- (i) the subject's right to make a complaint orally or in writing to:
 - (i) in relation to the Organisation—the Inspector-General of Intelligence and Security under the *Inspector-General of Intelligence and Security Act 1986*; or
 - (ii) in relation to the Australian Federal Police—the Ombudsman under the *Ombudsman Act 1976*; or
 - (iii) in relation to the police force or police service of a State or Territory—a complaints agency of the State or Territory concerned;
- (j) the subject's right to give information orally or in writing, under Division 2 of Part V of the *Australian Federal Police Act 1979*, to a person referred to in subsection 40SA(1) of that Act in relation to the Australian Federal Police;
- (k) the fact that the subject may seek from a federal court a remedy relating to the warrant or the treatment of the subject in connection with the warrant.

Note: Under sections 34DN and 34DO, if an interpreter is required, the prescribed authority must defer informing the subject under this section until the interpreter is present.

- (2) To avoid doubt, subsection (1) does not apply to a prescribed authority if the subject has previously appeared before another prescribed authority for questioning under the warrant.
- (3) The prescribed authority must also:
 - (a) inform the subject of the reason for the presence of each person who is present at any time during the questioning; and

Section 34DD

- (b) at least once in every 24 hour period during which questioning of the subject under the warrant occurs, inform the subject of the fact that the subject may seek from a federal court a remedy relating to the warrant or the treatment of the subject in connection with the warrant.

Note: For example, the subject may be able to apply to the Federal Court of Australia under subsection 39B(1) of the *Judiciary Act 1903*, or the High Court under paragraph 75(v) of the Constitution, for a remedy in relation to the warrant or the treatment of the subject in connection with the warrant.

- (4) Despite paragraph (3)(a):
 - (a) the prescribed authority must not name any person except with the consent of the person to be named; and
 - (b) the obligation to inform the subject about the reason for a particular person's presence need only be complied with once (even if that particular person subsequently returns to the questioning).

34DD Additional requirements for prescribed authorities in relation to minor questioning warrants

- (1) This section applies if the subject of a minor questioning warrant appears before a prescribed authority for questioning under the warrant.
- (2) In addition to the requirements of section 34DC, the prescribed authority must, as soon as practicable:
 - (a) inform the subject that a lawyer for the subject must be present during the questioning; and
 - (b) direct any person proposing to question the subject under the warrant that questioning is to occur only when the lawyer is present; and
 - (c) inform the subject that the subject may request that a minor's representative (a *non-lawyer representative*) for the subject who is not also a lawyer for the subject be present during the questioning; and

Section 34DE

- (d) if the subject requests that a non-lawyer representative be present during the questioning:
 - (i) if the warrant includes an immediate appearance requirement—give a direction under paragraphs 34FD(2)(c) and (d); or
 - (ii) if the warrant does not include an immediate appearance requirement—give a direction under paragraph 34FD(3)(c) or (d); and
- (e) if the subject voluntarily chooses not to request that a non-lawyer representative be present during the questioning—give a direction under paragraph 34FD(2)(c) or subsection 34FD(4), as the case requires; and
- (f) direct any person proposing to question the subject under the warrant that questioning is to occur only for continuous periods of 2 hours or less, separated by breaks directed by the prescribed authority.

Note 1: The prescribed authority may set breaks between periods of questioning by giving appropriate directions under paragraph 34DE(1)(e) for the subject's further appearance before the prescribed authority for questioning.

Note 2: Under sections 34DN and 34DO, if an interpreter is required, the prescribed authority must defer informing the subject under this section until the interpreter is present.

- (3) To avoid doubt, paragraph (2)(f) does not affect the operation of section 34DJ (permitted questioning time) or 34DK (extra permitted questioning time if interpreter present).

34DE Directions while subject is before prescribed authority for questioning

- (1) At any time when the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant, the prescribed authority may, either orally or in writing, give any of the following directions:
 - (a) a direction in accordance with subsection 34GF(6) permitting the subject to disclose specified information to a specified person;

Section 34DE

- (b) a direction permitting the subject to contact an identified person (including a person identified by reference to the fact that the person has a particular legal or familial relationship with the subject) or any person, and to disclose information other than specified information while in contact with that person;
- (c) a direction under paragraph 34FB(2)(a), 34FC(2)(a) or (3)(b) that a specified lawyer must be present during the questioning;
- (d) a direction to defer questioning of the subject under the warrant;
- (e) a direction for the subject's further appearance before the prescribed authority for questioning under the warrant, or for the subject to be excused or released from further attendance at questioning.

Note: A questioning warrant may be varied to require the subject's further appearance before a prescribed authority at an earlier day and time than that specified in a direction given under this subsection: see subsection 34BE(5).

- (2) However, the prescribed authority must not give a direction that is inconsistent with the warrant unless:
 - (a) the prescribed authority:
 - (i) has been informed under section 34DM of a concern of the Inspector-General of Intelligence and Security; and
 - (ii) is satisfied that giving the direction is necessary to address the concern satisfactorily; or
 - (b) the direction has been approved, in writing, by the Attorney-General.
- (3) If, at any time when the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant:
 - (a) a record or other thing is in the possession or control of a police officer because of the operation of section 34CC, 34CE or 34D; and

(b) a person exercising authority under the warrant requests that the record or thing be returned to the subject for the purpose of enabling the subject to comply with a request (the *warrant request*) made by the Organisation in accordance with the warrant;

the prescribed authority must give a direction that the record or thing be given to the subject for only such time as the prescribed authority considers reasonable to enable the subject to comply with the warrant request.

(4) If a prescribed authority gives a direction under subsection (1) or (3), the prescribed authority may vary or revoke the direction.

34DF Directions in relation to confidentiality

Prohibition or limitation on use or disclosure

(1) A prescribed authority must, in writing, give a direction that questioning material:

- (a) must not be used or disclosed; or
- (b) may only be used by, or disclosed to, specified persons in specified ways or on specified conditions;

if the prescribed authority is satisfied that the failure to give such a direction:

- (c) might prejudice a person's safety; or
- (d) would reasonably be expected to prejudice the fair trial of the subject for the material, if the subject has been charged with a related offence or such a charge is imminent.

(2) A prescribed authority may give a direction under subsection (1) in relation to questioning material at any time when the subject for the material has not been excused or released from further attendance at questioning.

(3) A direction given under subsection (1) by a prescribed authority in relation to questioning material may be varied or revoked, in writing, by:

- (a) the prescribed authority; or

Section 34DF

- (b) if the subject for the material has been excused or released from further attendance at questioning—the Director-General.
- (4) However, the direction cannot be varied or revoked if the prescribed authority or the Director-General (as the case requires) is satisfied that the variation or revocation:
 - (a) might prejudice a person’s safety; or
 - (b) would reasonably be expected to prejudice the fair trial of the subject for the material, if the subject has been charged with a related offence or such a charge is imminent.

Court certificate in relation to questioning material in respect of which a direction has been given

- (5) If:
 - (a) a person has been charged with an offence before a federal court or a court of a State or Territory; and
 - (b) the court considers that it may be desirable in the interests of justice that particular questioning material, in respect of which a prescribed authority has given a direction under subsection (1), be made available to the person or to a lawyer representing the person;the court may give to the Director-General a certificate to that effect. If the court does so, the Director-General must make the questioning material available to the court.
- (6) If:
 - (a) the Director-General makes questioning material available to a court under subsection (5); and
 - (b) the court, after examining the questioning material, is satisfied that the interests of justice so require;the court may make the questioning material available to the person charged with the offence concerned or to a lawyer representing the person.

34DG Direction that persons under 14 not be questioned

If:

- (a) the subject of a questioning warrant appears before a prescribed authority for questioning under the warrant; and
- (b) the prescribed authority is satisfied on reasonable grounds that the subject is under 14 years old;

the prescribed authority must, as soon as practicable, give a direction that the person is not to be questioned.

34DH Other matters relating to the functions and powers of prescribed authorities

- (1) A direction given by a prescribed authority has effect, and may be implemented or enforced, according to its terms.

Note: A prescribed authority must not give a direction that is inconsistent with a questioning warrant, except in limited circumstances: see subsection 34DE(2).

- (2) A prescribed authority is not subject to direction by the Director-General or the Attorney-General in relation to the performance of the prescribed authority's functions or the exercise of the prescribed authority's powers (including the making of a direction), other than in relation to the approval of a direction by the Attorney-General under paragraph 34DE(2)(b).

Note: A prescribed authority must not give a direction that is inconsistent with a questioning warrant, except in limited circumstances: see subsection 34DE(2).

- (3) To avoid doubt, a direction given by a prescribed authority cannot be varied or revoked by the Director-General or the Attorney-General, other than in accordance with subsection 34BE(5) or 34DF(3).

34DI Complaints while appearing before prescribed authority for questioning

If:

Section 34DJ

- (a) the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant; and
- (b) the subject informs the prescribed authority that the subject wants:
 - (i) to make a complaint of a kind referred to in paragraph 34DC(1)(i); or
 - (ii) to give information of the kind referred to in paragraph 34DC(1)(j); and
- (c) the subject requests facilities to make the complaint or give the information; and
- (d) the prescribed authority gives a direction under paragraph 34DE(1)(d) deferring questioning of the subject under the warrant;

a person exercising authority under the warrant must give the subject facilities for making the complaint or giving the information.

34DJ Permitted questioning time

- (1) This section applies if an interpreter is not present in accordance with section 34DN or 34DO while the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant.

Note: Section 34DK applies if an interpreter is present at any time during the questioning.

Time for questioning

- (2) The subject of a questioning warrant must not be questioned under the warrant by a person exercising authority under the warrant for longer than the permitted questioning period.
- (3) For the purposes of subsection (2), the ***permitted questioning period*** is:
 - (a) 8 hours; or

Section 34DJ

- (b) if a prescribed authority before whom the subject is being questioned has extended the period in accordance with subsection (4) or (5)—that longer period.

Note: The subject of a questioning warrant may be questioned for a longer period of time if an interpreter is required: see section 34DK.

Extension of time for questioning

- (4) If:
- (a) the subject has been questioned under the warrant for a total of less than 8 hours; and
 - (b) the prescribed authority before whom the subject is being questioned is satisfied of the matters in subsection (7);
- the prescribed authority may, just before the end of the 8 hours, extend the permitted questioning period to 16 hours.
- (5) If:
- (a) the subject has been questioned under the warrant for a total of more than 8 hours and less than 16 hours; and
 - (b) the prescribed authority before whom the subject is being questioned is satisfied of the matters in subsection (7);
- the prescribed authority may, just before the end of the 16 hours, extend the permitted questioning period to 24 hours.
- (6) A person exercising authority under a questioning warrant may request the prescribed authority to extend the permitted questioning period. The request may be made in the absence of:
- (a) the subject of the warrant; and
 - (b) a lawyer for the subject; and
 - (c) if the warrant is a minor questioning warrant—a minor's representative for the subject; and
 - (d) any person the subject is permitted to contact.
- (7) The prescribed authority may extend the permitted questioning period only if the prescribed authority is satisfied that:
- (a) the questioning of the subject was conducted properly and without delay; and

Section 34DK

- (b) there are reasonable grounds for believing that the extension will substantially assist the collection of intelligence that is important in relation to:
 - (i) if the warrant is an adult questioning warrant—an adult questioning matter; or
 - (ii) if the warrant is a minor questioning warrant—a minor questioning matter.
- (8) The prescribed authority may revoke the extension of the permitted questioning period. Revocation of the extension does not affect the legality of anything done in relation to the subject under the warrant before the revocation.

34DK Extra permitted questioning time if interpreter present

- (1) This section applies if, in accordance with section 34DN or 34DO, an interpreter is present at any time while the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant.
- (2) The subject must not be questioned under the warrant by a person exercising authority under the warrant for longer than the extra permitted questioning period.
- (3) For the purposes of subsection (2), the *extra permitted questioning period* is:
 - (a) 24 hours; or
 - (b) if a prescribed authority before whom the subject is being questioned has extended the period in accordance with subsection (4) or (5)—that longer period.

Extension of extra time for questioning

- (4) If:
 - (a) the subject has been questioned under the warrant for a total of less than 24 hours; and
 - (b) the prescribed authority before whom the subject is being questioned is satisfied of the matters in subsection (7);

the prescribed authority may, just before the end of the 24 hours, extend the extra permitted questioning period to 32 hours.

- (5) If:
- (a) the subject has been questioned under the warrant for a total of more than 24 hours and less than 32 hours; and
 - (b) the prescribed authority before whom the subject is being questioned is satisfied of the matters in subsection (7);
- the prescribed authority may, just before the end of the 32 hours, extend the extra permitted questioning period to 40 hours.
- (6) A person exercising authority under a questioning warrant may request the prescribed authority to extend the extra permitted questioning period. The request may be made in the absence of:
- (a) the subject of the warrant; and
 - (b) a lawyer for the subject; and
 - (c) if the warrant is a minor questioning warrant—a minor’s representative for the subject; and
 - (d) any person the subject is permitted to contact.
- (7) The prescribed authority may extend the extra permitted questioning period only if the prescribed authority is satisfied that:
- (a) the questioning of the subject was conducted properly and without delay; and
 - (b) there are reasonable grounds for believing that the extension will substantially assist the collection of intelligence that is important in relation to:
 - (i) if the warrant is an adult questioning warrant—an adult questioning matter; or
 - (ii) if the warrant is a minor questioning warrant—a minor questioning matter.
- (8) The prescribed authority may revoke the extension of the extra permitted questioning period. Revocation of the extension does not affect the legality of anything done in relation to the subject under the warrant before the revocation.

Section 34DL

34DL Time that is not questioning time

For the purposes of working out the time that the subject of a questioning warrant has been questioned under the warrant, disregard the following times:

- (a) the time taken by a prescribed authority to inform the subject of the matters referred to in section 34DC and, if applicable, section 34DD;
- (b) any time during which a prescribed authority has deferred questioning of the subject under the warrant to allow:
 - (i) the change of a thing in equipment being used to record the questioning of the subject; or
 - (ii) the subject to make a complaint of the kind referred to in paragraph 34DC(1)(i); or
 - (iii) the subject to give information of the kind referred to in paragraph 34DC(1)(j); or
 - (iv) the subject to contact a lawyer or another person as provided by this Division; or
 - (v) a lawyer to be present in accordance with a direction given under paragraph 34FB(2)(a) or 34FC(2)(a) or (3)(b); or
 - (vi) the subject to receive medical attention; or
 - (vii) the subject to engage in religious practices in accordance with the subject's religion; or
 - (viii) the subject to rest or recuperate;
- (c) any time during which a prescribed authority has suspended questioning of the subject under the warrant as mentioned in paragraph 34DM(4)(a);
- (d) any other time determined by a prescribed authority before whom the subject appears for questioning.

34DM Suspension of questioning etc. in response to concern of Inspector-General of Intelligence and Security

- (1) This section applies if the Inspector-General of Intelligence and Security is concerned about impropriety or illegality in connection

Section 34DN

with the exercise or purported exercise of powers under this Division in relation to the subject of a questioning warrant.

Note: For example, the Inspector-General may be concerned because the Inspector-General has been present at a questioning in accordance with section 34JB.

- (2) When the subject is appearing before a prescribed authority for questioning under the warrant, the Inspector-General:
 - (a) may inform the prescribed authority of the Inspector-General's concern; and
 - (b) must, as soon as practicable after informing the prescribed authority, inform the Director-General of the concern.
- (3) The prescribed authority must consider the Inspector-General's concern.
- (4) The prescribed authority may give a direction suspending:
 - (a) questioning of the subject under the warrant; or
 - (b) the exercise of another power under this Division that is specified in the direction;until the prescribed authority is satisfied that the Inspector-General's concern has been satisfactorily addressed.

34DN Interpreter provided at request of prescribed authority

- (1) This section applies if:
 - (a) the subject of a questioning warrant appears before a prescribed authority for questioning under the warrant; and
 - (b) the prescribed authority believes on reasonable grounds that the subject is unable, because of inadequate knowledge of the English language or a physical disability, to communicate with reasonable fluency in that language.
- (2) A person exercising authority under the warrant must arrange for the presence of an interpreter.
- (3) The prescribed authority must:

Section 34DO

- (a) defer informing the subject under section 34DC and, if applicable, section 34DD until the interpreter is present; and
- (b) give a direction under paragraph 34DE(1)(d) deferring questioning of the subject under the warrant until the interpreter is present.

34DO Interpreter provided at request of subject

- (1) This section applies if the subject of a questioning warrant appearing before a prescribed authority under the warrant requests the presence of an interpreter.
- (2) The prescribed authority must determine that an interpreter is to be present unless the prescribed authority believes on reasonable grounds that the subject:
 - (a) has an adequate knowledge of the English language to communicate with reasonable fluency in that language; or
 - (b) is physically able to communicate with reasonable fluency in that language.
- (3) A person exercising authority under the warrant must arrange for the presence of an interpreter if the prescribed authority makes a determination under subsection (2).
- (4) If questioning under the warrant has not commenced and the prescribed authority makes a determination under subsection (2):
 - (a) the prescribed authority must defer informing the subject under section 34DC and, if applicable, section 34DD until an interpreter is present; and
 - (b) a person exercising authority under the warrant must defer the questioning until an interpreter is present.
- (5) If questioning under the warrant commences before the subject requests the presence of an interpreter and the prescribed authority makes a determination under subsection (2):
 - (a) a person exercising authority under the warrant must defer any further questioning until an interpreter is present; and

- (b) when an interpreter is present, the prescribed authority must again inform the subject of anything of which the subject was previously informed under section 34DC or 34DD.

34DP Video recording of procedures

- (1) The Director-General must ensure that video recordings are made of the following:
 - (a) the appearance of the subject of a questioning warrant before a prescribed authority for questioning under the warrant;
 - (b) any other matter or thing in relation to the warrant that the prescribed authority directs is to be video recorded.
- (2) The Director-General must ensure that, if practicable, video recordings are made of any complaint made by the subject of a questioning warrant when the subject is not appearing before a prescribed authority for questioning under the warrant.

Subdivision E—Particular uses or disclosures of questioning material and derivative material

34E Obtaining derivative material

- (1) An entity mentioned in subsection (3), that may lawfully use or disclose questioning material, may lawfully use or disclose the material for the purpose of obtaining derivative material if the use or disclosure is:
 - (a) a pre-charge use or disclosure of the material; or
 - (b) a post-charge use or disclosure of pre-charge questioning material; or
 - (c) a post-charge use or disclosure of post-charge questioning material; or
 - (d) a pre-confiscation application use or disclosure of the material; or
 - (e) a post-confiscation application use or disclosure of pre-confiscation application questioning material; or

Section 34EA

(f) a post-confiscation application use or disclosure of post-confiscation application questioning material.

(2) Subsection (1) has effect subject to:

- (a) any direction given under subsection 34DF(1); and
- (b) paragraph 34EA(1)(b), in the case of a disclosure to a prosecutor of the subject for the material.

Subsection (1) does not, by implication, limit the use or disclosure of the questioning material for any other purpose.

(3) The entities are as follows:

- (a) the Director-General;
- (b) an entrusted person;
- (c) a person or body investigating whether the subject for the material committed an offence against a law of the Commonwealth or of a State or Territory;
- (d) a prosecutor of the subject for the material;
- (e) a prosecuting authority;
- (f) a proceeds of crime authority;
- (g) any other person or body lawfully in possession of the questioning material.

(4) Without limiting its effect apart from this subsection, this Act also has the effect it would have if:

- (a) one or more of paragraphs (1)(b), (c), (e) and (f) had not been enacted; or
- (b) subsection (3) were, by express provision, confined to persons or bodies other than either or both of the following:
 - (i) prosecutors of the subject for the material;
 - (ii) proceeds of crime authorities.

34EA Disclosing questioning material to prosecutors of the subject

- (1) A person or body, that may lawfully disclose questioning material, may lawfully disclose the material to a prosecutor of the subject for the material if the disclosure is:
 - (a) a pre-charge disclosure of the material; or
-

- (b) a post-charge disclosure of:
- (i) pre-charge questioning material; or
 - (ii) post-charge questioning material;
- under an order made under subsection 34EC(1).
- (2) Subsection (1) has effect subject to any direction given under subsection 34DF(1), in the case of a pre-charge disclosure of the material.

Note: In the case of a post-charge disclosure, the court may have regard to any direction given under subsection 34DF(1) in deciding whether to make an order under subsection 34EC(1).

- (3) Without limiting its effect apart from this subsection, this Act also has the effect it would have if paragraph (1)(b), or either of its subparagraphs, had not been enacted.

34EB Disclosing derivative material to prosecutors of the subject

- (1) A person or body, that may lawfully disclose derivative material, may lawfully disclose the material to a prosecutor of the subject for the material if the disclosure is:
- (a) a pre-charge disclosure of the material; or
 - (b) a post-charge disclosure of derivative material obtained from pre-charge questioning material (whether from a pre-charge use of that questioning material or otherwise); or
 - (c) a post-charge disclosure of derivative material obtained from post-charge questioning material, and the disclosure is under an order made under subsection 34EC(1).
- (2) Without limiting its effect apart from this subsection, this Act also has the effect it would have if paragraph (1)(b) or (c), or both, had not been enacted.

34EC Court's powers to order disclosure and to ensure a fair trial

Court may order that material may be disclosed

- (1) A court may, on application or on its own initiative, order that questioning material or derivative material may be disclosed to prosecutors of the subject for the material if the court is satisfied that the disclosure is required:

- (a) in the interests of justice; and
- (b) despite any direction given under subsection 34DF(1).

The order may specify the prosecutors (by any means), and the uses to which the prosecutors may put the material.

- (2) Subsection (1) applies to:

- (a) if the subject has been charged with a related offence before a federal court or a court of a State or Territory—that court; or
- (b) otherwise—a federal court (other than the Federal Circuit and Family Court of Australia (Division 1)) or a court of a State or Territory.

Court's powers to ensure the subject's fair trial

- (3) This Subdivision does not, by implication, restrict a court's power to make any orders necessary to ensure that the fair trial of a subject for questioning material or derivative material is not prejudiced by the possession or use of the material by a prosecutor of the subject.

- (4) However, a person's trial for:

- (a) an offence against a law of the Commonwealth or of a Territory; or
- (b) an offence against a law of a State that has a federal aspect (within the meaning of the *Australian Crime Commission Act 2002*);

is not unfair merely because the person has been the subject of a questioning warrant. This applies whether the person became the subject:

Section 34ED

- (c) before being charged with the offence and before such a charge was imminent; or
 - (d) after being charged with the offence or after such a charge was imminent.
- (5) Without limiting its effect apart from this subsection, this Act also has the effect it would have if subsection (4), or paragraph (4)(d), had not been enacted.

34ED Certain material may always be disclosed to prosecutors of the subject

- (1) A person or body, that may lawfully disclose questioning material of a kind covered by paragraph 34AB(1)(c) or (d), may lawfully disclose the material to a prosecutor of the subject for the material.
- (2) A person or body, that may lawfully disclose questioning material or derivative material, may lawfully disclose the material to a prosecutor of the subject for the material if the subject is suspected of, or has been charged with:
 - (a) an offence against this Division in relation to the relevant questioning warrant; or
 - (b) an offence against section 137.1 or 137.2 of the *Criminal Code* (about false or misleading information or documents) in relation to the relevant questioning warrant.
- (3) Subsection (1) or (2) has effect subject to any direction given under subsection 34DF(1).
- (4) Subsection (1) or (2) applies whether the disclosure is:
 - (a) a pre-charge disclosure of the material; or
 - (b) a post-charge disclosure of:
 - (i) pre-charge questioning material; or
 - (ii) derivative material obtained from pre-charge questioning material (whether from a pre-charge use of the questioning material or otherwise); or
 - (c) a post-charge disclosure of:
 - (i) post-charge questioning material; or

Section 34EE

- (ii) derivative material obtained from post-charge questioning material;
and whether or not an order has been made under subsection 34EC(1).
- (5) Without limiting its effect apart from this subsection, this Act also has the effect it would have if paragraph (4)(b) or (c), or both, had not been enacted.

34EE Other matters about prosecutors and subjects

- (1) If:
 - (a) a person lawfully possesses questioning material or derivative material; and
 - (b) the person is a prosecutor of the subject for the material;
the person may use that material for purposes that include:
 - (c) making a decision whether to prosecute the subject; and
 - (d) prosecuting the subject.This use of the questioning material is subject to subsection 34GD(6) and any direction given under subsection 34DF(1).
- (2) If material is lawfully in the possession of a prosecutor of the subject for the material, the fact that the material is questioning material or derivative material does not prevent it from being admissible in evidence against the subject in a criminal proceeding.

Note: The material may be inadmissible for other reasons (for example, because of subsection 34GD(6)).
- (3) This Subdivision does not, by implication, restrict the use of questioning material or derivative material by, or the disclosure of that material to:
 - (a) a prosecuting authority; or
 - (b) an individual employed or engaged by a prosecuting authority;who is not a prosecutor of the subject for the material.

- (4) This section has effect subject to any other law of the Commonwealth, or a law of a State or a Territory.

34EF Proceeds of crime authorities and questioning under a questioning warrant

- (1) A person or body, that may lawfully disclose questioning material or derivative material, may lawfully disclose the material to a proceeds of crime authority if the disclosure is:
- (a) a pre-confiscation application disclosure of the material; or
 - (b) a post-confiscation application disclosure of:
 - (i) pre-confiscation application questioning material; or
 - (ii) derivative material obtained from pre-confiscation application questioning material (whether from a pre-confiscation application use of the questioning material or otherwise); or
 - (c) a post-confiscation application disclosure of:
 - (i) post-confiscation application questioning material; or
 - (ii) derivative material obtained from post-confiscation application questioning material.
- (2) Subsection (1) has effect subject to any direction given under subsection 34DF(1).
- (3) If material is lawfully in the possession of a proceeds of crime authority, the fact that the material is questioning material or derivative material does not prevent it from being admissible in evidence against the subject for the material in a confiscation proceeding.
- Note: The material may be inadmissible for other reasons (for example, because of subsection 34GD(6)).
- (4) Subsection (3) of this section and subsection 34GD(6) do not, by implication, restrict a court's power to make any orders necessary to prevent prejudice to the proper administration of justice.

Section 34F

- (5) Without limiting its effect apart from this subsection, this Act also has the effect it would have if paragraph (1)(b) or (c), or both, had not been enacted.

Subdivision F—Lawyers and minor’s representatives

34F Person specified in warrant may contact lawyer or minor’s representative

Right to contact lawyer or minor’s representative

- (1) At any time after the subject of a questioning warrant is given notice of the warrant in accordance with subsection 34BH(2) or (3), the subject may:
- (a) contact a lawyer for the purpose of obtaining legal advice in relation to the warrant; and
 - (b) if the warrant is a minor questioning warrant—contact a minor’s representative for the subject.

Limit on contacting lawyers

- (2) If:
- (a) the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant; and
 - (b) a lawyer for the subject is present during the questioning; the prescribed authority may direct that the subject be prevented from contacting another lawyer if:
 - (c) the lawyer for the subject is not a person (an ***appointed lawyer***) specified in a direction given under paragraph 34FB(2)(a) or 34FC(2)(a) or (3)(b); or
 - (d) the lawyer for the subject is an appointed lawyer and the prescribed authority is satisfied that the subject has had reasonable opportunity to contact another lawyer.
- (3) If:

Section 34FA

- (a) the subject of an adult questioning warrant is appearing before a prescribed authority for questioning under the warrant; and
- (b) a lawyer for the subject is not present during the questioning; the prescribed authority may direct that the subject be prevented from contacting a lawyer if the prescribed authority is satisfied that the subject has had reasonable opportunity to contact a lawyer.

Limit on choice of lawyer

- (4) A prescribed authority may direct that the subject of a questioning warrant be prevented from contacting a particular lawyer if the prescribed authority is satisfied, on the basis of circumstances relating to the lawyer, that, if the subject is permitted to contact the lawyer:
 - (a) a person involved in an activity prejudicial to security may be alerted that the activity is being investigated; or
 - (b) a record or other thing that the subject has been or may be requested, in accordance with the warrant, to produce may be destroyed, damaged or altered.
- (5) To avoid doubt, subsection (4) does not prevent the subject from choosing another lawyer to contact, but the subject may be prevented from contacting that other lawyer under another application of that subsection.

Effect of section

- (6) This section has effect despite paragraph 34CB(2)(a).

34FA Questioning in absence of lawyer for subject

- (1) The subject of a minor questioning warrant must not be questioned under the warrant in the absence of a lawyer for the subject.
- (2) The subject of an adult questioning warrant may be questioned under the warrant in the absence of a lawyer for the subject if:
 - (a) the subject voluntarily chooses to be questioned in the absence of a lawyer; or

Section 34FB

- (b) a prescribed authority gives a direction under paragraph 34FB(3)(b) or subparagraph 34FF(7)(c)(iii) in relation to the subject.
- (3) This section does not permit questioning of the subject of a questioning warrant by a person exercising authority under the warrant at a time when a person exercising authority under the warrant is required by another section of this Division not to question the subject.

Example: This section does not permit the subject of a questioning warrant to be questioned when a person exercising authority under the warrant is required by section 34DN or 34DO to defer questioning because an interpreter is not present.

34FB Directions in relation to lawyers for subjects of adult questioning warrants

- (1) This section applies in relation to the subject of an adult questioning warrant if:
 - (a) a lawyer for the subject is not present while the subject is appearing before a prescribed authority for questioning under the warrant; and
 - (b) the subject requests at any time that a lawyer for the subject be present during the questioning.

If warrant includes immediate appearance requirement

- (2) If the warrant includes an immediate appearance requirement, the prescribed authority must, either orally or in writing:
 - (a) give a direction that:
 - (i) a specified person (the **appointed lawyer**) be appointed as the lawyer for the subject; and
 - (ii) the appointed lawyer be present during the questioning; and
 - (iii) the subject be questioned in the presence of the appointed lawyer; and

- (b) give a direction that a person exercising authority under the warrant give the subject facilities for contacting a lawyer (a *lawyer of choice*) other than the appointed lawyer.

If warrant does not include immediate appearance requirement

- (3) If the warrant does not include an immediate appearance requirement, the prescribed authority must, either orally or in writing:
 - (a) both:
 - (i) give a direction under paragraph 34DE(1)(d) deferring questioning of the subject for such time as the prescribed authority considers reasonable to enable a lawyer for the subject to be present during the questioning; and
 - (ii) give a direction that a person exercising authority under the warrant give the subject facilities for contacting a lawyer of choice; or
 - (b) give a direction that the subject may be questioned in the absence of a lawyer for the subject, if:
 - (i) the prescribed authority is satisfied that such time as is reasonable to enable a lawyer for the subject to be present during the questioning has passed; and
 - (ii) a lawyer for the subject is not present during the questioning.

When lawyer of choice is present

- (4) If:
 - (a) a direction under paragraph (2)(a) is in force in relation to the appointed lawyer for the subject of an adult questioning warrant; and
 - (b) both the appointed lawyer and a lawyer of choice are present during the questioning;the prescribed authority must, either orally or in writing:

Section 34FC

- (c) give a direction under paragraph 34DE(1)(d) deferring questioning of the subject for such time as the prescribed authority considers reasonable to enable:
 - (i) the appointed lawyer to brief the lawyer of choice; and
 - (ii) the lawyer of choice to provide advice to the subject; and
- (d) revoke the direction under paragraph (2)(a).

If subject chooses to be questioned in absence of lawyer

- (5) If a direction under paragraph (2)(a) is in force in relation to the appointed lawyer for the subject of an adult questioning warrant, the direction is revoked if the subject voluntarily chooses to be questioned under the warrant in the absence of a lawyer.

34FC Directions in relation to lawyers for subjects of minor questioning warrants

- (1) This section applies in relation to the subject of a minor questioning warrant if a lawyer for the subject is not present while the subject is appearing before a prescribed authority for questioning under the warrant.

If warrant includes immediate appearance requirement

- (2) If the warrant includes an immediate appearance requirement, the prescribed authority must, either orally or in writing:
 - (a) give a direction that:
 - (i) a specified person (the **appointed lawyer**) be appointed as the lawyer for the subject; and
 - (ii) the appointed lawyer be present during the questioning; and
 - (iii) the subject be questioned in the presence of the appointed lawyer; and
 - (b) give a direction that a person exercising authority under the warrant give the subject facilities for contacting a lawyer (a **lawyer of choice**) other than the appointed lawyer.

If warrant does not include immediate appearance requirement

- (3) If the warrant does not include an immediate appearance requirement, the prescribed authority must, either orally or in writing:
- (a) both:
 - (i) give a direction under paragraph 34DE(1)(d) deferring questioning of the subject for such time as the prescribed authority considers reasonable to enable a lawyer for the subject to be present during the questioning; and
 - (ii) give a direction that a person exercising authority under the warrant give the subject facilities for contacting a lawyer; or
 - (b) if the prescribed authority is satisfied that such time as is reasonable to enable a lawyer for the subject to be present during the questioning has passed—give a direction that:
 - (i) a specified person (the **appointed lawyer**) be appointed as the lawyer for the subject; and
 - (ii) the appointed lawyer be present during the questioning; and
 - (iii) the subject be questioned in the presence of the appointed lawyer.

When lawyer of choice is present

- (4) If:
- (a) a direction under paragraph (2)(a) or (3)(b) is in force in relation to the appointed lawyer for the subject of a minor questioning warrant; and
 - (b) both the appointed lawyer and a lawyer of choice are present during the questioning;
- the prescribed authority must, either orally or in writing:
- (c) give a direction under paragraph 34DE(1)(d) deferring questioning of the subject for such time as the prescribed authority considers reasonable to enable:
 - (i) the appointed lawyer to brief the lawyer of choice; and

Section 34FD

- (ii) the lawyer of choice to provide advice to the subject;
and
- (d) revoke the direction under paragraph (2)(a) or (3)(b) (as the case requires).

34FD Directions in relation to minor's representatives

- (1) This section applies if:
 - (a) the subject of a minor questioning warrant is appearing before a prescribed authority for questioning under the warrant; and
 - (b) a minor's representative (a *non-lawyer representative*) for the subject, who is not also a lawyer for the subject, is not present.

If warrant includes immediate appearance requirement

- (2) If:
 - (a) the warrant includes an immediate appearance requirement; and
 - (b) a lawyer for the subject is present during the questioning; the prescribed authority must, either orally or in writing:
 - (c) give a direction that the subject may be questioned under the warrant in the absence of a non-lawyer representative; and
 - (d) if the subject requests that a non-lawyer representative be present during the questioning—give a direction that the subject must be permitted to contact a non-lawyer representative.

Note 1: The subject of a minor questioning warrant may only be questioned if a lawyer for the subject is present: see subsection 34FA(1).

Note 2: In the absence of a non-lawyer representative, the lawyer for the subject is also the minor's representative for the subject.

If warrant does not include immediate appearance requirement

- (3) If:

Section 34FD

- (a) the warrant does not include an immediate appearance requirement; and
 - (b) the subject requests that a non-lawyer representative be present during the questioning;
- the prescribed authority must, either orally or in writing:
- (c) give a direction under paragraph 34DE(1)(d) deferring questioning of the subject for such time as the prescribed authority considers reasonable to enable:
 - (i) the subject to contact a non-lawyer representative; and
 - (ii) a non-lawyer representative to be present during the questioning; or
 - (d) give a direction that the subject may be questioned under the warrant in the absence of a non-lawyer representative, if:
 - (i) the prescribed authority is satisfied that such time as is reasonable to enable a non-lawyer representative to be present during the questioning has passed; and
 - (ii) a lawyer for the subject is present during the questioning.

Note: In the absence of a non-lawyer representative, the lawyer for the subject is also the minor's representative for the subject.

- (4) If:
- (a) the warrant does not include an immediate appearance requirement; and
 - (b) the subject voluntarily chooses not to request that a non-lawyer representative be present during the questioning; and
 - (c) a lawyer for the subject is present during the questioning;
- the prescribed authority must, either orally or in writing, give a direction that the subject may be questioned under the warrant in the absence of a non-lawyer representative.

Note: In the absence of a non-lawyer representative, the lawyer for the subject is also the minor's representative for the subject.

Section 34FE

When non-lawyer representative is present

- (5) A direction under paragraph (2)(c) or (3)(d) or subsection (4) in relation to the subject of a minor questioning warrant ceases to have effect if:
- (a) the subject contacts a non-lawyer representative; and
 - (b) the non-lawyer representative is present during the questioning.

34FE Lawyer may request copy of warrant

- (1) This section applies in relation to a lawyer who is acting for the subject of a questioning warrant in connection with the warrant.
- (2) Subject to subsection (4), a person exercising authority under the warrant must, if requested to do so by the lawyer, give the lawyer:
- (a) if the warrant is issued in writing—a copy of the warrant; or
 - (b) if the warrant is issued orally—a copy of the written record of the warrant made in accordance with subsection 34BF(3).
- (3) Subject to subsection (4), if the warrant is varied, a person exercising authority under the warrant must, if requested to do so by the lawyer, give the lawyer:
- (a) if the variation is issued in writing—a copy of the variation; or
 - (b) if the variation is issued orally—a copy of the written record of the variation made in accordance with subsection 34BG(7).
- (4) For the purposes of subsections (2) and (3), the Director-General may make such deletions from a document mentioned in subsection (5) as the Director-General considers necessary in order to avoid prejudice to security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs or the privacy of individuals.
- (5) The documents covered by this subsection are as follows:
- (a) a questioning warrant;

- (b) a written record of a questioning warrant;
 - (c) a variation of a questioning warrant;
 - (d) a written record of a variation of a questioning warrant.
- (6) Subsections (2) and (3) do not:
- (a) require more than one person to give the lawyer a copy of the warrant, the written record of the warrant, the variation or the written record of the variation (as the case requires); or
 - (b) entitle the lawyer to be given a copy of, or see, a document other than the warrant, the written record of the warrant, the variation or the written record of the variation (as the case requires).

34FF Involvement of lawyers

- (1) This section applies if:
- (a) the subject of a questioning warrant is appearing before a prescribed authority for questioning under the warrant; and
 - (b) a lawyer for the subject is present during the questioning.

Breaks in questioning

- (2) The prescribed authority must provide a reasonable opportunity for the lawyer to advise the subject during breaks in the questioning.

Note: The prescribed authority may set breaks between periods of questioning by giving directions under paragraph 34DE(1)(e) for the subject's further appearance before the prescribed authority for questioning. Paragraphs 34DL(b) to (d) also contain examples of procedural breaks in questioning.

- (3) The lawyer must not intervene in the questioning of the subject or address the prescribed authority before whom the subject is being questioned, except:
- (a) to request clarification of an ambiguous question; or
 - (b) to request a break in the questioning of the subject in order to provide advice to the subject.

Section 34FF

- (4) During a break in the questioning of the subject, the lawyer may request the prescribed authority for an opportunity to address the prescribed authority on a matter.

Note: The prescribed authority may set breaks between periods of questioning by giving directions under paragraph 34DE(1)(e) for the subject's further appearance before the prescribed authority for questioning. Paragraphs 34DL(b) to (d) also contain examples of procedural breaks in questioning.

- (5) The prescribed authority must approve or refuse a request under subsection (3) or (4).

Removal of lawyer for disrupting questioning

- (6) If the prescribed authority considers the lawyer's conduct is unduly disrupting the questioning of the subject, the prescribed authority may direct a person exercising authority under the warrant to remove the lawyer from the place where the questioning is occurring.

- (7) If the prescribed authority directs the removal of the lawyer:

(a) the prescribed authority must also direct that the subject may contact another lawyer; and

(b) if the subject chooses to contact another lawyer, the prescribed authority must give a direction under paragraph 34DE(1)(d) deferring questioning of the subject for such time as the prescribed authority considers reasonable to enable a lawyer for the subject to be present; and

(c) if:

(i) the time mentioned in paragraph (b) has passed and a lawyer for the subject is not present; or

(ii) the subject chooses not to contact another lawyer;

the prescribed authority must:

(iii) if the warrant is an adult questioning warrant—give a direction that the subject may be questioned in the absence of a lawyer for the subject; and

- (iv) if the warrant is minor questioning warrant—give a direction under paragraph 34FC(2)(a) or (3)(b) (as the case requires).

If lawyer is also a minor's representative for the subject

- (8) If section 34FG also applies to the lawyer in another capacity in relation to the subject, this section does not apply to conduct of the lawyer in that other capacity.

34FG Conduct of minor's representatives

- (1) This section applies in relation to a minor's representative for the subject of a minor questioning warrant who either:
 - (a) is, or has been, contacted by the subject as permitted by the warrant or a direction given by a prescribed authority; or
 - (b) is, or has been, present when the subject was before a prescribed authority for questioning under the warrant.
- (2) If a prescribed authority considers that the minor's representative's conduct is unduly disrupting questioning of the subject, the prescribed authority may, subject to subsection (3), direct a person exercising authority under the warrant to remove the minor's representative from the place where the questioning is occurring.
- (3) If the prescribed authority directs the removal of the minor's representative:
 - (a) the prescribed authority must inform the subject that:
 - (i) the subject may request that another minor's representative (a **replacement representative**) for the subject be present during the questioning; and
 - (ii) the subject may contact a replacement representative to request that the replacement representative be present during the questioning; and
 - (b) the prescribed authority must direct that:
 - (i) the subject may contact a replacement representative to request that the replacement representative be present during the questioning; and

Section 34FG

- (ii) a person exercising authority under the warrant must give the subject facilities for contacting a replacement representative.

(4) If:

- (a) the prescribed authority informs the subject under subsection (3); and
- (b) a lawyer for the subject is present during the questioning; and
- (c) the subject requests that a replacement representative (other than the lawyer) be present during the questioning;

the prescribed authority must:

- (d) if the warrant includes an immediate appearance requirement—give a direction that the subject may be questioned under the warrant in the absence of the replacement representative; and
- (e) if the warrant does not include an immediate appearance requirement—do either or both of the following:
 - (i) give a direction under paragraph 34DE(1)(d) deferring questioning of the subject for such time as the prescribed authority considers reasonable to enable the replacement representative to be present during the questioning;
 - (ii) if the prescribed authority is satisfied that such time as is reasonable to enable the replacement representative to be present during the questioning has passed—give a direction that the subject may be questioned under the warrant in the absence of the replacement representative.

Note: If a prescribed authority gives a direction under this subsection that the subject of a minor questioning warrant be questioned in the absence of a replacement representative, the lawyer for the subject is also the minor's representative for the subject until the replacement representative is present.

(5) If:

- (a) the prescribed authority informs the subject under subsection (3); and

- (b) a lawyer for the subject is present during the questioning; and
- (c) the subject voluntarily chooses not to request that a replacement representative (other than the lawyer) be present during the questioning;

the prescribed authority must give a direction that the subject may be questioned under the warrant in the absence of the replacement representative.

Note: If a prescribed authority gives a direction under this subsection that the subject of a minor questioning warrant be questioned in the absence of a replacement representative, the lawyer for the subject is also the minor's representative for the subject.

34FH Lawyers' access to information for proceedings relating to warrant

The regulations may prohibit or regulate access to information, access to which is otherwise controlled or limited on security grounds, by lawyers acting for a person in connection with proceedings for a remedy relating to:

- (a) a questioning warrant in relation to the person; or
- (b) the treatment of the person in connection with such a warrant.

34FI Law relating to legal professional privilege not affected

To avoid doubt, this Division does not affect the law relating to legal professional privilege.

Subdivision G—Offences

34G Surrender of travel documents by person in relation to whom questioning warrant is sought

- (1) If:
 - (a) the Director-General has requested the Attorney-General to issue a questioning warrant in relation to a person; and
 - (b) the Director-General believes on reasonable grounds that:

Section 34G

- (i) the person may leave Australia; and
 - (ii) the person's leaving would be likely to impact on the person's ability to comply with the questioning warrant;the Director-General may cause the person to be notified of the request and of the effect of subsection (2).
 - (2) The person must, as soon as practicable after being notified in accordance with subsection (1), deliver to an enforcement officer:
 - (a) all Australian travel documents that:
 - (i) have been issued to the person; and
 - (ii) are in the person's possession or control; and
 - (b) all passports or other travel documents that:
 - (i) have been issued to the person by or on behalf of the government of a foreign country; and
 - (ii) are in the person's possession or control.
 - (3) A person commits an offence if:
 - (a) the person is notified in accordance with subsection (1); and
 - (b) the person fails to comply with subsection (2).
- Penalty: Imprisonment for 5 years.
- (4) The Director-General must cause any document delivered under subsection (2) to be returned to the person to whom it was issued as soon as practicable after:
 - (a) if the Attorney-General refuses to issue a questioning warrant in relation to the person—that refusal; or
 - (b) if a questioning warrant is issued in relation to the person—the end of the period specified in the warrant as the period during which the warrant is to be in force;but the Director-General may cause the document to be returned to that person earlier.
 - (5) Subsection (4) does not require:
 - (a) the return of a document during the period specified in another warrant, issued in relation to the person under this

Division, as the period during which the other warrant is to be in force; or

- (b) the return of a document that has been cancelled.
- (6) If a questioning warrant is issued in relation to the person, a person approved under section 24 in relation to the warrant may, after a document of the first-mentioned person is delivered under subsection (2) of this section and before it is returned under subsection (4) of this section:
- (a) inspect or examine the document; and
 - (b) make copies or transcripts of it.
- (7) In this section:

enforcement officer means any of the following:

- (a) a member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*);
- (b) an officer of the police force of a State or Territory;
- (c) an officer of Customs (within the meaning of the *Customs Act 1901*).

34GA Person in relation to whom questioning warrant is requested must not leave Australia without permission

- (1) A person commits an offence if:
- (a) the person has been notified of:
 - (i) the making of a request by the Director-General for a questioning warrant in relation to the person; and
 - (ii) the effect of this subsection in connection with that request; and
 - (b) the person leaves Australia; and
 - (c) the leaving occurs after the person has been notified as mentioned in paragraph (a), and before:
 - (i) if the Attorney-General refuses to issue a questioning warrant in relation to the person—that refusal; or
 - (ii) if a questioning warrant is issued in relation to the person—the end of the period specified in the warrant

Section 34GB

as the period during which the warrant is to be in force;
and

- (d) the person does not have written permission from the Director-General to leave Australia at the time the person leaves Australia.

Penalty: Imprisonment for 5 years.

- (2) The Director-General may give written permission for a person in relation to whom a questioning warrant is requested to leave Australia at a specified time. The permission may be given either unconditionally or subject to specified conditions.

Note: The Director-General may revoke or amend the permission: see subsection 33(3) of the *Acts Interpretation Act 1901*.

- (3) If a permission under subsection (2) is given subject to a condition and the condition is not met, the permission is not in force.

34GB Surrender of travel documents by subject of questioning warrant

- (1) If:
- (a) a questioning warrant is issued; and
 - (b) the Director-General believes on reasonable grounds that:
 - (i) the subject of the warrant may leave Australia; and
 - (ii) the subject's leaving would be likely to impact on the subject's ability to comply with the warrant;

the Director-General may cause the subject to be notified of the issue of the warrant and of the effect of subsection (2).

Note: A notice of the issue of a questioning warrant under this subsection may be given under section 34BH or otherwise.

- (2) As soon as practicable after the subject is notified in accordance with subsection (1), the subject must deliver to a person exercising authority under the warrant:
- (a) all Australian travel documents that:
 - (i) have been issued to the subject; and
 - (ii) are in the subject's possession or control; and

- (b) all passports or other travel documents that:
 - (i) have been issued to the subject by or on behalf of the government of a foreign country; and
 - (ii) are in the subject's possession or control.
 - (3) The subject of a questioning warrant commits an offence if:
 - (a) the subject is notified in accordance with subsection (1); and
 - (b) the subject fails to comply with subsection (2).
- Penalty: Imprisonment for 5 years.
- (4) The Director-General must cause any document delivered under subsection (2) to be returned to the subject as soon as practicable after the end of the period specified in the warrant as the period during which the warrant is to be in force, but may cause the document to be returned to the subject earlier.
 - (5) Subsection (4) does not require:
 - (a) the return of a document during the period specified in another warrant, issued in relation to the subject under this Division, as the period during which the other warrant is to be in force; or
 - (b) the return of a document that has been cancelled.
 - (6) After the subject of a questioning warrant delivers a document under subsection (2) and before the document is returned under subsection (4), a person approved under section 24 in relation to the warrant may:
 - (a) inspect or examine the document; and
 - (b) make copies or transcripts of it.

34GC Subject of questioning warrant must not leave Australia without permission

- (1) The subject of a questioning warrant commits an offence if:
 - (a) the subject is notified of:
 - (i) the issue of the warrant; and
 - (ii) the effect of this subsection; and

Section 34GD

- (b) the subject leaves Australia; and
- (c) the leaving occurs:
 - (i) after the subject is notified as mentioned in paragraph (a); and
 - (ii) before the end of the period specified in the warrant as the period during which the warrant is to be in force; and
- (d) the subject does not have written permission from the Director-General to leave Australia at the time the subject leaves Australia.

Note: A notice of the issue of a questioning warrant under subparagraph (a)(i) may be given under section 34BH or otherwise.

Penalty: Imprisonment for 5 years.

- (2) The Director-General may give written permission for the subject of a questioning warrant to leave Australia at a specified time. The permission may be given either unconditionally or subject to specified conditions.

Note: The Director-General may revoke or amend the permission: see subsection 33(3) of the *Acts Interpretation Act 1901*.

- (3) If a permission under subsection (2) is given subject to a condition and the condition is not met, the permission is not in force.

34GD Giving information and producing things etc.

Failure to appear

- (1) The subject of a questioning warrant commits an offence if the subject fails to appear before a prescribed authority for questioning in accordance with:
 - (a) the warrant; or
 - (b) a direction given under subsection 34DE(1).

Penalty: Imprisonment for 5 years.

- (2) For the purposes of subsection (1), the subject of a questioning warrant is taken to fail to appear before a prescribed authority for questioning if, under subsection 34D(10), the subject is refused entry to the place where the questioning is to occur.

Note: Subsection 34D(10) provides for a police officer to refuse entry to a person if the person does not comply with a request made by the officer under section 34D.

Failure to give information etc.

- (3) The subject of a questioning warrant commits an offence if:
- (a) the subject is appearing before a prescribed authority for questioning under the warrant; and
 - (b) the Organisation requests, in accordance with the warrant, the subject to:
 - (i) give any information; or
 - (ii) produce any record or other thing; and
 - (c) the subject fails to comply with the request.

Penalty: Imprisonment for 5 years.

- (4) Subsection (3) does not apply if the subject:
- (a) does not have the information; or
 - (b) does not have possession or control of the record or thing.

Note: A defendant bears an evidential burden in relation to a matter in this subsection: see subsection 13.3(3) of the *Criminal Code*.

Self-incrimination etc.

- (5) The subject of a questioning warrant is not excused from:
- (a) giving information; or
 - (b) producing a record or other thing;
- that the Organisation requests, in accordance with the warrant, the subject to give or produce, on the ground that the information, or production of the record or thing, might tend to incriminate the subject in relation to an offence.

- (6) However:

Section 34GD

- (a) anything said by the subject, while appearing before a prescribed authority for questioning under the warrant, to comply with the request; and
 - (b) the production of a record or other thing by the subject, while appearing before a prescribed authority for questioning under the warrant, to comply with the request;
- are not admissible in evidence against the subject in a criminal proceeding, other than:
- (c) a confiscation proceeding, if the thing was said, or the record or thing was produced, at a time when the proceeding had not commenced and was not imminent; or
 - (d) proceedings for an offence against this section; or
 - (e) proceedings for an offence against section 34GF; or
 - (f) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* that relates to this section.
- (7) If, at general law, the subject of a questioning warrant would otherwise be able to claim the privilege against self-exposure to a penalty (other than an offence) in relation to giving information or producing a record or other thing in connection with the warrant, the subject is not excused from giving the information or producing the record or thing on that ground.

False or misleading statements

- (8) The subject of a questioning warrant commits an offence if:
- (a) the subject is appearing before a prescribed authority for questioning under the warrant; and
 - (b) the Organisation requests, in accordance with the warrant, the subject to give information; and
 - (c) the subject makes a statement that is, to the subject's knowledge, false or misleading; and
 - (d) the statement is made in purported compliance with the request.

Penalty: Imprisonment for 5 years.

Section 34GE

- (9) Subsection (8) does not apply if the statement is not false or misleading in a material particular.

Note: A defendant bears an evidential burden in relation to the matter in this subsection: see subsection 13.3(3) of the *Criminal Code*.

Rendering records or things illegible etc.

- (10) The subject of a questioning warrant commits an offence if:
- (a) the subject is requested, in connection with a questioning warrant, to produce a record or other thing; and
 - (b) the subject engages in conduct; and
 - (c) as a result of the conduct, the record or thing is unable to be produced, or to be produced in wholly legible or usable form.

Penalty: Imprisonment for 5 years.

34GE Offences of contravening safeguards

- (1) A person commits an offence if:
- (a) the person has been approved under section 24 to exercise authority conferred by a questioning warrant; and
 - (b) the person exercises, or purports to exercise, the authority; and
 - (c) the exercise, or purported exercise, contravenes a condition or restriction in the warrant on the authority; and
 - (d) the person knows of the contravention.

Penalty: Imprisonment for 2 years.

- (2) A person commits an offence if:
- (a) the person is a police officer; and
 - (b) the person engages in conduct in the exercise of, or the purported exercise of, authority conferred by this Division; and
 - (c) the conduct contravenes section 34C; and
 - (d) the person knows of the contravention.

Part III Functions and powers of Organisation

Division 3 Compulsory questioning powers

Section 34GE

Note: If a police officer engaged in the conduct in the exercise of a power otherwise than under this Division, paragraph (b) would not apply and the officer would not commit an offence against this subsection.

Penalty: Imprisonment for 2 years.

- (3) A person commits an offence if:
- (a) a prescribed authority gives a direction under:
 - (i) subsection 34DD(2); or
 - (ii) paragraph 34DE(1)(b), (d) or (e); or
 - (iii) section 34DG; or
 - (iv) subsection 34DM(4); and
 - (b) the person is identified (whether by name, reference to a class that includes the person or some other means) in the direction as a person who is to implement the direction; and
 - (c) the person engages in conduct; and
 - (d) the conduct contravenes the direction; and
 - (e) the person knows of the contravention.

Penalty: Imprisonment for 2 years.

- (4) A person commits an offence if:
- (a) the person uses or discloses questioning material (whether or not the person is the first to do so); and
 - (b) the use or disclosure contravenes a direction given under subsection 34DF(1) about the questioning material; and
 - (c) the person knows of the contravention; and
 - (d) the use or disclosure is not under subsection 34DF(5) or (6) or paragraph 34EA(1)(b).

Penalty: Imprisonment for 2 years.

- (5) A person commits an offence if:
- (a) the person engages in conduct; and
 - (b) the conduct contravenes:
 - (i) subsection 34AG(2); or
 - (ii) paragraph 34CB(2)(c); or

- (iii) section 34DI; or
- (iv) paragraph 34DN(3)(b); or
- (v) paragraph 34DO(4)(b) or (5)(a); and
- (c) the person knows of the contravention.

Penalty: Imprisonment for 2 years.

- (6) A person commits an offence if:
- (a) the person has been approved under section 24 to exercise authority conferred by a questioning warrant; and
 - (b) the person exercises, or purports to exercise, the authority by questioning the subject of the warrant; and
 - (c) the questioning contravenes section 34DJ or 34DK; and
 - (d) the person knows of the contravention.

Penalty: Imprisonment for 2 years.

34GF Secrecy relating to warrants and questioning

Before warrant ceases to be in force

- (1) A person (the *discloser*) commits an offence if:
- (a) a questioning warrant is issued; and
 - (b) the discloser discloses information; and
 - (c) either or both of the following apply:
 - (i) the information indicates the fact that the warrant has been issued, or a fact relating to the content of the warrant or to the questioning or apprehension of a person in connection with the warrant;
 - (ii) the information is operational information; and
 - (d) if subparagraph (c)(ii) applies but subparagraph (c)(i) does not—the discloser has the information as a direct or indirect result of:
 - (i) the issue of the warrant; or
 - (ii) the doing of anything authorised by the warrant, by a direction given by a prescribed authority in connection

Section 34GF

with the warrant or by another provision of this Division in connection with the warrant; and

- (e) the disclosure occurs before the end of the period specified in the warrant as the period for which the warrant is to be in force; and
- (f) the disclosure is not a permitted disclosure.

Penalty: Imprisonment for 5 years.

In the 2 years after warrant ceases to be in force

- (2) A person (the *discloser*) commits an offence if:
 - (a) a questioning warrant is issued; and
 - (b) the discloser discloses information; and
 - (c) the information is operational information; and
 - (d) the discloser has the information as a direct or indirect result of:
 - (i) the issue of the warrant; or
 - (ii) the doing of anything authorised by the warrant, by a direction given by a prescribed authority in connection with the warrant or by another provision of this Division in connection with the warrant; and
 - (e) the disclosure occurs before the end of the 2 years starting at the end of the period specified in the warrant as the period during which the warrant is to be in force; and
 - (f) the disclosure is not a permitted disclosure.

Penalty: Imprisonment for 5 years.

Strict liability

- (3) Strict liability applies to paragraphs (1)(c) and (2)(c) if the discloser is:
 - (a) the subject of the warrant; or
 - (b) a lawyer who has at any time been:

Section 34GF

- (i) present, as the lawyer for the subject of the warrant, during the questioning of the subject under the warrant; or
- (ii) contacted for the purpose of the subject obtaining legal advice in connection with the warrant; or
- (iii) contacted for the purpose of the subject obtaining representation in legal proceedings seeking a remedy relating to the warrant or the treatment of the subject in connection with the warrant.

Otherwise, the fault element applying to paragraphs (1)(c) and (2)(c) is recklessness.

Note: For strict liability, see section 6.1 of the *Criminal Code*. For recklessness, see section 5.4 of the *Criminal Code*.

Immunity from liability

- (3A) Subsections (1) and (2) do not apply to a person who discloses information if, as a result of the operation of a law of the Commonwealth, the person is not subject to any civil or criminal liability for the conduct.

Note 1: The *Public Interest Disclosure Act 2013* provides that an individual is not subject to any civil or criminal liability for making a public interest disclosure.

Note 2: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3) of the *Criminal Code*).

Extended geographical jurisdiction—category D

- (4) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against subsection (1) or (2) of this section.

Definitions

- (5) In this section:

operational information means information indicating one or more of the following:

- (a) information that the Organisation has or had;

Section 34GF

- (b) a source of information (other than the subject of the warrant mentioned in subsection (1) or (2)) that the Organisation has or had;
- (c) an operational capability, method or plan of the Organisation.

permitted disclosure means any of the following:

- (a) a disclosure made by a person in the course of any of the following:
 - (i) exercising a power, or performing a function or duty, under this Act;
 - (ii) doing anything the person is authorised to do by a warrant issued under this Act;
 - (iii) doing anything the person is required or permitted to do by a direction given by a prescribed authority;
 - (iv) exercising a power (including a power to make a complaint or to give information), or performing a function or duty, under Part V of the *Australian Federal Police Act 1979*, the *Ombudsman Act 1976* or a law of a State or Territory appointing or establishing a complaints agency;
- (aa) a disclosure made to or by an IGIS official for the purposes of the IGIS official exercising a power, or performing a function or duty, as an IGIS official;
- (b) a disclosure that is:
 - (i) made in the course of the questioning of the subject of a questioning warrant under the warrant; and
 - (ii) made by a person who is present during the questioning when making the disclosure;
- (c) a disclosure to a lawyer for the purpose of:
 - (i) obtaining legal advice in connection with a questioning warrant; or
 - (ii) obtaining representation in legal proceedings seeking a remedy relating to such a warrant or the treatment of a person in connection with such a warrant;
- (d) a disclosure for the purpose of the initiation, conduct or conclusion (by judgment or settlement) of legal proceedings

- relating to a remedy relating to a questioning warrant or the treatment of a person in connection with such a warrant;
- (e) a disclosure that is permitted by a prescribed authority to be made;
 - (f) a disclosure to one or more of the following persons, by the subject of a minor questioning warrant, by a parent, guardian or sibling of the subject, or by a minor's representative for the subject, of information described in paragraph (1)(c) or (2)(c) of this section in relation to the warrant:
 - (i) the subject;
 - (ii) a minor's representative for the subject;
 - (iii) a parent, guardian or sibling of the subject;
 - (iv) a prescribed authority;
 - (v) a person exercising authority under the warrant;
 - (vi) an IGIS official;
 - (vii) the Commonwealth Ombudsman;
 - (viii) a complaints agency;
 - (g) a disclosure for the purpose of making an application for assistance under subsection 34JE(1);
 - (h) a disclosure that is permitted by the Director-General to be made;
 - (i) a disclosure that is permitted by the Attorney-General to be made;
 - (j) a disclosure that is prescribed by the regulations.
- (6) For the purposes of paragraph (e) of the definition of *permitted disclosure* in subsection (5), a prescribed authority may give a direction, not inconsistent with the regulations (if any), permitting:
- (a) the subject of a questioning warrant; or
 - (b) a lawyer for the subject of a questioning warrant; or
 - (c) a minor's representative mentioned in subsection 34FG(1);
- to disclose specified information to a specified person. The direction may be given either unconditionally or subject to specified conditions.

Part III Functions and powers of Organisation

Division 3 Compulsory questioning powers

Section 34GF

Note: The prescribed authority may revoke or amend the direction: see subsection 33(3) of the *Acts Interpretation Act 1901*.

- (7) A prescribed authority may give written permission under subsection (6):
- (a) on the prescribed authority's own initiative; or
 - (b) on application by, or on behalf of, the person to whom the permission relates.
- (8) For the purposes of paragraph (h) of the definition of ***permitted disclosure*** in subsection (5), the Director-General may give written permission for a disclosure. The permission may be given either unconditionally or subject to specified conditions.

Note: The Director-General may revoke or amend the permission: see subsection 33(3) of the *Acts Interpretation Act 1901*.

- (9) For the purposes of paragraph (i) of the definition of ***permitted disclosure*** in subsection (5), the Attorney-General may, after obtaining advice from the Director-General, give written permission for a disclosure. The permission may be given either unconditionally or subject to specified conditions.

Note: The Attorney-General may, after obtaining advice from the Director-General, revoke or amend the permission: see subsection 33(3) of the *Acts Interpretation Act 1901*.

- (10) In deciding whether to give permission to a person under subsection (6), (8) or (9), the prescribed authority, the Director-General or the Attorney-General (as the case requires) must take into account:
- (a) the person's family and employment interests, to the extent that the prescribed authority, the Director-General or the Attorney-General (as the case requires) is aware of those interests; and
 - (b) the public interest; and
 - (c) the risk to security if the permission were given; and
 - (d) any submissions made by the person, the person's lawyer or the Organisation.

This subsection does not limit the matters that may be taken into account.

- (11) If a permission under subsection (6), (8) or (9) is given subject to a condition and the condition is not met, the permission is not in force.
- (12) Regulations made for the purposes of paragraph (j) of the definition of *permitted disclosure* in subsection (5) may prescribe a disclosure by reference to one or more of the following:
- (a) the person making the disclosure;
 - (b) the person to whom the disclosure is made;
 - (c) the circumstances in which the disclosure is made;
 - (d) the purpose of the disclosure;
 - (e) the nature of information disclosed;
 - (f) an opinion of a specified person about the possible or likely effect of the disclosure.

This subsection does not limit the way in which such regulations may prescribe a disclosure.

Offences apply to original and previously disclosed information

- (13) To avoid doubt, subsections (1) and (2) apply whether or not the discloser has the information that the discloser discloses as a result of a disclosure by another person.

Relationship with other laws prohibiting disclosure

- (14) This section has effect in addition to, and does not limit, other laws of the Commonwealth that prohibit the disclosure of information.

Subdivision H—Complaints, reporting and records

34H Complaints and information about contravention of procedural statement

- (1) Contravention of the written statement of procedures in force under section 34AF may be the subject of:

Section 34HA

- (a) a complaint to the Inspector-General of Intelligence and Security under the *Inspector-General of Intelligence and Security Act 1986*; or
 - (b) a complaint to the Ombudsman under the *Ombudsman Act 1976*; or
 - (c) information given under Division 2 of Part V of the *Australian Federal Police Act 1979* to a person referred to in subsection 40SA(1) of that Act; or
 - (d) a complaint to a complaints agency in relation to the police force or police service of the State or Territory concerned.
- (2) This section does not limit:
- (a) the subjects of complaint under:
 - (i) the *Inspector-General of Intelligence and Security Act 1986*; or
 - (ii) the *Ombudsman Act 1976*; or
 - (b) the subject of information given under Division 2 of Part V of the *Australian Federal Police Act 1979*.

34HA Providing reports to the Attorney-General

- (1) The Director-General must, for each questioning warrant, give the Attorney-General a written report that includes:
- (a) details of the extent to which the action taken under the warrant has assisted the Organisation in carrying out its functions; and
 - (b) if the subject of the warrant was apprehended—details of the apprehension, including whether any force was used in apprehending the subject; and
 - (c) if a record or other thing found during a search of the subject was seized—details of the seizure; and
 - (d) if an order was made under subsection 34AAD(2) in relation to accessing data that was held in, or accessible from, a computer or data storage device that was seized under subsection 34CC(4) or (5)—details of the extent to which compliance with the order has assisted the Organisation in carrying out its functions.

- (2) The Director-General must give the report within 3 months of the day on which the warrant ceases to be in force.

34HB Providing information to the Inspector-General

The Director-General must, as soon as practicable, give each of the following to the Inspector-General of Intelligence and Security:

- (a) for each request for a questioning warrant—a copy of the request;
- (b) for each questioning warrant—a copy of the warrant, or of the written record of the warrant made in accordance with subsection 34BF(3), as the case requires;
- (c) for each request to vary a questioning warrant—a copy of the request;
- (d) for each variation to a questioning warrant—a copy of the variation, or of the written record of the variation made in accordance with subsection 34BG(7), as the case requires;
- (e) a statement containing details of any seizure or apprehension under this Division;
- (f) if the Director-General is informed of a concern of the Inspector-General under section 34DM—a statement describing any action the Director-General has taken as a result;
- (g) a copy of any video recording made under section 34DP.

Note 1: If a request for a questioning warrant is made orally, the Director-General is also required to provide the written record of the request as soon as practicable, and no later than 48 hours after the request is made, to the Inspector-General: see paragraph 34B(6)(b).

Note 2: If a request to vary a questioning warrant is made orally, the Director-General is also required to provide the written record of the request as soon as practicable, and no later than 48 hours after the request is made, to the Inspector-General: see paragraph 34BG(5)(b).

34HC Destruction of certain records obtained under warrant

The Director-General must cause a record or copy to be destroyed if:

Section 34J

- (a) the record or copy was made because of a questioning warrant; and
- (b) the record or copy is in the possession or custody, or under the control, of the Organisation; and
- (c) the Director-General is satisfied that the record or copy is not required for the purposes of the performance of functions or exercise of powers under this Act.

Subdivision I—Miscellaneous

34J Discontinuance of action before cessation of warrant

If, before a questioning warrant ceases to be in force, the Director-General is satisfied that the grounds on which the warrant was issued have ceased to exist, the Director-General must:

- (a) inform the Attorney-General and the Inspector-General of Intelligence and Security accordingly; and
- (b) take such steps as are necessary to ensure that action under the warrant is discontinued.

34JA Certain functions and powers not affected

- (1) This Division does not affect a function or power of the Inspector-General of Intelligence and Security under the *Inspector-General of Intelligence and Security Act 1986*.
- (2) This Division does not affect a function or power of the Ombudsman under the *Ombudsman Act 1976* in relation to the Australian Federal Police.
- (3) This Division does not affect a function or power of a person under Part V of the *Australian Federal Police Act 1979*.

34JB IGIS official may be present at questioning or apprehension

To avoid doubt, for the purposes of exercising a power or performing a function or duty as an IGIS official, an IGIS official

may be present at the questioning or apprehension of a person under this Division.

34JC Rules of Court about proceedings connected with warrants

Rules of Court of the High Court or the Federal Court of Australia may make special provision in relation to proceedings for a remedy relating to a questioning warrant or the treatment of a person in connection with such a warrant.

34JD Jurisdiction of State and Territory courts excluded

- (1) A court of a State or Territory does not have jurisdiction in proceedings for a remedy if:
 - (a) the remedy relates to a questioning warrant or the treatment of a person in connection with such a warrant; and
 - (b) the proceedings are commenced while the warrant is in force.
- (2) This section has effect despite any other law of the Commonwealth (whether passed or made before or after the commencement of this section).

34JE Financial assistance

Application for assistance

- (1) An application for financial assistance may be made to the Attorney-General in respect of the subject of a questioning warrant's appearance before a prescribed authority for questioning under the warrant.
- (2) An application under subsection (1) may be made by, or on behalf of, the subject.

Authorisation of assistance

- (3) The Attorney-General may authorise the Commonwealth to provide the subject with financial assistance, determined by the

Part III Functions and powers of Organisation

Division 3 Compulsory questioning powers

Section 34JF

Attorney-General, in respect of the subject's appearance before a prescribed authority for questioning under the warrant.

- (4) Financial assistance may be given subject to such conditions (if any) as the Attorney-General determines.

Guidelines

- (5) The Attorney-General may, in writing, determine guidelines that are to be applied in authorising the provision of assistance under this section.
- (6) Guidelines under subsection (5) are not legislative instruments.

Limit on assistance

- (7) This section does not apply in relation to:
- (a) any complaint the subject makes that is of the kind mentioned in paragraph 34DC(1)(i); or
 - (b) any information the subject gives that is of a kind mentioned in paragraph 34DC(1)(j); or
 - (c) any remedy the subject seeks that is of the kind mentioned in paragraph 34DC(1)(k).

34JF Cessation of effect of Division

This Division ceases to have effect on 7 September 2025.

Division 4—Special intelligence operations

35A Relationship to other laws and matters

- (1) Subject to subsection (2) and section 35R, this Division is not intended to limit a discretion that a court has:
 - (a) to admit or exclude evidence in any proceedings; or
 - (b) to stay criminal proceedings in the interests of justice.
- (2) In determining whether evidence should be admitted or excluded in any proceedings, the fact that the evidence was obtained as a result of a person engaging in criminal activity is to be disregarded if:
 - (a) the person was a participant in a special intelligence operation authorised under this Division acting in the course of the special intelligence operation; and
 - (b) the criminal activity was special intelligence conduct.

35B Applications for authorities to conduct special intelligence operations

- (1) The Director-General may apply to the Attorney-General for an authority to conduct a special intelligence operation on behalf of the Organisation.
- (2) An application may be made:
 - (a) in writing signed by the Director-General; or
 - (b) if the Director-General reasonably believes that the delay caused by making a written application may be prejudicial to security—orally in person, or by telephone or other means of communication.
- (3) To avoid doubt, nothing in this Division prevents an application for a special intelligence operation authority being made in respect of a special intelligence operation that has been the subject of a previous application.

Note: A special intelligence operation authority can be varied, but not so as to extend beyond 12 months—see section 35F.

Section 35C

- (4) As soon as practicable after making an application in accordance with paragraph (2)(b), the Director-General must:
- (a) make a written record of the application; and
 - (b) give a copy of it to the Attorney-General.

35C Granting of special intelligence operation authorities

- (1) If:
- (a) an application for an authority to conduct a special intelligence operation is made under section 35B; and
 - (b) the Attorney-General is satisfied that there are reasonable grounds on which to believe that the matters in subsection (2) exist;

the Attorney-General may authorise the special intelligence operation by granting the authority.

- (2) The matters are as follows:
- (a) the special intelligence operation will assist the Organisation in the performance of one or more special intelligence functions;
 - (b) the circumstances are such as to justify the conduct of a special intelligence operation;
 - (c) any unlawful conduct involved in conducting the special intelligence operation will be limited to the maximum extent consistent with conducting an effective special intelligence operation;
 - (d) the special intelligence operation will not be conducted in such a way that a person is likely to be induced to commit an offence against a law of the Commonwealth, a State or a Territory that the person would not otherwise have intended to commit;
 - (e) any conduct involved in the special intelligence operation will not:
 - (i) cause the death of, or serious injury to, any person; or
 - (ia) constitute torture; or

- (ii) involve the commission of a sexual offence against any person; or
 - (iii) result in significant loss of, or serious damage to, property.
- (3) A special intelligence operation authority may be granted unconditionally or subject to conditions.
- (4) A special intelligence operation authority may be granted:
 - (a) by means of a written document signed by the Attorney-General; or
 - (b) if the Attorney-General is satisfied there are reasonable grounds on which to believe that the delay caused by giving a written authority may be prejudicial to security—orally in person, or by telephone or other means of communication.
- (5) If a special intelligence operation authority is granted in accordance with paragraph (4)(b), a written record of the special intelligence operation authority that complies with section 35D must be issued within 7 days.
- (6) To avoid doubt, nothing in this Division prevents a special intelligence operation authority being granted in respect of a special intelligence operation that has been the subject of a previous special intelligence operation authority.

Note: A special intelligence operation authority can be varied, but not so as to extend beyond 12 months—see section 35F.
- (7) The following are not legislative instruments:
 - (a) a document referred to in paragraph (4)(a);
 - (b) a written record referred to in subsection (5).

35D Contents of special intelligence operation authorities

- (1) A special intelligence operation authority must:
 - (a) state how the special intelligence operation will assist the Organisation in the performance of one or more special intelligence functions; and

Section 35E

- (b) identify the persons authorised to engage in special intelligence conduct for the purposes of the special intelligence operation; and
 - (c) state a description of the nature of the special intelligence conduct that the persons referred to in paragraph (b) may engage in; and
 - (d) specify the period of effect of the special intelligence operation authority, being a period not exceeding 12 months; and
 - (e) specify any conditions to which the conduct of the special intelligence operation is subject; and
 - (f) state the date and time when the special intelligence operation authority is granted.
- (2) A person is sufficiently identified for the purposes of paragraph (1)(b) if the person is identified:
- (a) by an assumed name under which the person is operating; or
 - (b) by a code name or code number;
- as long as the person's identity can be matched to the assumed name, code name or code number.

35E Commencement and duration of special intelligence operation authorities

- (1) A special intelligence operation authority comes into force at the time the special intelligence operation authority is granted under section 35C.
- (2) A special intelligence operation authority has effect for the period specified in accordance with paragraph 35D(1)(d) unless:
 - (a) it is cancelled before the end of the period of effect; or
 - (b) the period of effect is extended under section 35F.

35F Variation of special intelligence operation authorities

- (1) The Attorney-General may vary a special intelligence operation authority on application by the Director-General.

Application for variation

- (2) An application under subsection (1) may be made:
- (a) in writing signed by the Director-General; or
 - (b) if the Director-General reasonably believes that the delay caused by making a written application may be prejudicial to security—orally in person, or by telephone or other means of communication.
- (3) As soon as practicable after making an application in accordance with paragraph (2)(b), the Director-General must:
- (a) make a written record of the application; and
 - (b) give a copy of it to the Attorney-General.

Limits on variation

- (4) The Attorney-General must not vary the special intelligence operation authority unless the Attorney-General:
- (a) is satisfied that there are reasonable grounds on which to believe that the special intelligence operation, conducted in accordance with the special intelligence operation authority as varied, will assist the Organisation in the performance of one or more special intelligence functions; and
 - (b) considers it is appropriate to do so.
- (5) If a variation extends, or further extends, the period of effect of a special intelligence operation authority, the total period of effect must not be longer than 12 months.

Manner of variation

- (6) The variation may be made:
- (a) by means of a written document signed by the Attorney-General; or
 - (b) if the Attorney-General is satisfied there are reasonable grounds on which to believe that the delay caused by giving a written variation may be prejudicial to security—orally in person, or by telephone or other means of communication.

Section 35G

- (7) If a special intelligence operation authority is varied in accordance with paragraph (6)(b), a written record of the variation must be issued within 7 days.

Authority may be varied more than once

- (8) A special intelligence operation authority may be varied more than once under this section.

35G Cancellation of special intelligence operation authorities

- (1) The Director-General or a Deputy Director-General may cancel a special intelligence operation authority at any time and for any reason.
- (2) A cancellation of a special intelligence operation authority must:
- (a) be in writing; and
 - (b) specify when the cancellation takes effect.

35H Effect of special intelligence operation authorities

- (1) A special intelligence operation authority authorises each person who is identified in the special intelligence operation authority to engage in the special intelligence conduct specified in the special intelligence operation authority in respect of that person.
- (2) The authorisation, in relation to a person identified in the special intelligence operation authority, is for the period of effect of the special intelligence operation authority, unless:
- (a) the special intelligence operation authority specifies a shorter period during which the person is so authorised; or
 - (b) the special intelligence operation authority is varied under section 35F to provide that the person is no longer so authorised; or
 - (c) the special intelligence operation authority is cancelled before the end of that period.

35J Defect in a special intelligence operation authority

An application for a special intelligence operation authority or variation of such an authority, and any special intelligence operation authority or variation of such an authority granted on the basis of such an application, is not invalidated by any defect, other than a defect that affects the application, special intelligence operation authority or variation in a material particular.

35K Immunity from liability for special intelligence conduct during special intelligence operations

- (1) A participant in a special intelligence operation is not subject to any civil or criminal liability for or in relation to conduct if:
- (a) the participant engages in the conduct in the course of, and for the purposes of, the special intelligence operation; and
 - (b) the participant engages in the conduct in accordance with the special intelligence operation authority to conduct the special intelligence operation; and
 - (c) the participant is identified in the special intelligence operation authority as a person authorised to engage in special intelligence conduct for the purposes of the special intelligence operation; and
 - (d) the conduct does not involve the participant intentionally inducing another person to commit an offence against a law of the Commonwealth, a State or a Territory that the other person would not otherwise have intended to commit; and
 - (e) the conduct does not involve the participant engaging in any conduct that:
 - (i) causes the death of, or serious injury to, any person; or
 - (ia) constitutes torture; or
 - (ii) involves the commission of a sexual offence against any person; or
 - (iii) causes significant loss of, or serious damage to, property; and
 - (f) the requirements (if any) specified in a determination under subsection (2) have been met.

Section 35L

- (2) The Attorney-General may, by legislative instrument, determine requirements for the purposes of paragraph (1)(f).

35L Requirements for warrants etc. not affected

- (1) If, apart from this Division, the Organisation could not do a particular act without it being authorised by warrant issued under this Act or under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*, this Division does not allow the Organisation to do the act without the warrant.
- (2) If, apart from this Division, the Organisation could not obtain particular information other than in accordance with Division 3 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*, this Division does not allow the Organisation to obtain the information otherwise than in accordance with that Division of the *Telecommunications (Interception and Access) Act 1979*.
- (3) This section is enacted to avoid doubt.

35M Effect of being unaware of variation or cancellation of special intelligence operation authority

- (1) If an authority to conduct a special intelligence operation is varied in a way that limits its scope, this Division continues to apply to a participant in the special intelligence operation as if the authority had not been varied in that way, for so long as the participant:
- (a) is unaware of the variation; and
 - (b) is not reckless about the existence of the variation.
- (2) If an authority to conduct a special intelligence operation is cancelled, this Division continues to apply to a person who was a participant in the special intelligence operation immediately before the cancellation as if the authority had not been cancelled in that way, for so long as the person:
- (a) is unaware of the cancellation; and
 - (b) is not reckless about the existence of the cancellation.

- (3) For the purposes of this section, a person is reckless about the existence of the variation or cancellation of a special intelligence operation authority if:
- (a) the person is aware of a substantial risk that the variation or cancellation has happened; and
 - (b) having regard to the circumstances known to the person, it is unjustifiable to take the risk that the special intelligence operation authority has not been varied or cancelled.

35N Protection from criminal responsibility for certain ancillary conduct

- (1) This section applies if:
- (a) a person engages in conduct (the *ancillary conduct*) that relates to special intelligence conduct (the *related conduct*) engaged in by another person; and
 - (b) engaging in the ancillary conduct is an ancillary offence in relation to the offence constituted by the related conduct.
- (2) Despite any other law of the Commonwealth, a State or a Territory, the person who engaged in the ancillary conduct is not criminally responsible for the ancillary offence, if, at the time the person engaged in the ancillary conduct, he or she believed the related conduct was being engaged in, or would be engaged in, by a participant in a special intelligence operation authorised under this Division.
- (3) For the purposes of this section, *ancillary offence*, in relation to an offence constituted by related conduct, means an offence against a law of the Commonwealth, a State or a Territory:
- (a) of conspiring to commit the offence constituted by the related conduct; or
 - (b) of aiding, abetting, counselling or procuring, inciting or being in any way knowingly concerned in, the commission of the offence constituted by the related conduct.

Section 35P

35P Unauthorised disclosure of information

Disclosures by entrusted persons

- (1) A person commits an offence if:
- (a) the person is, or has been, an entrusted person; and
 - (b) information came to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and
 - (c) the person discloses the information; and
 - (d) the information relates to a special intelligence operation.

Penalty: Imprisonment for 5 years.

Note: Recklessness is the fault element for paragraphs (1)(b) and (d)—see section 5.6 of the *Criminal Code*.

- (1A) Strict liability applies to paragraph (1)(a).

Note: For strict liability, see section 6.1 of the *Criminal Code*.

- (1B) A person commits an offence if:

- (a) the person is, or has been, an entrusted person; and
- (b) information came to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and
- (c) the person discloses the information; and
- (d) the information relates to a special intelligence operation; and
- (e) either or both of the following subparagraphs apply:
 - (i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation;
 - (ii) the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 10 years.

Note: Recklessness is the fault element for paragraphs (1B)(b) and (d) and subparagraph (1B)(e)(ii)—see section 5.6 of the *Criminal Code*.

(1C) Strict liability applies to paragraph (1B)(a).

Note: For strict liability, see section 6.1 of the *Criminal Code*.

Other disclosures

(2) A person commits an offence if:

- (a) the person discloses information; and
- (b) the information relates to a special intelligence operation; and
- (c) the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 5 years.

Note: Recklessness is the fault element for paragraphs (2)(b) and (c)—see section 5.6 of the *Criminal Code*.

(2A) A person commits an offence if:

- (a) the person discloses information; and
- (b) the information relates to a special intelligence operation; and
- (c) either or both of the following subparagraphs apply:
 - (i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation;
 - (ii) the person knows that the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 10 years.

Note: Recklessness is the fault element for paragraph (2A)(b)—see section 5.6 of the *Criminal Code*.

Exceptions

(3) Subsections (1) to (2A) do not apply if the disclosure was:

- (a) in connection with the administration or execution of this Division; or

Section 35P

- (b) for the purposes of any legal proceedings arising out of or otherwise related to this Division or of any report of any such proceedings; or
- (c) in accordance with any requirement imposed by law; or
- (d) in connection with the performance of functions or duties, or the exercise of powers, of the Organisation; or
- (e) for the purpose of obtaining legal advice in relation to the special intelligence operation; or
- (f) to an IGIS official for the purpose of exercising powers, or performing functions or duties, as an IGIS official; or
- (g) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, as an IGIS official.

Note: A defendant bears an evidential burden in relation to the matters in subsection (3) (see subsection 13.3(3) of the *Criminal Code*).

- (3A) Subsections (2) and (2A) do not apply to a person disclosing information if:
- (a) the information has already been communicated, or made available, to the public (the *prior publication*); and
 - (b) the person was not involved in the prior publication (whether directly or indirectly); and
 - (c) at the time of the disclosure, the person believes that the disclosure:
 - (i) will not endanger the health or safety of any person; and
 - (ii) will not prejudice the effective conduct of a special intelligence operation; and
 - (d) having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

Note: A defendant bears an evidential burden in relation to the matters in subsection (3A)—see subsection 13.3(3) of the *Criminal Code*.

Extended geographical jurisdiction

- (4) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against subsection (1), (1B), (2) or (2A).

- (5) Subsection (4) does not, by implication, affect the interpretation of any other provision of this Act.

35PA Notifications by Director-General

- (1) The Director-General must cause the Inspector-General of Intelligence and Security to be notified if a special intelligence operation is authorised under this Division.
- (2) The notification must be given:
- (a) in writing; and
 - (b) as soon as practicable after the special intelligence operation authority is granted.

35Q Reports by the Director-General

- (1) If a special intelligence operation is authorised under this Division, the Director-General must give the Attorney-General and the Inspector-General of Intelligence and Security a written report:
- (a) if the special intelligence operation authority has effect for a period of 6 months or less—for that period; or
 - (b) otherwise:
 - (i) for the first 6-months during which the special intelligence operation authority has effect; and
 - (ii) for the remainder of the period during which the special intelligence operation authority has effect.
- (2) A report under subsection (1) must report on the extent to which the special intelligence operation has, during the period to which the report relates, assisted the Organisation in the performance of one or more special intelligence functions.

Note: The Inspector-General of Intelligence and Security has oversight powers in relation to conduct engaged in accordance with this Division: see section 8 of the *Inspector-General of Intelligence and Security Act 1986*.

- (2A) A report under subsection (1) must report on whether conduct of a participant in a special intelligence operation:

Section 35R

- (a) caused the death of, or injury to, any person; or
 - (b) involved the commission of a sexual offence against any person; or
 - (c) resulted in loss of, or damage to, property.
- (3) A report under subsection (1) is not a legislative instrument.

35R Evidence relating to granting of special intelligence operation authority

- (1) The Attorney-General may issue a written certificate signed by the Attorney-General setting out such facts as the Attorney-General considers relevant with respect to the granting of a special intelligence operation authority.
- (2) In any proceeding, a certificate under subsection (1) is prima facie evidence of the matters stated in the certificate.

Part IV—Security assessments

Division 1—Preliminary

35 Interpretation

- (1) In this Part, unless the contrary intention appears:

adverse security assessment means a security assessment in respect of a person that contains:

- (a) any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and
- (b) a recommendation that prescribed administrative action be taken or not be taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.

agency head means:

- (a) the Director-General; or
- (b) the Director-General of the Australian Secret Intelligence Service; or
- (ba) the Director-General of the Australian Signals Directorate; or
- (c) the Director-General of National Intelligence; or
- (d) the Director of that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation; or
- (e) the Director of that part of the Defence Department known as the Defence Intelligence Organisation.

applicant means a person who has applied to the Tribunal for a review of a security assessment.

authority of a State includes a State Minister, Department or Police Force.

Commonwealth contractor means a person performing work or rendering services, otherwise than as an employee, for the purposes

Section 35

of the Commonwealth or an authority of the Commonwealth, including a person performing such work or rendering such services as a sub-contractor or as an adviser or consultant.

delayed security assessment has the meaning given by subsection 41(1).

prescribed administrative action, subject to subsections (1A) and (2), means:

- (a) action that relates to or affects:
 - (i) access by a person to any information or place access to which is controlled or limited on security grounds; or
 - (ii) a person's ability to perform an activity in relation to, or involving, a thing (other than information or a place), if that ability is controlled or limited on security grounds; including action affecting the occupancy of any office or position under the Commonwealth or an authority of the Commonwealth or under a State or an authority of a State, or in the service of a Commonwealth contractor, the occupant of which has or may have any such access or ability; or
- (b) the exercise of any power, or the performance of any function, in relation to a person under the *Migration Act 1958* or the regulations under that Act; or
- (c) the exercise of any power, or the performance of any function, in relation to a person under the *Australian Citizenship Act 2007*, the *Australian Passports Act 2005* or the regulations under either of those Acts; or
- (ca) the exercise of a power under Chapter 2 or 4 of the *Digital ID Act 2024*; or
- (d) the exercise of a power under any of the following provisions of the *Telecommunications Act 1997*:
 - (i) section 58A;
 - (iii) clause 57A of Schedule 3A;
 - (iv) clause 72A of Schedule 3A; or
- (e) the exercise of a power under subsection 30EF(1) or 32(2) of the *Security of Critical Infrastructure Act 2018*; or

- (f) the exercise of a power under Part 5.2 (accreditation framework) of the *Data Availability and Transparency Act 2022*; or
- (g) the exercise of any power, or the performance of any function, in relation to any of the following decisions under a law of the Commonwealth, a State or a Territory:
 - (i) a decision about whether to release a person from prison on parole or on licence;
 - (ii) a decision otherwise relating to the release of a person on parole or on licence (including a decision in relation to conditions or supervision);
 - (iii) a decision about whether to revoke a parole order or a licence mentioned in subparagraph (i); or
- (h) the exercise of any power, or the performance of any function, in relation to any of the following decisions under a law of a State or Territory:
 - (i) a decision about whether to issue a firearms licence or a licence to work as a security guard to a person or otherwise relating to the issue of such a licence (including in relation to conditions);
 - (ii) a decision about whether to revoke a licence mentioned in subparagraph (i); or
- (i) subject to subsection 36AA(1), another action prescribed by the regulations for the purposes of this paragraph.

Note: A condition imposed by a control order is not prescribed administrative action (see subsection (2)). A decision made under the *Foreign Acquisitions and Takeovers Act 1975* or the regulations under that Act is also not prescribed administrative action (see subsection (1A)).

qualified security assessment means a security assessment in respect of a person that:

- (a) contains any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and

Section 35

- (b) does not contain a recommendation of the kind referred to in paragraph (b) of the definition of ***adverse security assessment***;

whether or not the matters contained in the assessment would, by themselves, justify prescribed administrative action being taken or not being taken in respect of the person to the prejudice of the interests of the person.

security assessment or ***assessment*** means a statement in writing furnished by the Organisation to a Commonwealth agency, State or authority of a State expressing any recommendation, opinion or advice on, or otherwise referring to, the question whether it would be consistent with the requirements of security for prescribed administrative action to be taken in respect of a person or the question whether the requirements of security make it necessary or desirable for prescribed administrative action to be taken in respect of a person, and includes any qualification or comment expressed in connection with any such recommendation, opinion or advice, being a qualification or comment that relates or that could relate to that question.

staff member of the Organisation or an intelligence or security agency means:

- (a) the agency head of the Organisation or agency; or
- (b) an employee or officer of the Organisation or agency; or
- (c) a consultant or contractor to the Organisation or agency; or
- (d) a person who is made available by an authority of the Commonwealth, authority of a State or other person to perform services for the Organisation or agency.

Tribunal means the Administrative Review Tribunal.

- (1A) A decision made under the *Foreign Acquisitions and Takeovers Act 1975* or the regulations under that Act is not prescribed administrative action.
- (2) To avoid doubt, none of the following is prescribed administrative action:

Section 36AA

- (a) a condition imposed on a person by a control order made under Division 104 of the *Criminal Code* (control orders);
- (b) a condition imposed on a person by an extended supervision order or interim supervision order under Division 105A of the *Criminal Code* (post-sentence orders);
- (c) action covered by any of subsections 105A.7E(2) to (5) of the *Criminal Code* (actions relating to electronic monitoring);
- (d) a condition imposed on a person by a community safety supervision order under Division 395 of the *Criminal Code* (community safety orders);
- (e) action covered by any of subsections 395.17(2) to (5) of the *Criminal Code* (actions relating to electronic monitoring).

36AA Prescribing actions as *prescribed administrative action*

- (1) Regulations made for the purposes of paragraph (i) of the definition of *prescribed administrative action* in subsection 35(1) (the *relevant regulations*) may prescribe an action if:
 - (a) the action is likely to affect a person's liberty or livelihood; and
 - (b) matters relating to security would be a primary consideration in deciding whether to take the action.
- (2) The Committee on Intelligence and Security must:
 - (a) review the relevant regulations as soon as possible after they are made; and
 - (b) report the Committee's comments and recommendations to each House of the Parliament before the end of the applicable disallowance period for that House.
- (3) If the Committee's report on a review of the relevant regulations is tabled in a House of the Parliament:
 - (a) during the applicable disallowance period for that House; and
 - (b) on or after the eighth sitting day of the applicable disallowance period;then Part 2 of Chapter 3 of the *Legislation Act 2003* has effect, in relation to the relevant regulations and that House, as if each period

Section 36

of 15 sitting days referred to in that Part were extended in accordance with the following table.

Extension of applicable disallowance period		
Item	If the Committee's report is tabled in that House...	extend the period of 15 sitting days by...
1	on the fifteenth sitting day of the applicable disallowance period	8 sitting days of that House
2	on the fourteenth sitting day of the applicable disallowance period	7 sitting days of that House
3	on the thirteenth sitting day of the applicable disallowance period	6 sitting days of that House
4	on the twelfth sitting day of the applicable disallowance period	5 sitting days of that House
5	on the eleventh sitting day of the applicable disallowance period	4 sitting days of that House
6	on the tenth sitting day of the applicable disallowance period	3 sitting days of that House
7	on the ninth sitting day of the applicable disallowance period	2 sitting days of that House
8	on the eighth sitting day of the applicable disallowance period	1 sitting day of that House

- (4) The *applicable disallowance period* for a House of the Parliament means the period of 15 sitting days of that House after the relevant regulations, or a copy of the relevant regulations, were laid before that House in accordance with section 38 of the *Legislation Act 2003*.

36 Part not to apply to certain assessments

- (1) This Part (other than sections 35, 41 and 42 and subsections 37(1), (3) and (4)) does not apply to or in relation to:
- (a) a security assessment in relation to the employment, by engagement outside Australia for duties outside Australia, of

- a person who is not an Australian citizen or is not normally resident in Australia; or
- (b) a security assessment in relation to action of a kind referred to in paragraph (b) of the definition of ***prescribed administrative action*** in section 35 (other than an assessment made for the purposes of subsection 202(1) of the *Migration Act 1958*) in respect of a person who is not:
 - (i) an Australian citizen;
 - (ii) a person who is, within the meaning of the *Migration Act 1958*, the holder of a valid permanent visa; or
 - (iii) a person who holds a special category visa or is taken by subsection 33(2) of the *Migration Act 1958* to have been granted a special purpose visa; or
 - (ba) a security assessment that is a request under section 22A of the *Australian Passports Act 2005* for suspension of all Australian travel documents issued to a person; or
 - (bb) a security assessment in relation to an exercise of a power under Chapter 2 or 4 of the *Digital ID Act 2024* in respect of an entity (within the meaning of that Act) that is not an Australian entity (within the meaning of that Act); or
 - (c) a security assessment in relation to the engagement, or proposed engagement, of a person by or in the Organisation, or an intelligence or security agency, as a staff member of the Organisation or agency.
- (2) Despite paragraph (1)(b), this Part applies to a security assessment in respect of a person if:
- (a) the person was the holder of a valid permanent visa; and
 - (b) the visa was cancelled under section 134B of the *Migration Act 1958*; and
 - (c) the security assessment is made for the purposes of section 134C of that Act in relation to that cancellation.
- (3) This section does not, by implication, affect the interpretation of any other provision of this Part.

36A Part not to apply to security vetting and security clearance related activities

- (1) This Part (other than section 81) does not apply in relation to the exercise of a power or the performance of a function under Part IVA.
- (2) To avoid doubt:
 - (a) a communication made, including a security clearance suitability assessment furnished, by the Organisation in connection with the performance of its function under paragraph 17(1)(cb) is not a security assessment; and
 - (b) any decision made or not made, or action taken or not taken, by a Commonwealth agency, a State or an authority of a State, on the basis of a communication made by the Organisation in connection with the performance of its function under paragraph 17(1)(cb) is not prescribed administrative action within the meaning of paragraph (a) of the definition of *prescribed administrative action* in subsection 35(1).

Division 2—Furnishing of security assessments

37 Security assessments

- (1) The functions of the Organisation referred to in paragraph 17(1)(c) include the furnishing to Commonwealth agencies of security assessments relevant to their functions and responsibilities.
- (2) An adverse or qualified security assessment shall be accompanied by a statement of the grounds for the assessment, and that statement:
 - (a) shall contain all information that has been relied on by the Organisation in making the assessment, other than information the inclusion of which would, in the opinion of the Director-General, be contrary to the requirements of security; and
 - (b) shall, for the purposes of this Part, be deemed to be part of the assessment.
- (3) The regulations may prescribe matters that are to be taken into account, the manner in which those matters are to be taken into account, and matters that are not to be taken into account, in the making of assessments, or of assessments of a particular class, and any such regulations are binding on the Organisation and on the Tribunal.
- (4) Subject to any regulations made in accordance with subsection (3), the Director-General shall, in consultation with the Minister, determine matters of a kind referred to in subsection (3), but nothing in this subsection affects the powers of the Tribunal.
- (5) No proceedings, other than an application to the Tribunal under section 54, shall be brought in any court or tribunal in respect of the making of an assessment or anything done in respect of an assessment in accordance with this Act.

Section 38

38 Person to be notified of assessment

- (1) Subject to this section, where, after the commencement of this Act, an adverse or qualified security assessment in respect of a person is furnished by the Organisation to a Commonwealth agency or a State or an authority of a State, the Commonwealth agency, the State or the authority of the State shall, within 14 days after the day on which the assessment is so furnished, give to that person a notice in writing, to which a copy of the assessment is attached, informing him or her of the making of the assessment and containing prescribed information concerning his or her right to apply to the Tribunal under this Part.
- (2) The Minister may, by writing signed by the Minister delivered to the Director-General, certify that the Minister is satisfied that:
 - (a) the withholding of notice to a person of the making of a security assessment in respect of the person is essential to the security of the nation; or
 - (b) the disclosure to a person of the statement of grounds contained in a security assessment in respect of the person, or of a particular part of that statement, would be prejudicial to the interests of security.
- (3) Where the Minister issues a certificate under subsection (2), he or she shall cause a copy of the certificate to be delivered to the Commonwealth agency, State or authority of a State to which the assessment was furnished.
- (4) Subsection (1) does not require a notice to be given in relation to a security assessment to which a certificate in accordance with paragraph (2)(a) applies.
- (5) In the case of a security assessment in relation to which a certificate certifying in accordance with paragraph (2)(b) has been given, the copy of the assessment to be attached to a notice under subsection (1) shall not contain any matter to which the certificate applies.

- (6) A notice under subsection (1) may be given to a person by delivering it to him or her personally or by sending it to the person by registered post at his or her address last known to the Commonwealth agency, State or authority of a State.
- (7) Before the end of the following periods, the Minister must consider whether to revoke a certificate certifying in accordance with paragraph (2)(a) (if the certificate remains in force):
 - (a) 12 months after it was issued;
 - (b) 12 months after the Minister last considered whether to revoke it.

39 Effect of preliminary advice by Organisation

- (1) Subject to subsections (2), (3) and (4), a Commonwealth agency shall not take, refuse to take or refrain from taking prescribed administrative action on the basis of any communication in relation to a person made by the Organisation not amounting to a security assessment or on the basis of an adverse or qualified security assessment made by the Organisation before the commencement of this Act.
- (2) Subsection (1) does not prevent a Commonwealth agency from taking action of a temporary nature to prevent:
 - (a) access by a person to any information or place access to which is controlled or limited on security grounds; or
 - (b) a person from performing an activity in relation to, or involving, a thing (other than information or a place), if the person's ability to perform that activity is controlled or limited on security grounds;if, on the basis of a preliminary communication by the Organisation, the Commonwealth agency is satisfied that the requirements of security make it necessary to take that action as a matter of urgency pending the furnishing of an assessment by the Organisation.
- (3) Subsection (1) does not prevent a Commonwealth agency from taking prescribed administrative action within the meaning of

Section 40

paragraph (h) of the definition of *prescribed administrative action* in subsection 35(1) on the basis of a communication made under subsection 18(3) or 19A(4) to a staff member of the Commonwealth agency.

- (4) Subsection (1) does not prevent a Commonwealth agency from taking action that is of a temporary nature and is:
- (a) of a kind referred to in paragraph (g) or (h) of the definition of *prescribed administrative action* in subsection 35(1); or
 - (b) of a kind:
 - (i) referred to in paragraph (i) of the definition of *prescribed administrative action* in subsection 35(1); and
 - (ii) prescribed by the regulations for the purposes of this subparagraph;

if, on the basis of a preliminary communication by the Organisation, the Commonwealth agency is satisfied that the requirements of security make it necessary to take that action as a matter of urgency pending the furnishing of an assessment by the Organisation.

40 Assessments and preliminary communications for State purposes

- (1) It is within the functions of the Organisation:
- (a) to furnish a security assessment in respect of a person to a Commonwealth agency for transmission to a State or an authority of a State for use in considering the taking of prescribed administrative action by the State or authority in respect of the person; or
 - (b) to furnish a security assessment in respect of a person to a State or an authority of a State for use in considering the taking of prescribed administrative action by the State or authority in respect of the person.
- (1A) It is also a function of the Organisation to make a preliminary communication, pending the furnishing of a security assessment by the Organisation, to:

- (a) a State or an authority of a State; or
 - (b) a Commonwealth agency for transmission to a State or an authority of a State;
- if the Director-General, or a person authorised by the Director-General under subsection (4), is satisfied that the requirements of security make it necessary as a matter of urgency for the State or authority to take the action referred to in subsection (1B).
- (1B) For the purposes of subsection (1A), the action is any of the following:
- (a) action of a temporary nature to prevent:
 - (i) access by a person to any information or place access to which is controlled or limited on security grounds; or
 - (ii) a person from performing an activity in relation to, or involving, a thing (other than information or a place), if the person's ability to perform that activity is controlled or limited on security grounds;
 - (b) action that is of a temporary nature and of a kind referred to in paragraph (g) or (h) of the definition of ***prescribed administrative action*** in subsection 35(1);
 - (c) action that is of a temporary nature and is of a kind:
 - (i) referred to in paragraph (i) of the definition of ***prescribed administrative action*** in subsection 35(1); and
 - (ii) prescribed by the regulations for the purposes of this subparagraph.
- (2) The Organisation must not, other than in the form of an assessment or in accordance with subsection (1A):
- (a) furnish to a State or an authority of a State any information, recommendation, opinion or advice concerning a person which the Organisation knows is intended or likely to be used by the State or an authority of the State in considering prescribed administrative action in relation to that person; or
 - (b) furnish to a Commonwealth agency any information, recommendation, opinion or advice concerning a person if

Section 41

the Organisation knows that the Commonwealth agency intends to communicate it to a State or an authority of a State for use in considering prescribed administrative action in relation to that person.

- (3) However, subsection (2) does not prevent the communication of information under subsection 18(3) or 19A(4) which the Organisation knows is intended or likely to be used by a State or an authority of a State in considering prescribed administrative action within the meaning of paragraph (h) of the definition of *prescribed administrative action* in subsection 35(1).
- (4) The Director-General may, in writing, authorise a person for the purposes of subsection (1A) if the person is an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.

41 Notification of delayed security assessment

Notification of delayed security assessment

- (1) If a security assessment is not furnished under this Part within 12 months after the Organisation starts to prepare the assessment (the *delayed security assessment*), the Director-General must cause the Inspector-General of Intelligence and Security to be notified of the delayed security assessment.

Note: A protocol made under subsection 42(1) must specify when the Organisation is taken to have started to prepare a security assessment, which may be specified differently for different classes of security assessments (see subsections 42(3) and (4)).

- (2) The notification must:
 - (a) be made within the period specified, for the purposes of subparagraph 42(3)(b)(i), in the protocol made under subsection 42(1), as in force from time to time; and
 - (b) include the information specified in that protocol for the purposes of subparagraph 42(3)(b)(ii); and

- (c) comply with any other requirements specified in the protocol for the purposes of paragraph 42(3)(d).

Exceptions to requirement to notify

- (3) However, subsection (1) does not apply if:
 - (a) the Organisation has been notified that the security assessment is no longer required; or
 - (b) the Organisation initiated the preparation of the security assessment without a request for the assessment being made by another Commonwealth agency, a State or an authority of a State.

Application of this section

- (4) This section applies to a security assessment that the Organisation starts to prepare on or after the commencement of this section.

42 Protocol for dealing with delayed security assessments

Requirement to make protocol

- (1) The Director-General must make a written protocol for dealing with delayed security assessments.
 - Note 1: For variation of a protocol, see subsection 33(3) of the *Acts Interpretation Act 1901*.
 - Note 2: A protocol made under this subsection may be combined with a protocol made under subsection 82GB(1) (protocol for dealing with delayed security clearance decisions and delayed security clearance suitability assessments).
- (2) The Director-General must consult with the Inspector-General of Intelligence and Security before making a protocol under subsection (1).
- (3) The protocol:
 - (a) must specify when the Organisation is taken to have started to prepare a security assessment; and

Section 42

- (b) must specify the following in relation to the notification of a delayed security assessment under section 41:
 - (i) the period within which the notification must be made;
 - (ii) the information to be included in the notification; and
 - (c) must deal with steps to be taken by the Organisation in relation to the delayed security assessment after the notification referred to in paragraph (b) is made; and
 - (d) may specify other requirements, or deal with any other matters, that:
 - (i) relate to a delayed security assessment or the notification of the assessment under section 41; and
 - (ii) the Director-General considers appropriate.
- (4) Without limiting subsection (1), the protocol may provide differently for different classes of security assessments.
- (5) A protocol made under subsection (1) is not a legislative instrument.

Requirement to comply with protocol

- (6) The Organisation must, in relation to a delayed security assessment to which subsection 41(1) applies, comply with a protocol made under subsection (1) of this section, as in force from time to time.

Division 4—Review of security assessments

54 Applications to Tribunal

- (1) An application may be made to the Tribunal for a review of an adverse or qualified security assessment.
- (2) The application may be made by the person in respect of whom the assessment was made and who has been given notice of the assessment under section 38.

61 Effect of findings

Where an assessment has been reviewed by the Tribunal, every Commonwealth agency, State and authority of a State concerned with prescribed administrative action to which the assessment is relevant, and any tribunal, person or authority having power to hear appeals from, or to review, a decision with respect to any prescribed administrative action to which the assessment is relevant, shall treat the findings of the Tribunal, to the extent that they do not confirm the assessment, as superseding that assessment.

64 Restriction on further assessments after review

Where the Tribunal has made findings upon a review of an assessment, the Organisation shall not make a further assessment in respect of the person concerned that is not in accordance with those findings except on the basis of matters occurring after the review or of which evidence was not available at the time of the review.

65 Reference of certain matters to Tribunal by Attorney-General

- (1) Where:
 - (a) before the commencement of this Act, the Organisation furnished, or is alleged to have furnished, to a

Section 65

Commonwealth agency a security assessment, or a communication of a similar nature, concerning a person; or

- (b) after the commencement of this Act, the Organisation has furnished, or is alleged to have furnished, to a Commonwealth agency, State or authority of a State a security assessment, or a communication of a similar nature, concerning a person, other than a security assessment of which a copy has been delivered to that person in accordance with this Part;

the Attorney-General may, if satisfied that it is desirable to do so by reason of special circumstances, require the Tribunal to inquire and report to the Attorney-General and the Minister upon any question concerning that action or alleged action of the Organisation, and may require the Tribunal to review any such assessment or communication and any information or matter on which any such assessment or communication was based, and the Tribunal shall comply with the requirement and report its findings to the Attorney-General and the Minister.

- (1A) For the purposes of determining whether it is desirable to make a requirement of the Tribunal under subsection (1) in relation to a matter, the Attorney-General may request the Inspector-General of Intelligence and Security to inquire into the matter or into a specified aspect of the matter and to report to the Attorney-General and the Minister the results of the inquiry, and the Inspector-General shall comply with any such request.
- (2) The constitution and procedure of the Tribunal under this section shall be as determined by the President of the Tribunal.
- (3) Sections 54, 105, 107, 108, 111 and 112 and Subdivision B of Division 5 of Part 6 of the *Administrative Review Tribunal Act 2024* and section 61 of this Act do not apply in relation to a review under this section but, when the Tribunal has made findings under this section, the Attorney-General shall, subject to the requirements of security, take or cause to be taken such action in relation to those findings, by way of communication or publication of the findings or alteration of records, as the Attorney-General considers appropriate in the interests of justice.

81 Secrecy

- (1) A person who is or has been a member or an officer of the Tribunal shall not, either directly or indirectly, except for the purposes of this Act:
- (a) make a record of, or divulge or communicate to any person, any information acquired by him or her by reason of his or her office or employment under or for the purposes of this Act; or
 - (b) produce to any person a document furnished for the purposes of this Act.

Penalty: Imprisonment for 2 years.

- (2) A person who is or has been a member or an officer of the Tribunal shall not be required to produce in a court any document of which the person has custody, or to which the person has access, by virtue of his or her office or employment under or for the purposes of this Act, or to divulge or to communicate to a court any information obtained by him or her by reason of such an office or employment, except when it is necessary to do so for the purposes of this Act.
- (3) In this section:

court includes any tribunal, authority or person having power to require the production of documents or the answering of questions.

officer of the Tribunal means:

- (a) the Principal Registrar within the meaning of the *Administrative Review Tribunal Act 2024*; or
- (b) a staff member within the meaning of that Act.

produce includes permit access to, and **production** has a corresponding meaning;

and a reference in this section to information or a document shall be read as a reference to information or a document supplied to the Tribunal for the purposes of this Part or Part IVA or otherwise related to proceedings under this Part or Part IVA.

Part IVA—Security vetting and security clearance related activities

Division 1—Preliminary

82 Purpose of this Part

- (1) This Part is made for the purposes of paragraph 17(1)(cb) (which specifies the Organisation’s function in relation to security vetting and security clearance related activities).

Note: Section 81 (secrecy) applies in relation to this Part.

- (2) To avoid doubt:
- (a) the Organisation’s performance of the function specified in paragraph 17(1)(cb) is not limited by the operation of subsection 17(2) (which specifies limits on the Organisation carrying out or enforcing measures for security within an authority of the Commonwealth); and
 - (b) paragraph 17(1)(cb) and this Part do not limit the capacity of any other authority of the Commonwealth to undertake the kinds of activities referred to in that paragraph.

82A Definitions

In this Part:

affected person:

- (a) in relation to an internally reviewable decision—has the meaning given by section 82H; and
- (b) in relation to an externally reviewable decision—has the meaning given by section 83; and
- (c) in relation to an independently reviewable decision—has the meaning given by section 83EA.

authority of a State includes the following:

- (a) a State Minister;

- (b) a Department of State, or a Department of the Public Service, of a State;
- (c) a Police Force of a State;
- (d) a body, whether incorporated or not, established for public purposes by or under a law of a State;
- (e) a body corporate in which a State or a body referred to in paragraph (d) has a controlling interest.

delayed security clearance decision has the meaning given by subsection 82GA(1).

delayed security clearance suitability assessment has the meaning given by subsection 82GA(2).

externally reviewable decision has the meaning given by section 83.

independently reviewable decision has the meaning given by section 83EA.

independent reviewer means a person engaged as an independent reviewer under section 83EF.

internally reviewable decision has the meaning given by section 82H.

internal reviewer has the meaning given by subsection 82L(1).

prejudicial security clearance suitability assessment means a security clearance suitability assessment in respect of a person that contains information that would or could be prejudicial to a security clearance decision in respect of the person.

security vetting agency means an authority of the Commonwealth, a State or an authority of a State, whose functions or activities include making security clearance decisions.

sponsoring agency, in relation to a security clearance, means the Commonwealth agency, State or authority of a State that sponsors

Section 82B

the security clearance or would sponsor the security clearance if it were granted.

82B Simplified outline of this Part

This Part deals with the Organisation's function in relation to security vetting and security clearance related activities.

The function includes undertaking security vetting to assess a person's suitability to hold, or to continue to hold, a security clearance, making security clearance decisions in respect of a person and furnishing security clearance suitability assessments in respect of a person.

The Director-General may, on behalf of the Organisation, exercise the powers and perform the functions of the Organisation under this Part, and may delegate those powers and functions under section 16.

There are some limitations on the actions certain persons or bodies can take on the basis of a communication from the Organisation under this Part that is not in the form of a security clearance suitability assessment. There are also some limitations on when the Organisation can make a communication under this Part to certain persons or bodies if the communication is not in the form of a security clearance suitability assessment.

The Director-General must cause the Inspector-General of Intelligence and Security to be notified of delayed security clearance decisions and delayed security clearance suitability assessments. The Director-General must make a protocol for dealing with such decisions and suitability assessments.

Certain persons may apply to the Organisation for internal review of certain security clearance decisions. Certain persons may apply to the Administrative Review Tribunal for review of certain security clearance decisions made by an internal reviewer and

Section 82B

prejudicial security clearance suitability assessments furnished by the Organisation to a security vetting agency. Certain persons may apply to an independent reviewer for review of certain security clearance decisions made by an internal reviewer.

Certain security clearance decisions and security clearance suitability assessments may be reviewed by the Administrative Review Tribunal if required by the Attorney-General.

Division 2—Security vetting and security clearance related decisions

82C Security vetting and security clearance related activities

- (1) For the purposes of the Organisation's function under paragraph 17(1)(cb), the Organisation may do any of the following:
- (a) undertake security vetting to assess a person's suitability to hold a security clearance;
 - (b) make security clearance decisions;
 - (c) undertake ongoing security vetting and assessment of a person's suitability to continue to hold a security clearance that has been granted, or is taken under paragraph (2)(a) of this section to have been granted, by the Organisation;
 - (d) furnish a security clearance suitability assessment in respect of a person;
 - (e) communicate with a sponsoring agency for a security clearance in relation to the ongoing suitability of a person to hold the security clearance;
 - (f) assume responsibility for a security clearance that has been granted to a person by another security vetting agency;
 - (g) do anything incidental to a thing mentioned in any of paragraphs (a) to (f) of this subsection.

Note: In respect of communications made by the Organisation under this Part, it is the Organisation's responsibility to determine a person's suitability on security grounds to hold a security clearance. In respect of a person employed, or proposed to be employed, by a Commonwealth agency or other body, it is the responsibility of that agency or body to determine the person's suitability on employment grounds to be employed by that agency or body.

- (2) If, at a time, the Organisation assumes responsibility for a security clearance under paragraph (1)(f):
- (a) the security clearance is, after that time, taken to have been granted by the Organisation; and

- (b) this Part applies in relation to a security clearance decision made after that time in respect of the security clearance.

Note: Internal review and review by the Administrative Review Tribunal, as provided for by this Part, do not apply to a security clearance decision made by a security vetting agency in respect of a security clearance before the Organisation assumes responsibility for the clearance.

- (3) To avoid doubt, nothing in this Act prevents the Organisation from making a security clearance decision to impose a condition, or vary a condition imposed, on a security clearance in respect of a person in the following circumstances:
- (a) where the person is not required to agree to the condition, or the variation of the condition, in order for the security clearance to be granted or continued;
 - (b) where the sponsoring agency for the security clearance, or the employer of the person, must agree to the condition, or the variation of the condition, in order for the security clearance to be granted to the person or continued in respect of the person.

82D Director-General's powers, functions and duties

- (1) The powers and functions of the Organisation under this Part may be exercised or performed on behalf of the Organisation by the Director-General.

Note: See section 16 for the Director-General's power to delegate powers and functions under this subsection.

- (2) The Director-General must ensure that the Organisation has policies and procedures in place in relation to the exercise of a power or the performance of a function under this Part, including policies and procedures for the following:
- (a) undertaking security vetting of a person;
 - (b) making security clearance suitability assessments and security clearance decisions.
- (3) If a policy or procedure referred to in subsection (2) is in writing, the policy or procedure is not a legislative instrument.

Section 82E

82E Communications by Organisation to another Commonwealth security vetting agency

- (1) This section applies in relation to a communication by the Organisation to another security vetting agency that is an authority of the Commonwealth (a *Commonwealth security vetting agency*).
- (2) A Commonwealth security vetting agency must not make, refuse to make or refrain from making a security clearance decision in respect of a person on the basis of any communication in relation to the person made by the Organisation not amounting to a security clearance suitability assessment.
- (3) Subsection (2) does not prevent a Commonwealth security vetting agency from making a security clearance decision to temporarily:
 - (a) suspend a security clearance, or revoke a suspension of a security clearance, held by a person; or
 - (b) impose a condition, or vary a condition imposed, on a security clearance in respect of a person;in the circumstances referred to in subsection (4).
- (4) The circumstances are that:
 - (a) the Organisation makes a communication to the Commonwealth security vetting agency pending the furnishing of a security clearance suitability assessment in respect of the person; and
 - (b) the Commonwealth security vetting agency is satisfied, on the basis of that communication, that the requirements of security make it necessary as a matter of urgency to make the security clearance decision pending the furnishing of the security clearance suitability assessment.

82F Communications by Organisation to State security vetting agency

- (1) This section applies in relation to a communication (including a security clearance suitability assessment) by the Organisation to a

security vetting agency that is a State or an authority of a State (a *State security vetting agency*).

- (2) Without limiting paragraph 82C(1)(d), the Organisation may furnish a security clearance suitability assessment in respect of a person to a State security vetting agency by:
 - (a) furnishing the assessment directly to the State security vetting agency; or
 - (b) furnishing the assessment to a Commonwealth agency for transmission to the State security vetting agency.
- (3) The Organisation must not furnish a communication concerning a person, other than in the form of a security clearance suitability assessment or in accordance with subsection (4), to:
 - (a) a State security vetting agency if the Organisation knows the communication is intended or likely to be used by the State security vetting agency in considering whether to make, refuse to make or refrain from making a security clearance decision in respect of the person; or
 - (b) a Commonwealth agency if the Organisation knows that the Commonwealth agency intends to transmit the communication to a State security vetting agency for use in considering whether to make, refuse to make or refrain from making a security clearance decision in respect of the person.
- (4) The Organisation may make a communication, pending the furnishing by the Organisation of a security clearance suitability assessment in respect of a person, to:
 - (a) a State security vetting agency; or
 - (b) a Commonwealth agency for transmission to a State security vetting agency;if the Director-General, or a person authorised by the Director-General under subsection (6), is satisfied that the requirements of security make it necessary as a matter of urgency for the State security vetting agency to make a security clearance decision referred to in subsection (5) in respect of the person.

Section 82G

- (5) For the purposes of subsection (4), the security clearance decision is a decision to temporarily:
 - (a) suspend a security clearance, or revoke a suspension of a security clearance, held by the person; or
 - (b) impose a condition, or vary a condition imposed, on a security clearance in respect of the person.
- (6) The Director-General may, in writing, authorise a person for the purposes of subsection (4) if the person is an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.

82G Statement of grounds for prejudicial security clearance suitability assessments

- (1) The Organisation must prepare a statement of grounds for a prejudicial security clearance suitability assessment furnished in respect of a person.
- (2) The statement of grounds must contain all information that has been relied on by the Organisation in making the prejudicial security clearance suitability assessment, other than information the inclusion of which would, in the opinion of the Director-General or a person authorised by the Director-General under subsection (4), be prejudicial to security.
- (3) For the purposes of this Part, the statement of grounds is taken to be part of the prejudicial security clearance suitability assessment.
- (4) The Director-General may, in writing, authorise a person for the purposes of subsection (2) if the person is an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.

82GA Notification of delayed security clearance decision or delayed security clearance suitability assessment

Notification of delayed security clearance decision or security clearance suitability assessment

- (1) If a security clearance decision is not made under this Part within 12 months after the Organisation starts to consider making the decision (the ***delayed security clearance decision***), the Director-General must cause the Inspector-General of Intelligence and Security to be notified of the delayed security clearance decision.

Note: A protocol made under subsection 82GB(1) must specify when the Organisation is taken to have started to consider making a security clearance decision, which may be specified differently for different classes of security clearance decisions (see subsections 82GB(3) and (4)).

- (2) If a security clearance suitability assessment is not furnished under this Part within 12 months after the Organisation starts to prepare the suitability assessment (the ***delayed security clearance suitability assessment***), the Director-General must cause the Inspector-General of Intelligence and Security to be notified of the delayed security clearance suitability assessment.

Note: A protocol made under subsection 82GB(1) must specify when the Organisation is taken to have started to prepare a security clearance suitability assessment, which may be specified differently for different classes of security clearance suitability assessments (see subsections 82GB(3) and (4)).

- (3) A notification under subsection (1) or (2) must:
- (a) be made within the period specified, for the purposes of subparagraph 82GB(3)(b)(i), in the protocol made under subsection 82GB(1), as in force from time to time; and
 - (b) include the information specified in that protocol for the purposes of subparagraph 82GB(3)(b)(ii); and
 - (c) comply with any other requirements specified in the protocol for the purposes of paragraph 82GB(3)(d).

Section 82GB

Exceptions to requirement to notify

- (4) However, subsection (1) or (2) does not apply if:
- (a) the Organisation has been notified that the security clearance decision or security clearance suitability assessment is no longer required; or
 - (b) the Organisation initiated the making of the security clearance decision or the preparation of the security clearance suitability assessment without a request for the decision or suitability assessment being made by another Commonwealth agency, a State or an authority of a State.

Application of this section

- (5) This section applies to:
- (a) a security clearance decision that the Organisation starts to consider making on or after the commencement of this section; and
 - (b) a security clearance suitability assessment that the Organisation starts to prepare on or after the commencement of this section.

82GB Protocol for dealing with delayed security clearance decisions and delayed security clearance suitability assessments

Requirement to make protocol

- (1) The Director-General must make a written protocol for dealing with delayed security clearance decisions and delayed security clearance suitability assessments.

Note 1: For variation of a protocol, see subsection 33(3) of the *Acts Interpretation Act 1901*.

Note 2: A protocol made under this subsection may be combined with a protocol made under subsection 42(1) (protocol for dealing with delayed security assessments).

- (2) The Director-General must consult with the Inspector-General of Intelligence and Security before making a protocol under subsection (1).
- (3) The protocol:
- (a) must specify the following:
 - (i) when the Organisation is taken to have started to consider making a security clearance decision;
 - (ii) when the Organisation is taken to have started to prepare a security clearance suitability assessment; and
 - (b) must specify the following in relation to the notification under section 82GA of a delayed security clearance decision or delayed security clearance suitability assessment:
 - (i) the period within which the notification must be made;
 - (ii) the information to be included in the notification; and
 - (c) must deal with steps to be taken by the Organisation in relation to the delayed security clearance decision or delayed security clearance suitability assessment after the notification referred to in paragraph (b) is made; and
 - (d) may specify other requirements, or deal with any other matters, that:
 - (i) relate to a delayed security clearance decision or delayed security clearance suitability assessment, or the notification of the decision or suitability assessment under section 82GA; and
 - (ii) the Director-General considers appropriate.
- (4) Without limiting subsection (1), the protocol may provide differently for different classes of security clearance decisions or security clearance suitability assessments.
- (5) A protocol made under subsection (1) is not a legislative instrument.

Requirement to comply with protocol

- (6) The Organisation must, in relation to a delayed security clearance decision or delayed security clearance suitability assessment to
-

Part IVA Security vetting and security clearance related activities

Division 2 Security vetting and security clearance related decisions

Section 82GB

which subsection 82GA(1) or (2) applies, comply with a protocol made under subsection (1) of this section, as in force from time to time.

Division 3—Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Subdivision A—Internal review of certain security clearance decisions

82H Internally reviewable decisions

Internally reviewable decisions

- (1) For the purposes of this Division, each of the following security clearance decisions is an ***internally reviewable decision***:
 - (a) a decision by the Organisation to deny a security clearance in respect of a person (the ***affected person***);
 - (b) a decision by the Organisation to revoke a security clearance held by a person (the ***affected person***);
 - (c) a decision by the Organisation to impose a condition, or vary a condition imposed, on a security clearance in respect of a person (the ***affected person***) if:
 - (i) in the case of a security clearance that has not yet been granted—the affected person must agree to the condition before the security clearance will be granted;
or
 - (ii) in the case of a security clearance that has already been granted—the affected person must agree to the condition, or the variation of the condition, otherwise the security clearance will be revoked.

Exceptions

- (2) A decision of an internal reviewer, on behalf of the Organisation, under subsection 82L(3) is not an ***internally reviewable decision*** for the purposes of this Division.

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 82J

- (3) A security clearance decision in respect of a person is not an *internally reviewable decision* for the purposes of this Division if the person:
- (a) is engaged, or proposed to be engaged, for employment outside Australia for duties outside Australia; and
 - (b) is not an Australian citizen or is not normally resident in Australia.

82J Notification of internally reviewable decision

- (1) Within 14 days after the day on which an internally reviewable decision is made, the Organisation must give the affected person, and the sponsoring agency for the security clearance in relation to which the decision was made, notice in writing of the decision and reasons for the decision.
- (2) A notice given under subsection (1) must also contain prescribed information concerning the affected person's right to apply to the Organisation under this Subdivision for internal review of the decision.
- (3) Section 25D of the *Acts Interpretation Act 1901* does not apply in relation to the reasons notified under subsection (1).
- (4) Without limiting what the Organisation can choose to include or not include in the reasons notified under subsection (1), the Organisation may withhold any of the following from the reasons:
 - (a) any information relating to a standard relating to the Commonwealth's highest level of security clearance that was used to make the decision if the inclusion of the information would, in the opinion of the Director-General or a person authorised by the Director-General under subsection (5), be prejudicial to security;
 - (b) any information that, in the opinion of the Director-General or a person authorised by the Director-General under subsection (5), would be contrary to the public interest:

Section 82K

- (i) because it would prejudice security, the defence of the Commonwealth or the conduct of the Commonwealth's international affairs; or
 - (ii) because it would reveal information that has been disclosed to the Organisation in confidence; or
 - (iii) for a reason that could form the basis for a claim by the Crown in right of the Commonwealth in a judicial proceeding that the information should not be disclosed;
- (c) any information that, in the opinion of the Director-General or a person authorised by the Director-General under subsection (5), could reveal the methodology underlying a psychological assessment of the affected person.
- (5) The Director-General may, in writing, authorise a person for the purposes of subsection (4) if the person is an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.

82K Application for internal review of decision

- (1) An affected person may apply under this section for the review of an internally reviewable decision.
- (2) An application for review must be made, in writing, to the Organisation within:
 - (a) 30 days after the day the person is given notice of the decision under section 82J; or
 - (b) any further period that the Organisation allows.

82L Decision on internal review

Decision on internal review

- (1) If an application for review of an internally reviewable decision is made in accordance with section 82K, the Organisation must arrange for a person (the **internal reviewer**) to review the decision in as timely a manner as is possible.

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 82L

- (2) The internal reviewer must not be the person who made the internally reviewable decision.
- (3) After reviewing the decision, the internal reviewer, on behalf of the Organisation:
 - (a) must make a decision to affirm, vary or set aside the internally reviewable decision; and
 - (b) if the internal reviewer sets aside the internally reviewable decision in respect of a person—may make another security clearance decision in respect of the person for the purposes of paragraph 82C(1)(b).
- (4) A decision of an internal reviewer under paragraph (3)(a) is also taken to be a security clearance decision made by the Organisation for the purposes of paragraph 82C(1)(b).

Notification of internal reviewer's decision

- (5) Within 14 days after the day on which the internal reviewer makes a decision under this section, the Organisation must give the affected person, and the sponsoring agency for the security clearance in relation to which the decision was made, notice in writing of the internal reviewer's decision and reasons for the decision.
- (6) If the internal reviewer's decision under subsection (3) is an externally reviewable decision under Subdivision B, the notice given under subsection (5) must also contain prescribed information concerning the affected person's right to apply to the Administrative Review Tribunal under that Subdivision for review of the decision.
- (6A) If the internal reviewer's decision under subsection (3) is an independently reviewable decision under Subdivision C, the notice given under subsection (5) must also contain prescribed information concerning the affected person's right to apply to an independent reviewer under that Subdivision for review of the decision.

Section 82L

- (7) Section 25D of the *Acts Interpretation Act 1901* does not apply in relation to the reasons notified under subsection (5).
- (8) Without limiting what the Organisation can choose to include or not include in the reasons notified under subsection (5) for a decision, the Organisation may withhold any of the following from the reasons:
- (a) any information relating to a standard relating to the Commonwealth's highest level of security clearance that was used to make the decision if the inclusion of the information would, in the opinion of the Director-General or a person authorised by the Director-General under subsection (9), be prejudicial to security;
 - (b) any information that, in the opinion of the Director-General or a person authorised by the Director-General under subsection (9), would be contrary to the public interest:
 - (i) because it would prejudice security, the defence of the Commonwealth or the conduct of the Commonwealth's international affairs; or
 - (ii) because it would reveal information that has been disclosed to the Organisation in confidence; or
 - (iii) for a reason that could form the basis for a claim by the Crown in right of the Commonwealth in a judicial proceeding that the information should not be disclosed;
 - (c) any information that, in the opinion of the Director-General or a person authorised by the Director-General under subsection (9), could reveal the methodology underlying a psychological assessment of the affected person.
- (9) The Director-General may, in writing, authorise a person for the purposes of subsection (8) if the person is an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.

Section 83

**Subdivision B—Review by the Administrative Review Tribunal
of certain security clearance decisions and security
clearance suitability assessments**

83 Externally reviewable decisions

- (1) For the purposes of this Division, each of the following security clearance decisions by an internal reviewer, on behalf of the Organisation, is an *externally reviewable decision*:
 - (a) a decision under paragraph 82L(3)(a) to affirm an internally reviewable decision in respect of a person (the *affected person*) who, immediately before the internally reviewable decision was made, held a security clearance or was a Commonwealth employee;
 - (b) a decision under paragraph 82L(3)(a) to vary an internally reviewable decision in respect of a person (the *affected person*) who, immediately before the internally reviewable decision was made, held a security clearance or was a Commonwealth employee;
 - (c) any of the following decisions under paragraph 82L(3)(b) in respect of a person (the *affected person*) who, immediately before the internally reviewable decision was made, held a security clearance or was a Commonwealth employee:
 - (i) a decision to deny a security clearance in respect of the affected person;
 - (ii) a decision to revoke a security clearance in respect of the affected person;
 - (iii) a decision to impose a condition, or vary a condition imposed, on a security clearance in respect of the affected person and a circumstance in subparagraph 82H(1)(c)(i) or (ii) applies.
- (2) For the purposes of this Division, a prejudicial security clearance suitability assessment in respect of a person (the *affected person*) furnished by the Organisation to a security vetting agency is an *externally reviewable decision*.

- (3) However, a security clearance decision or a prejudicial security clearance suitability assessment in respect of a person is not an ***externally reviewable decision*** for the purposes of this Division if the person:
- (a) is engaged, or proposed to be engaged, for employment outside Australia for duties outside Australia; and
 - (b) is not an Australian citizen or is not normally resident in Australia.
- (4) For the purposes of this section:

Commonwealth employee means a person who:

- (a) is:
 - (i) an APS employee; or
 - (ii) employed under the *Members of Parliament (Staff) Act 1984*; or
 - (iii) a Parliamentary Service employee (within the meaning of the *Parliamentary Service Act 1999*); or
 - (iv) a member of the Defence Force; or
 - (v) a member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*) or a special member (within the meaning of that Act); or
 - (vi) an employee of an agency within the national intelligence community (within the meaning of the *Office of National Intelligence Act 2018*); and
- (b) has completed any period of probation that applies to the employment; and
- (c) is not employed in a Commonwealth company (within the meaning of the *Public Governance, Performance and Accountability Act 2013*) or corporate Commonwealth entity (within the meaning of that Act).

Note: A person is not a Commonwealth employee if the person is engaged as a consultant, contractor or subcontractor.

Section 83A

83A Notification of prejudicial security clearance suitability assessment that is an externally reviewable decision

Notification of prejudicial security clearance suitability assessment

- (1) Within 14 days after the day on which the Organisation furnishes a prejudicial security clearance suitability assessment that is an externally reviewable decision to a security vetting agency, the security vetting agency must give the affected person notice in writing of the assessment and a copy of the assessment (including a copy of the statement of grounds for the assessment).

Note: The statement of grounds for a security clearance suitability assessment is taken to be part of the assessment (see subsection 82G(3)).

- (2) A notice given under subsection (1) must also contain prescribed information concerning the affected person's right to apply to the Administrative Review Tribunal under this Subdivision for review of the externally reviewable decision.
- (3) However:
- (a) subsections (1) and (2) do not apply if the Minister gives a certificate in accordance with paragraph (4)(a) in respect of the notice for the prejudicial security clearance suitability assessment; and
 - (b) if the Minister gives a certificate in accordance with paragraph (4)(b) in respect of the statement of grounds for the prejudicial security clearance suitability assessment, the copy of the statement of grounds, or that part of the statement to which the certificate applies, must not be given to the affected person.

Certificate to withhold notice or statement of grounds

- (4) The Minister may, by writing signed by the Minister and given to the Director-General, certify that the Minister is satisfied that:

Section 83A

- (a) the withholding of notice of the prejudicial security clearance suitability assessment in respect of the affected person is essential to the security of the nation; or
 - (b) the disclosure to an affected person of the statement of grounds for the prejudicial security clearance suitability assessment in respect of the affected person, or a particular part of that statement, would be prejudicial to the interests of security.
- (5) If the Minister gives a certificate under subsection (4), the Minister must cause a copy of the certificate to be given to the following:
- (a) the security vetting agency to which the prejudicial security clearance suitability assessment was furnished;
 - (b) the sponsoring agency for the security clearance in relation to which the prejudicial security clearance suitability assessment was furnished.
- (6) Before the end of the following periods, the Minister must consider whether to revoke a certificate given under paragraph (4)(a) (if the certificate remains in force):
- (a) 12 months after it was given;
 - (b) each 12 month period after the Minister last considered whether to revoke it.

Delegation

- (7) The Minister may, in writing, delegate the Minister's powers and functions under paragraph (4)(b) to an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.
- (8) In performing a function or exercising a power under a delegation under subsection (7), the delegate must comply with any written directions of the Minister.

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 83B

83B Applications to Administrative Review Tribunal

- (1) Applications may be made to the Administrative Review Tribunal for review of security clearance decisions, or security clearance suitability assessments, that are externally reviewable decisions.
- (2) The application may be made by the person in respect of whom the security clearance decision or security clearance suitability assessment was made and who has been given notice of the decision or assessment under subsection 82L(5) or 83A(1).

83C Statement of grounds for security clearance decision

- (1) This section applies if the Director-General is notified under section 139 of the *Administrative Review Tribunal Act 2024* of an application to the Administrative Review Tribunal for the review of a security clearance decision that is an externally reviewable decision.

Statement of grounds

- (2) As soon as practicable after the Director-General receives notice of the application, the Organisation must:
 - (a) prepare a statement of grounds for the security clearance decision; and
 - (b) subject to subsections (5) and (7), give a copy of the statement of grounds to the affected person.

Note: The Director-General must also lodge a copy of the statement of grounds with the Administrative Review Tribunal (see paragraph 141(2)(b) of the *Administrative Review Tribunal Act 2024*).

- (3) The statement of grounds must contain all information that has been relied on by the Organisation in making the security clearance decision.
- (4) For the purposes of this Part, the statement of grounds is taken to be part of the security clearance decision.

Information to be excluded from copy given to affected person

- (5) If the security clearance decision is in respect of the Commonwealth's highest level of security clearance, the copy of the statement of grounds given to the affected person must not include the following:
- (a) any information relating to a standard relating to the Commonwealth's highest level of security clearance that was used to make the decision if the inclusion of the information would, in the opinion of the Director-General or a person authorised by the Director-General under subsection (8), be prejudicial to security;
 - (b) any information that, in the opinion of the Director-General or a person authorised by the Director-General under subsection (8), would be contrary to the public interest:
 - (i) because it would prejudice security, the defence of the Commonwealth or the conduct of the Commonwealth's international affairs; or
 - (ii) because it would reveal information that has been disclosed to the Organisation in confidence; or
 - (iii) for a reason that could form the basis for a claim by the Crown in right of the Commonwealth in a judicial proceeding that the information should not be disclosed;
 - (c) any information that, in the opinion of the Director-General or a person authorised by the Director-General under subsection (8), could reveal the methodology underlying a psychological assessment of the affected person.

Certificate to withhold statement of grounds

- (6) The Minister may, by writing signed by the Minister and given to the Director-General, certify that the Minister is satisfied that the disclosure to an affected person of the statement of grounds for the security clearance decision in respect of the affected person, or a particular part of that statement, would be prejudicial to the interests of security.

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 83CA

- (7) If the Minister gives a certificate in accordance with subsection (6) in respect of the statement of grounds for the security clearance decision, the copy of the statement of grounds, or that part of the statement to which the certificate applies, must not be given to the affected person.

Delegations and authorisations

- (8) The Director-General may, in writing, authorise a person for the purposes of subsection (5) if the person is an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.
- (9) The Minister may, in writing, delegate the Minister's powers and functions under subsection (6) to an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.
- (10) In performing a function or exercising a power under a delegation under subsection (9), the delegate must comply with any written directions of the Minister.

83CA Access to security clearance standards

- (1) This section applies if:
- (a) an application is made to the Administrative Review Tribunal for review of a security clearance decision or a security clearance suitability assessment that is an externally reviewable decision; and
 - (b) for the purposes of the review, the Director-General of Security gives the Tribunal a copy of a standard (or a part of a standard) certified in writing by the Director-General as a standard relating to the Commonwealth's highest level of security clearance.
- (2) Despite section 149 of the *Administrative Review Tribunal Act 2024*, the applicant and any person representing the applicant must

not be present when the Tribunal is hearing submissions made or evidence adduced in relation to any part of the copy unless:

- (a) that part of the copy has already been disclosed to the applicant; or
- (b) the Director-General of Security consents to the applicant being present.

83D Effect of findings

- (1) If a security clearance decision, or security clearance suitability assessment, that is an externally reviewable decision has been reviewed by the Administrative Review Tribunal:
 - (a) every Commonwealth agency, State or authority of a State for which the security clearance decision or security clearance suitability assessment is relevant; and
 - (b) any tribunal, person or authority having power to hear appeals from, or to review, a decision with respect to the security clearance decision or security clearance suitability assessment;must treat the findings of the Administrative Review Tribunal, to the extent that they do not affirm the security clearance decision or security clearance suitability assessment, as superseding that decision or assessment.
- (2) If the Administrative Review Tribunal has made findings upon a review of a security clearance decision, or security clearance suitability assessment, that is an externally reviewable decision, the Organisation must not make a further security clearance decision or security clearance suitability assessment in respect of the affected person that is not in accordance with those findings except on the basis of matters occurring after the review or of which evidence was not available at the time of the review.

83E Conclusive certificates

- (1) The Minister may, in exceptional circumstances, issue a conclusive certificate in relation to a security clearance decision, or security

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 83EA

clearance suitability assessment, that is an externally reviewable decision if the Minister believes that:

- (a) it would be prejudicial to security to change the decision or assessment; or
 - (b) it would be prejudicial to security for the decision or assessment to be reviewed.
- (2) The Administrative Review Tribunal must not review, or continue to review, a security clearance decision or security clearance suitability assessment in relation to which the Minister has issued a conclusive certificate under subsection (1).

Subdivision C—Review by an independent reviewer

83EA Independently reviewable decisions

- (1) For the purposes of this Division, each of the following security clearance decisions by an internal reviewer, on behalf of the Organisation, is an *independently reviewable decision*:
- (a) a decision under paragraph 82L(3)(a) to affirm an internally reviewable decision in respect of a person (the *affected person*) who, immediately before the internally reviewable decision was made, neither held a security clearance nor was a Commonwealth employee;
 - (b) a decision under paragraph 82L(3)(a) to vary an internally reviewable decision in respect of a person (the *affected person*) who, immediately before the internally reviewable decision was made, neither held a security clearance nor was a Commonwealth employee;
 - (c) any of the following decisions under paragraph 82L(3)(b) in respect of a person (the *affected person*) who, immediately before the internally reviewable decision was made, neither held a security clearance nor was a Commonwealth employee:
 - (i) a decision to deny a security clearance in respect of the affected person;

Section 83EA

- (ii) a decision to revoke a security clearance in respect of the affected person;
 - (iii) a decision to impose a condition, or vary a condition imposed, on a security clearance in respect of the affected person and a circumstance in subparagraph 82H(1)(c)(i) or (ii) applies.
- (2) However, a security clearance decision in respect of a person is not an ***independently reviewable decision*** for the purposes of this Division if the person:
- (a) is engaged, or proposed to be engaged, for employment outside Australia for duties outside Australia; and
 - (b) is not an Australian citizen or is not normally resident in Australia.
- (3) For the purposes of this section:

Commonwealth employee means a person who:

- (a) is:
 - (i) an APS employee; or
 - (ii) employed under the *Members of Parliament (Staff) Act 1984*; or
 - (iii) a Parliamentary Service employee (within the meaning of the *Parliamentary Service Act 1999*); or
 - (iv) a member of the Defence Force; or
 - (v) a member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*) or a special member (within the meaning of that Act); or
 - (vi) an employee of an agency within the national intelligence community (within the meaning of the *Office of National Intelligence Act 2018*); and
- (b) has completed any period of probation that applies to the employment; and
- (c) is not employed in a Commonwealth company (within the meaning of the *Public Governance, Performance and Accountability Act 2013*) or corporate Commonwealth entity (within the meaning of that Act).

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 83EB

Note: A person is not a Commonwealth employee if the person is engaged as a consultant, contractor or subcontractor.

83EB Application for independent review of decision

- (1) An affected person may apply under this section for review of an independently reviewable decision.
- (2) An application for review must be made, in writing, to an independent reviewer within:
 - (a) 30 days after the day the person is given notice of the decision under section 82L(5); or
 - (b) any further period that an independent reviewer allows.

Note: The notice given to the affected person of the independently reviewable decision must contain prescribed information concerning the person's right to apply to an independent reviewer for review of the decision (see subsection 82L(6A)).

- (3) As soon as practicable after receiving an application made in accordance with subsection (2), the independent reviewer must:
 - (a) decide whether to review the independently reviewable decision; and
 - (b) give the affected person, the Director-General and the sponsoring agency for the security clearance in relation to which the independently reviewable decision was made notice in writing of the independent reviewer's decision under paragraph (a).

83EC Director-General to provide information to independent reviewer

- (1) If the Director-General receives notice under paragraph 83EB(3)(b) that the independent reviewer has decided to review the independently reviewable decision, the Director-General must, in as timely a manner as is possible, provide to the independent reviewer all information that was relied upon by the internal reviewer in making the independently reviewable decision.

Section 83EC

- (2) Without limiting subsection (1), the Director-General may provide to the independent reviewer a copy of any standard (or part thereof) certified in writing by the Director-General as a standard relating to the Commonwealth's highest level of security clearance that was used to make the independently reviewable decision.

Note: A standard relating to the Commonwealth's highest level of security clearance is part of the Australian Government's framework of protective security policy.

- (3) The independent reviewer may, in writing, request the Director-General to seek information from the affected person for the purposes of the independent review.
- (4) If the Director-General receives a request under subsection (3), the Director-General must use the Director-General's best endeavours to seek the information from the affected person and provide the information to the independent reviewer.
- (5) The independent reviewer must:
- (a) comply with any reasonable directions of the Director-General in relation to the protection or handling of information provided to the independent reviewer under this section; and
 - (b) do all things necessary to ensure that any information provided to the independent reviewer (including any copy of a standard provided to the independent reviewer under subsection (2)) is not disclosed to the affected person.

Delegation

- (6) The Director-General may, in writing, delegate the Director-General's powers and functions under subsection (1) to an ASIO employee, or an ASIO affiliate.
- (7) The Director-General may, in writing, delegate the Director-General's powers and functions under paragraph (5)(a) to an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 83ED

- (8) In performing a function or exercising a power under a delegation under subsection (6) or (7), the delegate must comply with any written directions of the Director-General.

83ED Independent review of decision

Consideration of decision

- (1) This section applies if the independent reviewer decides under subsection 83EB(3) to review the independently reviewable decision.
- (2) The independent reviewer must review the decision in as timely a manner as is possible.
- (3) In reviewing the decision the independent reviewer must:
- (a) consider all the information provided to the independent reviewer by the Director-General under section 83EC; and
 - (b) if the Director-General provided a certified copy of a standard (or part thereof) under subsection 83EC(2)—the independent reviewer must apply the standard (or part thereof).

Opinion in relation to decision

- (4) After reviewing the decision, the independent reviewer must give the Director-General, in writing, the independent reviewer's opinion as to whether the independently reviewable decision was reasonably open to have been made by the internal reviewer who made the decision.
- (5) The independent reviewer must also give a copy of the opinion to the Inspector-General of Intelligence and Security.
- (6) Within 14 days after the day on which the independent reviewer gives the Director-General the opinion under subsection (4), the independent reviewer must give the affected person, and the sponsoring agency for the security clearance in relation to which

the independently reviewable decision was made, notice that the opinion has been given.

- (7) The independent reviewer must not give the opinion to the affected person or the sponsoring agency for the security clearance in relation to which the independently reviewable decision was made.

83EE Director-General's consideration of independent reviewer's opinion

- (1) If the independent reviewer has, under subsection 83ED(4), given the Director-General an opinion in relation to the independently reviewable decision, the Director-General must, in as timely a manner as is possible, consider the opinion and decide whether to take any action.

Note: An action may include causing the making, by the Organisation, of a new security clearance decision in respect of the affected person under Division 2.

- (2) The Director-General must, as soon as practicable after deciding whether to take any action, give the affected person, the Inspector-General of Intelligence and Security and the sponsoring agency for the security clearance in relation to which the independently reviewable decision was made notice in writing of the Director-General's decision.
- (3) If an action the Director-General decides to take is to cause the Organisation to make a new security clearance decision in respect of the affected person under Division 2, the Director-General must ensure that the new decision is not made by either of the following:
- (a) the internal reviewer who made the independently reviewable decision;
 - (b) the person who made the internally reviewable decision in respect of which the internal reviewer made the independently reviewable decision.

Part IVA Security vetting and security clearance related activities

Division 3 Review of certain security clearance decisions and prejudicial security clearance suitability assessments

Section 83EF

Delegation

- (4) The Director-General may, in writing, delegate the Director-General's powers and functions under subsection (1) to an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee.
- (5) In performing a function or exercising a power under a delegation under subsection (4), the delegate must comply with any written directions of the Director-General.

83EF Attorney-General may engage independent reviewers

- (1) The Attorney-General may, on behalf of the Commonwealth, engage one or more individuals, as contractors, to be independent reviewers for the purposes of this Subdivision.
- (2) The engagement must be by written agreement.
- (3) The Attorney-General must not engage a person to be an independent reviewer unless the Attorney-General is satisfied that:
 - (a) the person has appropriate skills or qualifications to perform the role; and
 - (b) the person holds a security clearance that is the Commonwealth's highest level of security clearance.
- (4) A person must not be engaged as an independent reviewer if the person is a current, or former, ASIO employee or ASIO affiliate.

Division 4—Other matters relating to review by the Administrative Review Tribunal

83F Reference of certain matters to Administrative Review Tribunal by Attorney-General

- (1) This section applies if:
 - (a) the Organisation has furnished to a security vetting agency a security clearance suitability assessment in respect of a person other than a security clearance suitability assessment of which a copy has been given to that person in accordance with this Part; or
 - (b) the Organisation has made a security clearance decision in respect of a person other than a security clearance decision that is an internally reviewable decision or an externally reviewable decision.
- (2) The Attorney-General may, if satisfied that it is desirable to do so by reason of special circumstances, require the Administrative Review Tribunal to:
 - (a) inquire and report to the Attorney-General and the Minister upon any question concerning the furnishing of the security clearance suitability assessment or the making of the security clearance decision; or
 - (b) review the security clearance suitability assessment or security clearance decision and any information or matter on which the assessment or decision was based.
- (3) If the Attorney-General makes a requirement of the Administrative Review Tribunal under subsection (2), the Tribunal must comply with the requirement and report its findings to the Attorney-General and the Minister.
- (4) For the purposes of determining whether it is desirable to make a requirement of the Administrative Review Tribunal under subsection (2) in relation to a matter, the Attorney-General may request the Inspector-General of Intelligence and Security to:

Section 83F

- (a) inquire into the matter or into a specified aspect of the matter;
and
 - (b) report to the Attorney-General and the Minister the results of the inquiry.
- (5) If the Attorney-General makes a request of the Inspector-General under subsection (4), the Inspector-General must comply with the request.
- (6) The constitution and procedure of the Administrative Review Tribunal under this section must be as determined by the President of the Tribunal.
- (7) The following provisions do not apply in relation to a review under this section:
 - (a) subsection 83D(1) of this Act (which is about the effect of findings);
 - (b) sections 54, 105, 107, 108, 111, 112 and 163 and Subdivision B of Division 5 of Part 6 of the *Administrative Review Tribunal Act 2024* (which are about the Tribunal's decision on review and the Tribunal's findings).
- (8) However, if the Administrative Review Tribunal has made findings under this section, the Attorney-General must, subject to the requirements of security, take or cause to be taken such action in relation to those findings, by way of communication or publication of the findings or alteration of records, as the Attorney-General considers appropriate in the interests of justice.

Part V—ASIO employees etc.

84 Employees of the Organisation

Employees

- (1) The Director-General may, on behalf of the Commonwealth, employ such persons as he or she considers necessary for the performance of the Organisation's functions and the exercise of the Organisation's powers.
- (2) The Director-General may from time to time determine in writing the terms and conditions of employment applying to persons employed under subsection (1).
- (3) The Director-General, on behalf of the Commonwealth, has all the rights, duties and powers of an employer in respect of persons employed under subsection (1).
- (4) Without limiting subsection (3), the Director-General has, in respect of persons employed under subsection (1), the rights, duties and powers that are prescribed by regulation.

Termination of employment

- (5) The Director-General may, at any time, by written notice, terminate the employment of a person employed under subsection (1).

Note: The *Fair Work Act 2009* has rules and entitlements that apply to termination of employment.

85 Consultants and contractors

- (1) The Director-General may engage persons as consultants or contractors to the Organisation.
- (2) An engagement under subsection (1) is to be made:

Section 86

- (a) on behalf of the Commonwealth; and
- (b) by written agreement.

86 Secondment of ASIO employees

Secondment

- (1) The Director-General may, in writing, arrange for an ASIO employee to be seconded for a specified period to a body or organisation whether within or outside Australia.

Termination of secondment

- (2) The Director-General may at any time, by notice given to the body or organisation to which an ASIO employee is seconded under subsection (1), terminate the secondment.

87 Secondment of persons to the Organisation

- (1) The Director-General may, by written agreement with a body or organisation (whether within or outside Australia), arrange for a person who is an officer, employee or other member of staff of the body or organisation to be made available to the Organisation to perform services in connection with the performance or the exercise of any of the Organisation's functions or powers.
- (2) The terms and conditions (including remuneration and allowances) applicable to a person performing services under an agreement are those specified in the agreement.

88 Applicability of principles of the *Public Service Act 1999*

Although ASIO employees are not employed under the *Public Service Act 1999*, the Director-General must adopt the principles of that Act in relation to ASIO employees to the extent to which the Director-General considers they are consistent with the effective performance of the functions of the Organisation.

89 Voluntary moves to APS

- (1) Section 26 of the *Public Service Act 1999* applies in relation to an ASIO employee as if the ASIO employee were an APS employee and the Organisation were an APS Agency.
- (2) An ASIO employee who moves to an APS Agency under that section is entitled to have his or her employment, as an ASIO employee, treated as if it were:
 - (a) employment as an APS employee; and
 - (b) at a corresponding classification, as agreed between the Director-General and the Australian Public Service Commissioner.

90 Regulations relating to employment of persons

- (1) The regulations may make provision for the employment of persons otherwise than under section 84 and may, in respect of persons so employed, make provision from time to time for their terms and conditions of employment (including salaries).
- (2A) The regulations may make provision for the establishment of a body, or for a person, to review actions of the Organisation affecting persons who are ASIO employees, ASIO affiliates, former ASIO employees or former ASIO affiliates, and for the immunity from civil proceedings of any such body or person in relation to their review of such actions.
- (3) Regulations made in accordance with this section have effect despite section 84.

91 Application of Crimes Act

The Director-General and ASIO employees and ASIO affiliates shall be deemed to be Commonwealth officers for the purposes of the *Crimes Act 1914*.

Section 92

92 Making public the identity of ASIO employees and ASIO affiliates

Offence

- (1) A person commits an offence if:
- (a) the person makes information public, or causes or permits information to be made public; and
 - (b) any of the following applies:
 - (i) the information identifies a person as being an ASIO employee, a former ASIO employee, an ASIO affiliate or a former ASIO affiliate;
 - (ii) the information could reasonably lead to establishing the identity of a person as being an ASIO employee, a former ASIO employee, an ASIO affiliate or a former ASIO affiliate;
 - (iii) the identity of a person as being an ASIO employee, a former ASIO employee, an ASIO affiliate or a former ASIO affiliate could reasonably be inferred from the information.

Penalty: Imprisonment for 10 years.

Exceptions

- (2) Subsection (1) does not apply to a person making information public, or causing or permitting information to be made public, if the Minister or Director-General has consented in writing to the information being made public.

Note: A defendant bears an evidential burden in relation to the matters in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

- (3) Subsection (1) does not apply to a person making information public, or causing or permitting information to be made public, if:
- (a) the information relates to a person who is a former ASIO employee or former ASIO affiliate; and
 - (b) the former ASIO employee or former ASIO affiliate has:

Section 92A

- (i) consented in writing to the information being made public; or
- (ii) caused or authorised the fact that the person is a former ASIO employee or former ASIO affiliate to be made public; and
- (c) the person making the information public, or causing or permitting the information to be made public, is not that former ASIO employee or former ASIO affiliate.

Note: A defendant bears an evidential burden in relation to the matters in subsection (3) (see subsection 13.3(3) of the *Criminal Code*).

Extended geographical jurisdiction

- (4) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against subsection (1) of this section.
- (5) Subsection (4) does not, by implication, affect the interpretation of any other provision of this Act or another Act.

Attorney-General's involvement in prosecution of offence

- (6) A prosecution for an offence against subsection (1) may only be instituted by, or with the consent of, the Attorney-General.

Note: For communication of information about an offence against this section to appropriate authorities, see subsection 18(3).

Minister or Director-General's consent

- (7) Consent given under this section is not a legislative instrument.

92A Disclosing the identity of ASIO employees and ASIO affiliates*Offence*

- (1) A person (the **defendant**) commits an offence if:
 - (a) either:
 - (i) the defendant discloses information to another person;
 - or

Section 92A

- (ii) the defendant engages in conduct that results in information being disclosed to another person; and
- (b) any of the following applies:
 - (i) the information identifies a person as being an ASIO employee, a former ASIO employee, an ASIO affiliate or a former ASIO affiliate;
 - (ii) the information could reasonably lead to establishing the identity of a person as being an ASIO employee, a former ASIO employee, an ASIO affiliate or a former ASIO affiliate;
 - (iii) the identity of a person as being an ASIO employee, a former ASIO employee, an ASIO affiliate or a former ASIO affiliate could reasonably be inferred from the information; and
- (c) any of the following applies:
 - (i) the defendant intends to endanger the health or safety of a person;
 - (ii) the defendant intends to prejudice the effective performance of the functions or duties, or the effective exercise of the powers, of the Organisation;
 - (iii) the defendant knows that the disclosure will endanger the health or safety of a person;
 - (iv) the defendant knows that the disclosure will prejudice the effective performance of the functions or duties, or the effective exercise of the powers, of the Organisation.

Penalty: Imprisonment for 10 years.

Extended geographical jurisdiction

- (2) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against subsection (1) of this section.
- (3) Subsection (2) does not, by implication, affect the interpretation of any other provision of this Act or another Act.

Section 92B

Attorney-General's involvement in prosecution of offences

- (4) A prosecution for an offence against subsection (1) may only be instituted by, or with the consent of, the Attorney-General.

Note: For communication of information about an offence against this section to appropriate authorities, see subsection 18(3).

92B Cover employment for ASIO employees and ASIO affiliates

- (1) A person who is an ASIO employee or ASIO affiliate, or a former ASIO employee or former ASIO affiliate, may identify an authority of the Commonwealth as that person's employer or place of work, in relation to a period during which the person is or was an ASIO employee or ASIO affiliate, in accordance with a determination made by the Director-General under subsection 92C(1).
- (2) Subsection (1) applies despite any other law of the Commonwealth, a State or a Territory (whether passed or made before, on or after the commencement of this section), including such other law that is expressed to apply despite any other law.

92C Cover employment—determining a specified authority of the Commonwealth*Determining specified authority of the Commonwealth*

- (1) Subject to subsection (5), the Director-General may, in writing, determine one or more specified authorities of the Commonwealth, within the meaning of paragraphs (a), (aa), (b) and (c) of the definition of *authority of the Commonwealth* in section 4, that may be identified as the employer or place of work of ASIO employees, ASIO affiliates, former ASIO employees or former ASIO affiliates.

Note: For variation and revocation of an instrument, see subsection 33(3) of the *Acts Interpretation Act 1901*.

- (2) Without limiting subsection (1), a determination under that subsection may do either or both of the following:

Section 92C

- (a) determine a specified authority of the Commonwealth in relation to a specified class of ASIO employees, ASIO affiliates, former ASIO employees or former ASIO affiliates;
 - (b) specify limitations or restrictions in relation to the identification of a specified authority of the Commonwealth as the employer or place of work of ASIO employees, ASIO affiliates, former ASIO employees or former ASIO affiliates.
- (3) To avoid doubt, and without limiting subsection (1) or (2), if a determination under subsection (1) determines a specified authority of the Commonwealth in relation to a class of ASIO employees, ASIO affiliates, former ASIO employees or former ASIO affiliates holding, occupying or performing the duties of a specified office or position, the class includes such an office or position that comes into existence after the determination is made.
- (4) Subsection (3) does not, by implication, affect the interpretation of any other provision of this Act.
- (5) The Director-General must not determine a specified authority of the Commonwealth under subsection (1) unless the head of that authority has agreed, in writing, to the authority being so determined.
- (6) To avoid doubt, the Chief of the Defence Force (within the meaning of the *Defence Act 1903*) is the head of the Defence Force for the purposes of subsection (5).
- Note: The Defence Force is an authority of the Commonwealth: see paragraph (b) of the definition of *authority of the Commonwealth* in section 4.
- (7) The following are not legislative instruments:
- (a) a determination under subsection (1);
 - (b) an agreement under subsection (5).

Delegation

- (8) The Director-General may, in writing, delegate the Director-General's powers or duties under this section to an ASIO

Section 92D

employee, or an ASIO affiliate, who holds or is acting in a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee with a classification of SES Band 3.

- (9) In exercising powers or discharging duties under a delegation under subsection (8), the delegate must comply with any written direction given by the Director-General to the delegate.

92D Protection from criminal liability—third parties

- (1) If a person does something that, apart from this section, would be an offence against a law of the Commonwealth, a State or a Territory, the person is not criminally responsible for the offence if:
- (a) the person is a staff member of any authority of the Commonwealth; and
 - (b) the thing is done in the course of the person exercising or performing the person's powers, functions or duties as such a staff member; and
 - (c) the thing is done to facilitate an ASIO employee or ASIO affiliate, or a former ASIO employee or former ASIO affiliate, (the *ASIO person*) to identify an authority of the Commonwealth as the ASIO person's employer or place of work in relation to a period for the purposes of subsection 92B(1), in accordance with a determination under subsection 92C(1); and
 - (d) doing the thing would not be an offence if the authority of the Commonwealth referred to in paragraph (c) were the ASIO person's employer or place of work for the period mentioned in that paragraph.
- (2) If a person does something that, apart from this section, would be an offence against a law of the Commonwealth, a State or a Territory, the person is not criminally responsible for the offence if:
- (a) the thing is done in the performance of the functions attaching to the person's professional capacity; and

Section 92D

- (b) the thing is done to facilitate an ASIO employee or ASIO affiliate, or a former ASIO employee or former ASIO affiliate, (the *ASIO person*) to identify an authority of the Commonwealth as the ASIO person's employer or place of work in relation to a period for the purposes of subsection 92B(1), in accordance with a determination under subsection 92C(1); and
- (c) doing the thing would not be an offence if the authority of the Commonwealth referred to in paragraph (b) were the ASIO person's employer or place of work for the period mentioned in that paragraph.

Part VI—Miscellaneous**93A Costs in certain ART reviews**

- (1) If:
- (a) a person makes an application under section 54 or 83B to the Administrative Review Tribunal for a review of a security assessment, security clearance decision or security clearance suitability assessment in respect of the person; and
 - (b) the applicant was, in the opinion of the Tribunal, successful, or substantially successful, in the application for review; and
 - (c) the Tribunal is satisfied that it is appropriate to do so in all the circumstances of the case;
- the Tribunal may order that the costs reasonably incurred by the applicant in connection with the application, or any part of those costs that is determined by the Tribunal, be paid by the Commonwealth.
- (2) For the purposes of section 115 of the *Administrative Review Tribunal Act 2024*, the Commonwealth is taken to be a party to the proceeding referred to in subsection (1) of this section.

93 Offences

- (5) Where, in proceedings for an offence against this Act in respect of any conduct engaged in by a body corporate, it is necessary to establish the state of mind of the body corporate, it is sufficient to show that a director, employee or agent of the body corporate, being a director, employee or agent by whom the conduct was engaged in within the scope of his or her actual or apparent authority, had that state of mind.
- (6) Any conduct engaged in on behalf of a body corporate:
- (a) by a director, employee or agent of the body corporate within the scope of his or her actual or apparent authority; or

Section 94

- (b) by any other person at the direction or with the consent or agreement (whether express or implied) of a director, employee or agent of the body corporate, where the giving of the direction, consent or agreement is within the scope of the actual or apparent authority of the director, employee or agent;
- shall be deemed, for the purposes of this Act, to have been engaged in by the body corporate.
- (7) A reference in subsection (5) to the state of mind of a person includes a reference to the knowledge, intention, opinion, belief or purpose of the person and the person's reasons for his or her intention, opinion, belief or purpose.

94 Annual report

- (1) The annual report prepared by the Director-General and given to the Minister under section 46 of the *Public Governance, Performance and Accountability Act 2013* for a period must include a statement of:
- (a) the total number of requests made during the period under Division 3 of Part III to the Attorney-General for the issue of warrants under that Division (including the number of requests made orally); and
 - (b) the total number of warrants issued during the period under that Division (including the number of warrants issued orally); and
 - (c) the number of times persons were apprehended during the period under that Division; and
 - (d) the number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the period under that Division and the total of all those hours for all those persons; and
 - (e) the number of times each prescribed authority had persons appear for questioning before the prescribed authority under warrants issued during the period under that Division.

- (2) A statement included under subsection (1) in a report must not name, or otherwise specifically identify, any person to whom information provided in the report relates.
- (2A) A report under subsection (1) must also include a statement of:
- (a) the total number of applications made under section 35B during the period for the granting of special intelligence operation authorities; and
 - (b) the total number of special intelligence operation authorities granted during the period; and
 - (c) the number of authorisations made during the period under section 175 and subsection 176(3) of the *Telecommunications (Interception and Access) Act 1979*; and
 - (d) the purposes for which those authorisations were made; and
 - (e) the lengths of time for which the information or documents that were, or would have been, covered by those authorisations had been held when access was sought; and
 - (f) the number of those authorisations that related to retained data that included information of a kind referred to in item 1 of the table in subsection 187AA(1) of that Act; and
 - (g) the number of those authorisations that related to retained data that included information of a kind referred to in item 2, 3, 4, 5 or 6 of the table in subsection 187AA(1) of that Act; and
 - (h) the number of those authorisations that were made under journalist information warrants issued under Subdivision B of Division 4C of Part 4-1 of that Act; and
 - (i) the number of journalist information warrants issued under that Subdivision during the period; and
 - (j) information of a kind declared under subsection (2C) of this section.
- (2B) A report under subsection (1) is to set out the matters referred to in paragraph (2A)(e) by specifying:
- (a) in relation to each of 8 successive periods of 3 months, the number of the authorisations sought for information or

Section 94

documents held for lengths of time included in that period;
and

- (b) the number of the authorisations sought for information or documents held for lengths of time exceeding 24 months.

(2BA) A report under subsection (1) must also include a statement of:

- (a) the total number of technical assistance requests given by the Director-General under paragraph 317G(1)(a) of the *Telecommunications Act 1997* during the period; and
- (b) the total number of technical assistance notices given by the Director-General under section 317L of the *Telecommunications Act 1997* during the period; and
- (c) the total number of technical capability notices given by the Attorney-General under section 317T of the *Telecommunications Act 1997* during the period that relate to the Organisation.

(2BB) For the purposes of paragraph (2BA)(c), a technical capability notice **relates to** the Organisation if the acts or things specified in the notice:

- (a) are directed towards ensuring that a designated communications provider (within the meaning of Part 15 of the *Telecommunications Act 1997*) is capable of giving listed help (within the meaning of section 317T of that Act) to the Organisation in relation to a matter covered by paragraph 317T(2)(a) of that Act; or
- (b) are by way of giving help to the Organisation in relation to a matter covered by paragraph 317T(2)(b) of the *Telecommunications Act 1997*.

(2BBA) A report under subsection (1) must also include a statement of:

- (a) the relevant statistics about applications made by the Organisation under clause 83 of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* during the period; and
- (b) the relevant statistics about applications made by the Organisation under clause 92 of that Schedule during the period; and

- (c) the relevant statistics about applications made by the Organisation under clause 101 of that Schedule during the period; and
- (d) the number of international production orders issued under clause 89 of that Schedule that were given by the Australian Designated Authority to prescribed communications providers during the period; and
- (e) the number of international production orders issued under clause 98 of that Schedule that were given by the Australian Designated Authority to prescribed communications providers during the period; and
- (f) the number of international production orders issued under clause 107 of that Schedule that were given by the Australian Designated Authority to prescribed communications providers during the period; and
- (g) for each designated international agreement—the number of international production orders issued under Part 4 of that Schedule that:
 - (i) were given by the Australian Designated Authority to prescribed communications providers during the period; and
 - (ii) invoked the designated international agreement; and
- (h) if subparagraph 89(2)(e)(ii) or (f)(ii) of that Schedule applied to one or more international production orders issued under clause 89 of that Schedule during the period—the number of those orders; and
- (i) the number of international production orders cancelled by the Australian Designated Authority under clause 112 of that Schedule during the period; and
- (j) the number of international production orders revoked by the Director-General of Security under clause 116 of that Schedule during the period; and
- (k) if one or more international production orders issued under Part 4 of that Schedule were cancelled by the Australian Designated Authority under clause 122 of that Schedule during the period—the number of those orders; and

Section 94

- (l) if there were one or more occasions during the period when protected information obtained in accordance with an international production order issued under Part 4 of that Schedule was communicated by an ASIO official to a person other than an ASIO official—the number of those occasions; and
 - (m) if one or more objections were received by the Australian Designated Authority under clause 121 of that Schedule during the period in relation to international production orders issued under Part 4 of that Schedule:
 - (i) the number of international production orders to which those objections relate; and
 - (ii) the number of each type of those orders; and
 - (iii) for each designated international agreement—the number of those orders that invoked the designated international agreement.
- (2BBB) An expression used in subsection (2BBA) has same meaning as in Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*.
- (2BC) A report under subsection (1) must also include a statement of:
- (a) the total number of requests made under paragraph 21A(1)(a) during the period; and
 - (b) the total number of orders made under subsection 34AAD(2) during the period.
- (2BD) A report under subsection (1) must also include a statement of:
- (a) the total number of requests made under subsection 26G(1) during the period; and
 - (b) the total number of authorisations given under section 26G during the period.
- (2C) The Minister may, by legislative instrument, declare kinds of information that are to be set out in a report under subsection (1).
- (3) A copy of the report must be given to the Leader of the Opposition in the House of Representatives, but it is the duty of the Leader of

the Opposition to treat as secret any part of the report that is not tabled in a House of the Parliament.

- (4) Subject to subsection (5), the Minister must cause a copy of the report to be laid before each House of the Parliament within 20 sitting days of that House after the report is received by the Minister.
- (5) For the purposes of subsection (4), the Minister may make such deletions from the report as the Minister, after obtaining advice from the Director-General, considers necessary in order to avoid prejudice to security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs or the privacy of individuals.
- (6) The Minister must not delete from a report a statement described in subsection (1).

95 Regulations

The Governor-General may make regulations, not inconsistent with this Act, prescribing all matters required or permitted by this Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to this Act.

Note: Regulations made for the purposes of paragraph (i) of the definition of *prescribed administrative action* in subsection 35(1) are subject to an extended disallowance period (see section 36AA).

Endnotes

Endnote 1—About the endnotes

Endnotes

Endnote 1—About the endnotes

The endnotes provide information about this compilation and the compiled law.

The following endnotes are included in every compilation:

Endnote 1—About the endnotes

Endnote 2—Abbreviation key

Endnote 3—Legislation history

Endnote 4—Amendment history

Abbreviation key—Endnote 2

The abbreviation key sets out abbreviations that may be used in the endnotes.

Legislation history and amendment history—Endnotes 3 and 4

Amending laws are annotated in the legislation history and amendment history.

The legislation history in endnote 3 provides information about each law that has amended (or will amend) the compiled law. The information includes commencement details for amending laws and details of any application, saving or transitional provisions that are not included in this compilation.

The amendment history in endnote 4 provides information about amendments at the provision (generally section or equivalent) level. It also includes information about any provision of the compiled law that has been repealed in accordance with a provision of the law.

Editorial changes

The *Legislation Act 2003* authorises First Parliamentary Counsel to make editorial and presentational changes to a compiled law in preparing a compilation of the law for registration. The changes must not change the effect of the law. Editorial changes take effect from the compilation registration date.

If the compilation includes editorial changes, the endnotes include a brief outline of the changes in general terms. Full details of any changes can be obtained from the Office of Parliamentary Counsel.

Misdescribed amendments

A misdescribed amendment is an amendment that does not accurately describe how an amendment is to be made. If, despite the misdescription, the amendment

Endnote 1—About the endnotes

can be given effect as intended, then the misdescribed amendment can be incorporated through an editorial change made under section 15V of the *Legislation Act 2003*.

If a misdescribed amendment cannot be given effect as intended, the amendment is not incorporated and “(md not incorp)” is added to the amendment history.

Endnotes

Endnote 2—Abbreviation key

Endnote 2—Abbreviation key

ad = added or inserted	o = order(s)
am = amended	Ord = Ordinance
amdt = amendment	orig = original
c = clause(s)	par = paragraph(s)/subparagraph(s) /sub-subparagraph(s)
C[x] = Compilation No. x	pres = present
Ch = Chapter(s)	prev = previous (prev...) = previously
def = definition(s)	Pt = Part(s)
Dict = Dictionary	r = regulation(s)/rule(s)
disallowed = disallowed by Parliament	reloc = relocated
Div = Division(s)	renum = renumbered
ed = editorial change	rep = repealed
exp = expires/expired or ceases/ceased to have effect	rs = repealed and substituted
F = Federal Register of Legislation	s = section(s)/subsection(s)
gaz = gazette	Sch = Schedule(s)
LA = <i>Legislation Act 2003</i>	Sdiv = Subdivision(s)
LIA = <i>Legislative Instruments Act 2003</i>	SLI = Select Legislative Instrument
(md) = misdescribed amendment can be given effect	SR = Statutory Rules
(md not incorp) = misdescribed amendment cannot be given effect	Sub-Ch = Sub-Chapter(s)
mod = modified/modification	SubPt = Subpart(s)
No. = Number(s)	<u>underlining</u> = whole or part not commenced or to be commenced

Endnote 3—Legislation history

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Australian Security Intelligence Organization Act 1979	113, 1979	25 Oct 1979	1 June 1980 (<i>Gazette</i> 1980, No. G21, p. 2)	
Australian Security Intelligence Organization Amendment Act 1979	182, 1979	4 Dec 1979	1 June 1980 (s 2)	—
Statute Law (Miscellaneous Provisions) Act (No. 1) 1985	65, 1985	5 June 1985	s 3: 3 July 1985	—
Australian Security Intelligence Organization Amendment Act 1986	122, 1986	2 Dec 1986	s 33–37: never commenced (s 2) Remainder: 1 Feb 1987 (<i>Gazette</i> 1987, No. S13)	—
as amended by				
Australian Security Intelligence Organization Amendment Act 1988	137, 1988	26 Dec 1988	26 Dec 1988	—
Law and Justice Legislation Amendment Act 1990	115, 1990	21 Dec 1990	(115, 1990 below)	—

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception) Amendment Act 1987	89, 1987	5 June 1987	s 1 and 2: 5 June 1987 s 5(1)(a), (2), 6 and 8: 16 Dec 1987 (s. 2(1A)) Remainder: 1 Sept 1988 (<i>Gazette</i> 1988, No. S256)	—
as amended by				
Crimes Legislation Amendment Act 1987	120, 1987	16 Dec 1987	s 53 and 54: 16 Dec 1987	—
Statute Law (Miscellaneous Provisions) Act 1987	141, 1987	18 Dec 1987	s 3: 18 Dec 1987	s 5(1)
Telecommunications Amendment Act 1988	121, 1988	14 Dec 1988	s 5, 6, 10, 12, 13, 23(2) and 26(1): 1 Jan 1989 (<i>Gazette</i> 1988, No. S402) s 14, 23(3) and 26(2): 30 June 1989 (<i>Gazette</i> 1989, No. S216) Remainder: 14 Dec 1988	—
Postal Services Amendment Act 1988	126, 1988	14 Dec 1988	s 4, 5, 9–11, 21(2) and 22(1): 1 Jan 1989 (<i>Gazette</i> 1988, No. S402) s 12, 21(3) and 22(2): 30 June 1989 (<i>Gazette</i> 1989, No. S216) Remainder: 14 Dec 1988	—
as amended by				
Telecommunications and Postal Services (Transitional Provisions and Consequential Amendments) Act 1989	63, 1989	19 June 1989	(63, 1989 below)	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Australian Security Intelligence Organization Amendment Act 1988	137, 1988	26 Dec 1988	26 Dec 1988	—
Telecommunications and Postal Services (Transitional Provisions and Consequential Amendments) Act 1989	63, 1989	19 June 1989	s 1 and 2: 19 June 1989 Pt 5 (s 17, 18): 30 June 1989 (s 2(3)) Remainder: 1 July 1989 (<i>Gazette</i> 1989, No. S230)	s 2(4)
as amended by Transport and Communications Legislation Amendment Act 1991	11, 1991	21 Jan 1991	s 45: 1 July 1989 (s 2(13)(e))	—
Courts and Tribunal Administration Amendment Act 1989	157, 1989	5 Dec 1989	Pt 1 and 6 (s 1, 2, 17, 18): 5 Dec 1989 Remainder: 1 Jan 1990 (<i>Gazette</i> 1989, No. S398)	s 2(3)
Migration Legislation Amendment (Consequential Amendments) Act 1989	159, 1989	18 Dec 1989	s 4: 19 Dec 1989 (s 2(2)) Remainder: 19 Dec 1989 (s 2(1))	—
Law and Justice Legislation Amendment Act 1989	11, 1990	17 Jan 1990	Pt 3 (s 6, 7): 22 Oct 1990	—
Defence Legislation Amendment Act 1990	75, 1990	22 Oct 1990	s 5: 22 Oct 1990	—
Law and Justice Legislation Amendment Act 1990	115, 1990	21 Dec 1990	s 1, 2 and 40–49: 21 Dec 1990 s 3, 5, 6, 8, 9, 16, 17, 20–23, 28, 30, 32, 33, 38 and 39: 4 Feb 1991 (<i>Gazette</i> 1991, No. GN3) Remainder: 21 June 1991	—

Australian Security Intelligence Organisation Act 1979

301

Compilation No. 80

Compilation date: 04/04/2025

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Industrial Relations Legislation Amendment Act 1991	122, 1991	27 June 1991	s 4(1), 10(b) and 15–20: 1 Dec 1988 s 28(b)–(e), 30 and 31: 10 Dec 1991 (<i>Gazette</i> 1991, No. S332) Remainder: 27 June 1991	s 31(2)
Law and Justice Legislation Amendment Act 1991	136, 1991	12 Sept 1991	s 4–9: 10 Oct 1991	—
Crimes (Aviation) Act 1991	139, 1991	27 Sept 1991	16 Mar 1992 (<i>Gazette</i> 1992, No. S65)	—
as amended by Crimes and Other Legislation Amendment Act 1994	182, 1994	19 Dec 1994	s 31: 16 Mar 1992 (s 2(5))	—
Transport and Communications Legislation Amendment Act 1994	64, 1994	30 May 1994	30 May 1994	s 2(2)–(4)
Crimes and Other Legislation Amendment Act 1994	182, 1994	19 Dec 1994	s 3–7: 19 Dec 1994	s 4 and 6(2)
Law and Justice Legislation Amendment Act (No. 1) 1995	175, 1995	16 Dec 1995	16 Dec 1995	Sch 1 (item 60)
Statute Law Revision Act 1996	43, 1996	25 Oct 1996	Sch 4 (item 40): 25 Oct 1996	—
Public Employment (Consequential and Transitional) Amendment Act 1999	146, 1999	11 Nov 1999	Sch 1 (items 252–258): 5 Dec 1999 (s 2(1) and <i>Gazette</i> 1999, No. S584)	—

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Australian Security Intelligence Organisation Legislation Amendment Act 1999	161, 1999	10 Dec 1999	Sch 1, Sch 2 and Sch 3 (item 21): 10 Dec 1999 (s 2(1), (2))	Sch 1 (items 44, 45) and Sch 2 (item 14)
Telecommunications (Interception) Legislation Amendment Act 2000	63, 2000	22 June 2000	Sch 3 (item 1): 22 June 2000	—
Broadcasting Services Amendment (Digital Television and Datacasting) Act 2000	108, 2000	3 Aug 2000	Sch 3 (item 1): 1 Jan 2001 (<i>Gazette</i> 2000, No. GN50)	—
Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000	137, 2000	24 Nov 2000	Sch 2 (items 50, 418, 419): 24 May 2001 (s 2(3))	Sch 2 (items 418, 419)
Privacy Amendment (Private Sector) Act 2000	155, 2000	21 Dec 2000	Sch 3: 21 Dec 2000 Remainder: 21 Dec 2001	Sch 3 (item 2)
Law and Justice Legislation Amendment (Application of Criminal Code) Act 2001	24, 2001	6 Apr 2001	s 4(1), (2) and Sch 4: 24 May 2001 (s 2(1)(a))	s 4(1) and (2)
Intelligence Services (Consequential Provisions) Act 2001	153, 2001	1 Oct 2001	29 Oct 2001 (s 2)	s 4 and Sch 1 (items 7–9)
Abolition of Compulsory Age Retirement (Statutory Officeholders) Act 2001	159, 2001	1 Oct 2001	29 Oct 2001	Sch 1 (item 97)
Cybercrime Act 2001	161, 2001	1 Oct 2001	21 Dec 2001 (<i>Gazette</i> 2001, No. S529)	—

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Australian Crime Commission Establishment Act 2002	125, 2002	10 Dec 2002	Sch 2 (items 2–4): 1 Jan 2003	—
Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003	77, 2003	22 July 2003	Sch 1: (items 1–8, 15–27C): 23 July 2003 (s 2(1) item 2) Sch 1 (items 10, 11): 23 July 2003 (s 2(1) item 3)	Sch 1 (items 5, 11, 20, 27C)
ASIO Legislation Amendment Act 2003	143, 2003	17 Dec 2003	18 Dec 2003	Sch 1 (items 2, 4, 6, 11)
Communications Legislation Amendment Act (No. 1) 2004	35, 2004	20 Apr 2004	21 Apr 2004	—
Anti-terrorism Act (No. 3) 2004	125, 2004	16 Aug 2004	Sch 2: 13 Sept 2004	Sch 2 (item 2)
Australian Security Intelligence Organisation Amendment Act 2004	141, 2004	14 Dec 2004	14 Dec 2004	—
Australian Passports (Transitionals and Consequential) Act 2005	7, 2005	18 Feb 2005	Sch 1 (items 2–4): 1 July 2005 (s 2(1))	—
Telstra (Transition to Full Private Ownership) Act 2005	118, 2005	23 Sept 2005	s. 3: 23 Sept 2005 Sch 1 (items 43–46): 24 Nov 2006 (F2006L03997)	s. 3
Intelligence Services Legislation Amendment Act 2005	128, 2005	4 Nov 2005	Sch 4 (item 1) and Sch 8 (items 2, 15–19): 2 Dec 2005	—
Anti-Terrorism Act (No. 2) 2005	144, 2005	14 Dec 2005	Sch 10 (items 1–25): 14 Dec 2005 Sch 10 (items 26–28): 15 Dec 2005	Sch 10 (item 25)

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Sch 1 (items 13–15): 13 June 2006 (F2006L01623)	—
ASIO Legislation Amendment Act 2006	54, 2006	19 June 2006	Sch 1 (items 1–10, 16–21) and Sch 2 (items 1–32): 20 June 2006 (s 2(1) items 2, 3)	Sch 1 (items 16–21)
Law Enforcement (AFP Professional Standards and Related Measures) Act 2006	84, 2006	30 June 2006	Sch 3A (items 1–9): never commenced (s 2(1) item 3) Sch 3A (items 10–22): 30 Dec 2006 (s 2(1) items 2, 4)	—
Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006	86, 2006	30 June 2006	Sch 1 (items 6–10): 30 Dec 2006 (s 2(1))	—
Privacy Legislation Amendment (Emergencies and Disasters) Act 2006	148, 2006	6 Dec 2006	7 Dec 2006	—
Law and Justice Legislation Amendment (Marking of Plastic Explosives) Act 2007	3, 2007	19 Feb 2007	Sch 3 (item 2): 25 Aug 2007 (s 2(1) item 2)	—
Australian Citizenship (Transitionals and Consequentials) Act 2007	21, 2007	15 Mar 2007	Sch 1 (item 5): 1 July 2007 (s 2(1) item 2)	—
Anti-People Smuggling and Other Measures Act 2010	50, 2010	31 May 2010	Sch 2: 1 June 2010 (s 2)	—

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011	4, 2011	22 Mar 2011	Sch 6 (items 1–17, 29): 23 Mar 2011 (s 2)	Sch 6 (item 29)
Statute Law Revision Act 2011	5, 2011	22 Mar 2011	Sch 6 (items 10, 11): 19 Apr 2011 (s 2(1) item 15)	—
Acts Interpretation Amendment Act 2011	46, 2011	27 June 2011	Sch 2 (item 242) and Sch 3 (items 10, 11): 27 Dec 2011 (s 2(1) items 3, 12)	Sch 3 (items 10, 11)
Intelligence Services Legislation Amendment Act 2011	80, 2011	25 July 2011	Sch 1 (items 1–18, 29–31): 26 July 2011 (s 2)	Sch 1 (items 29–31)
Federal Circuit Court of Australia (Consequential Amendments) Act 2013	13, 2013	14 Mar 2013	Sch 1 (items 51–53): 12 Apr 2013 (s 2(1) item 2)	Sch 1 (item 53)
Statute Law Revision Act 2013	103, 2013	29 June 2013	Sch 1 (item 23): 29 June 2013 (s 2(1) item 2)	—
Telecommunications Legislation Amendment (Submarine Cable Protection) Act 2014	33, 2014	27 May 2014	Sch 1 (items 2, 3): 28 May 2014 (s 2(1) item 2)	—
Public Governance, Performance and Accountability (Consequential and Transitional Provisions) Act 2014	62, 2014	30 June 2014	Sch 7 (items 437–439) and Sch 14: 1 July 2014 (s 2(1) items 6, 14)	Sch 14

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
as amended by				
Public Governance and Resources Legislation Amendment Act (No. 1) 2015	36, 2015	13 Apr 2015	Sch 2 (items 7–9) and Sch 7: 14 Apr 2015 (s 2)	Sch 7
as amended by				
Acts and Instruments (Framework Reform) (Consequential Provisions) Act 2015	126, 2015	10 Sept 2015	Sch 1 (item 486): 5 Mar 2016 (s 2(1) item 2)	—
Acts and Instruments (Framework Reform) (Consequential Provisions) Act 2015	126, 2015	10 Sept 2015	Sch 1 (item 495): 5 Mar 2016 (s 2(1) item 2)	—
National Security Legislation Amendment Act (No. 1) 2014	108, 2014	2 Oct 2014	Sch 1 (items 1–30, 78–87), Sch 2 (items 1–45, 45A, 46, 46A, 46B, 47, 50), Sch 3, Sch 4 and Sch 6 (items 1–5A, 23): 30 Oct 2014 (s 2(1) item 2) Sch 7 (items 72–83, 144, 145): 3 Oct 2014 (s 2(1) item 3)	Sch 1 (items 78–87), Sch 2 (item 50), Sch 6 (item 23) and Sch 7 (items 144, 145)
Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014	116, 2014	3 Nov 2014	Sch 1 (items 27–34B): 1 Dec 2014 (s 2(1) item 2) Sch 4 (items 6, 7): 4 Nov 2014 (s 2(1) item 3)	Sch 1 (items 29, 31, 34B)
Statute Law Revision Act (No. 1) 2015	5, 2015	25 Feb 2015	Sch 3 (item 42): 25 Mar 2015 (s 2(1) item 10)	—

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015	39, 2015	13 Apr 2015	Sch 1 (items 1A–1D, 7): 13 Oct 2015 (s 2(1) item 2) Sch 1 (items 8–12): 13 Apr 2015 (s 2(1) items 1, 3)	Sch 1 (items 7–12)
Passports Legislation Amendment (Integrity) Act 2015	122, 2015	10 Sept 2015	Sch 1 (items 79–92): 8 Oct 2015 (s 2(1) item 2)	—
Acts and Instruments (Framework Reform) (Consequential Provisions) Act 2015	126, 2015	10 Sept 2015	Sch 1 (items 59, 60): 5 Mar 2016 (s 2(1) item 2)	—
Counter-Terrorism Legislation Amendment Act (No. 1) 2016	82, 2016	29 Nov 2016	Sch 12 (items 1–9) and Sch 18: 30 Nov 2016 (s 2(1) items 2, 5)	Sch 12 (item 9)
Telecommunications and Other Legislation Amendment Act 2017	111, 2017	18 Sept 2017	Sch 1 (items 33–35): 18 Sept 2018 (s 2(1) item 2)	Sch 1 (item 35)
as amended by Home Affairs and Integrity Agencies Legislation Amendment Act 2018	31, 2018	9 May 2018	Sch 2 (item 283): 18 Sept 2018 (s 2(1) item 6) Sch 2 (item 284): 11 May 2018 (s 2(1) item 7)	Sch 2 (item 284)
Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018	25, 2018	11 Apr 2018	Sch 1 (items 47–52, 100–108): 1 July 2018 (s 2(1) item 2)	Sch 1 (items 100–108)

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Security of Critical Infrastructure (Consequential and Transitional Provisions) Act 2018	30, 2018	11 Apr 2018	Sch 1 (items 1–1B): 11 July 2018 (s 2(1) item 2)	—
Home Affairs and Integrity Agencies Legislation Amendment Act 2018	31, 2018	9 May 2018	Sch 2 (items 50–71, 284): 11 May 2018 (s 2(1) items 3, 7)	Sch 2 (item 284)
Counter-Terrorism Legislation Amendment Act (No. 1) 2018	74, 2018	24 Aug 2018	Sch 1 (item 18): 25 Aug 2018 (s 2(1) item 1)	—
Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018	148, 2018	8 Dec 2018	Sch 1 (item 1A), Sch 2 (items 1–18, 132) and Sch 5: 9 Dec 2018 (s 2(1) items 2, 4, 6)	Sch 2 (item 132)
Office of National Intelligence (Consequential and Transitional Provisions) Act 2018	156, 2018	10 Dec 2018	Sch 2 (items 22–25) and Sch 4: 20 Dec 2018 (s 2(1) items 2, 4)	Sch 4
Australian Security Intelligence Organisation Amendment (Sunsetting of Special Powers Relating to Terrorism Offences) Act 2019	61, 2019	12 Aug 2019	13 Aug 2019 (s 2(1) item 1)	—

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Australian Security Intelligence Organisation Amendment Act 2020	134, 2020	17 Dec 2020	Sch 1 (items 1–18) and Sch 2: 7 Sept 2020 (s 2(1) items 2, 5) Sch 1 (items 27, 28): never commenced (s 2(1) item 3) Sch 1 (item 29): 1 Sept 2021 (s 2(1) item 4) Note: This amending title was affected by an editorial change (see C2021C00363)	Sch 1 (items 13–18)
Federal Circuit and Family Court of Australia (Consequential Amendments and Transitional Provisions) Act 2021	13, 2021	1 Mar 2021	Sch 2 (items 118, 119): 1 Sept 2021 (s 2(1) item 5)	—
Telecommunications Legislation Amendment (International Production Orders) Act 2021	78, 2021	23 July 2021	Sch 1 (items 3, 4): 24 July 2021 (s 2(1) item 2)	—
Foreign Intelligence Legislation Amendment Act 2021	95, 2021	2 Sept 2021	Sch 2 (items 1, 2, 9): 21 Dec 2021 (s 2(1) item 1)	Sch 2 (item 9)
Counter-Terrorism Legislation Amendment (High Risk Terrorist Offenders) Act 2021	131, 2021	8 Dec 2021	Sch 1 (item 154): 9 Dec 2021 (s 2(1) item 2)	—
Data Availability and Transparency (Consequential Amendments) Act 2022	12, 2022	31 Mar 2022	Sch 1 (items 2, 3), Sch 2 and 3: 1 Apr 2022 (s 2(1) item 1)	Sch 2 and 3

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Act 2022	31, 2022	1 Apr 2022	Sch 13 (items 1, 2, 6): 2 Apr 2022 (s 2(1) item 8)	Sch 13 (item 6)
Australian Security Intelligence Organisation Amendment Act 2023	33, 2023	28 June 2023	Sch 1 (items 1–13): 1 July 2023 (s 2(1) item 1)	Sch 1 (item 13)
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Act 2023	53, 2023	11 Aug 2023	Sch 1 (item 2): 12 Aug 2023 (s 2(1) item 1)	—
Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Act 2023	73, 2023	20 Sept 2023	Sch 1 (items 169–175) and Sch 3 (item 2): 21 Sept 2023 (s 2(1) items 2, 5)	Sch 3 (item 2)
Statute Law Amendment (Prescribed Forms and Other Updates) Act 2023	74, 2023	20 Sept 2023	Sch 1 (items 7–9): 20 Mar 2024 (s 2(1) item 2)	Sch 1 (item 9)
Counter-Terrorism and Other Legislation Amendment Act 2023	96, 2023	24 Nov 2023	Sch 2 (items 59, 60): 25 Nov 2023 (s 2(1) item 1)	—
Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023	110, 2023	7 Dec 2023	Sch 2 (item 2): 8 Dec 2023 (s 2(1) item 1)	—

Endnotes

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Act 2024	24, 2024	21 May 2024	Sch 1 (items 1–25), Sch 2 (items 1, 2, 39, 40), Sch 3 (items 17, 20–26) and Sch 4 (items 1–4): 22 May 2024 (s 2(1) items 2–5, 7, 8) Sch 1 (items 26–28) and Sch 4 (items 5–7): 21 Nov 2024 (s 2(1) items 6, 9)	Sch 1 (items 5, 12, 22, 25), Sch 2 (item 40), Sch 3 (item 26) and Sch 4 (item 4)
Digital ID (Transitional and Consequential Provisions) Act 2024	26, 2024	30 May 2024	Sch 2 (items 3, 4): 30 Nov 2024 (s 2(1) item 1)	—
Administrative Review Tribunal (Consequential and Transitional Provisions No. 1) Act 2024	38, 2024	31 May 2024	Sch 4 (items 34–47): 14 Oct 2024 (s 2(1) item 2)	—
Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024	100, 2024	29 Nov 2024	Sch 5 (items 29, 30, 67): 4 Apr 2025 (s 2(1) items 3, 7) Sch 7: 30 Nov 2024 (s 2(1) item 9)	Sch 5 (item 67) and Sch 7 (items 4, 5)
Crown References Amendment Act 2024	115, 2024	10 Dec 2024	Sch 1 (items 6, 7): 11 Dec 2024 (s 2(1) item 1)	—

Endnote 3—Legislation history

Name	Registration	Commencement	Application, saving and transitional provisions
Coronavirus Economic Response Package (Deferral of Sunsetting—ASIO Special Powers Relating to Terrorism Offences) Determination 2020	4 Sept 2020 (F2020L01134)	5 Sept 2020	—

Endnotes

Endnote 4—Amendment history

Endnote 4—Amendment history

Provision affected	How affected
Title.....	am No 161, 1999
Part I	
s 1.....	am No 161, 1999
s 3.....	am No 161, 1999
s 4.....	am No 122, 1986; No 159, 1989; No 75, 1990; No 136, 1991; No 139, 1991 (as am by No 182, 1994); No 182, 1994; No 146, 1999; No 161, 1999; No 153, 2001; No 77, 2003; No 118, 2005; No 128, 2005; No 144, 2005; No 3, 2007; No 50, 2010; No 4, 2011; No 5, 2011; No 80, 2011; No 108, 2014; No 116, 2014; No 39, 2015; No 122, 2015; No 82, 2016; No 25, 2018; No 148, 2018; No 156, 2018; No 134, 2020; No 33, 2023; No 73, 2023; No 24, 2024
s 4AA.....	ad No 24, 2024
s 4A.....	ad No 24, 2001
s 5.....	rs No 122, 1986
s 5A.....	ad No 122, 1986
s 5B.....	ad No 53, 2023
Part II	
Part II heading	am No 161, 1999
s 6.....	am No 161, 1999
s 8.....	am No 122, 1986; No 161, 1999
s 8A.....	ad No 122, 1986 am No 137, 1988; No 161, 1999; No 153, 2001; No 128, 2005; No 108, 2014; No 31, 2018
s 9.....	am No 141, 1987; No 159, 2001
s 10.....	am No 141, 1987; No 43, 1996
s 11.....	rs No 122, 1991 am No 146, 1999
s 12.....	am No 141, 1987
s 13.....	am No 141, 1987; No 122, 1991
s 14.....	am No 141, 1987; No 161, 1999

Endnote 4—Amendment history

Provision affected	How affected
s 15.....	am No 141, 1987
s 16.....	rep No 65, 1985
	ad No 122, 1986
	am No 161, 1999
	rs No 108, 2014
	am No 148, 2018; No 33, 2023; No 24, 2024
Part III	
Part III heading.....	am No 161, 1999
Division 1	
s 17.....	am No 122, 1986; No 161, 1999; No 63, 2000; No 40, 2006; No 4, 2011; No 33, 2023; No 24, 2024
s 17AA.....	ad No 161, 1999
s 17A.....	ad No 122, 1986
	am No 161, 1999
s 18.....	am No 182, 1979; No 122, 1986; No 141, 1987; No 161, 1999; No 125, 2002; No 77, 2003; No 86, 2006; No 148, 2006; No 4, 2011; No 108, 2014; No 78, 2021; No 73, 2023
s 18A.....	ad No 108, 2014
	am No 82, 2016; No 73, 2023
s 18B.....	ad No 108, 2014
	am No 82, 2016; No 73, 2023
s 18C.....	ad No 108, 2014
	am No 31, 2018
s 18D.....	ad No 108, 2014
s 19.....	am No 122, 1986; No 161, 1999; No 4, 2011; No 108, 2014
s 19A.....	ad No 4, 2011
	am No 108, 2014; No 156, 2018
s 20.....	am No 161, 1999
s 21.....	am No 141, 1987
s 21A.....	ad No 148, 2018

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Division 2	
Subdivision A	
Subdivision A heading.....	ad No 108, 2014
s 22.....	am No 122, 1986; No 161, 1999; No 108, 2014; No 134, 2020
s 23.....	rep No 77, 2003
	ad No 144, 2005
	am No 108, 2014
s 24.....	am No 141, 1987
	rs No 182, 1994
	am No 146, 1999; No 161, 1999; No 77, 2003; No 54, 2006
	rs No 108, 2014
	am No 148, 2018; No 31, 2022
Subdivision B	
Subdivision B heading.....	ad No 108, 2014
s 25.....	am No 122, 1986; No 141, 1987
	rs No 161, 1999
	am No 77, 2003; No 144, 2005; No 108, 2014; No 31, 2018
s 25AA.....	ad No 77, 2003
Subdivision C	
Subdivision C heading.....	ad No 108, 2014
s 25A.....	ad No 161, 1999
	am No 161, 2001; No 144, 2005; No 54, 2006; No 80, 2011; No 108, 2014; No 31, 2018; No 148, 2018; No 134, 2020
Subdivision D	
Subdivision D heading.....	ad No 108, 2014
s 26.....	am No 122, 1986; No 89, 1987; No 141, 1987; No 121, 1988; No 64, 1994; No 161, 1999; No 118, 2005; No 40, 2006
	rs No 108, 2014
	am No 31, 2018
s 26A.....	ad No 161, 1999
	rs No 108, 2014

Endnote 4—Amendment history

Provision affected	How affected
	am No 31, 2018
s 26B	ad No 161, 1999
	rs No 108, 2014
s 26C	ad No 161, 1999
	rs No 108, 2014
s 26D	ad No 108, 2014
s 26E	ad No 108, 2014
	am No 134, 2020
s 26F	ad No 108, 2014
Subdivision DA	
Subdivision DA	ad No 134, 2020
s 26G	ad No 134, 2020
s 26H	ad No 134, 2020
s 26J	ad No 134, 2020
s 26K	ad No 134, 2020
s 26L	ad No 134, 2020
s 26M	ad No 134, 2020
s 26N	ad No 134, 2020
s 26P	ad No 134, 2020
s 26Q	ad No 134, 2020
s 26R	ad No 134, 2020
Subdivision E	
Subdivision E heading	ad No 108, 2014
s 27	am No 122, 1986; No 141, 1987; No 126, 1988 (as am by No 63, 1989); No 63, 1989 (as am by No 11, 1991); No 136, 1991; No 161, 1999; No 144, 2005; No 108, 2014; No 31, 2018
s 27AA	ad No 161, 1999
	am No 144, 2005; No 108, 2014; No 31, 2018
Subdivision F	
Subdivision F heading	ad No 108, 2014
s 27A	ad No 122, 1986

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 121, 1988; No 126, 1988; No 63, 1989 (as am by No 11, 1991); No 136, 1991; No 64, 1994; No 161, 1999; No 118, 2005; No 144, 2005; No 40, 2006; No 80, 2011; No 108, 2014; No 31, 2018; No 148, 2018; No 95, 2021
s 27B.....	ad No 161, 1999 am No 80, 2011; No 31, 2018
Subdivision G	
Subdivision G.....	ad No 108, 2014
s 27C.....	ad No 108, 2014 am No 31, 2018
s 27D.....	ad No 108, 2014 am No 31, 2018
s 27E.....	ad No 108, 2014 am No 31, 2018; No 148, 2018
s 27F.....	ad No 108, 2014 am No 31, 2018
s 27G.....	ad No 108, 2014 am No 31, 2018
s 27H.....	ad No 108, 2014 am No 31, 2018
s 27J.....	ad No 108, 2014 am No 31, 2018
Subdivision H	
Subdivision H heading.....	ad No 108, 2014 am No 134, 2020
s 29.....	am No 141, 1987; No 161, 1999; No 128, 2005; No 108, 2014; No 31, 2018; No 134, 2020
s 29A.....	ad No 108, 2014 am No 31, 2018; No 134, 2020
s 30.....	am No 141, 1987; No 161, 1999 rs No 108, 2014 am No 31, 2018; No 134, 2020

Endnote 4—Amendment history

Provision affected	How affected
s 31.....	rs No 122, 1986 am No 161, 1999
s 31A.....	ad No 108, 2014 am No 31, 2018
s 32.....	am No 141, 1987; No 161, 1999; No 31, 2018
s 33.....	am No 161, 1999 rep No 137, 2000 ad No 108, 2014 am No 148, 2018; No 134, 2020
s 34.....	am No 122, 1986; No 161, 1999; No 108, 2014; No 31, 2018; No 148, 2018; No 134, 2020
s 34A (first occurring)	ad No 148, 2018 renum No 134, 2020
s 34AAA (prev s 34A (first occurring))	
s 34AAB	ad No 134, 2020
s 34AA.....	ad No 108, 2014 am No 148, 2018 renum No 134, 2020
s 34AAC (prev s 34AA).....	am No 134, 2020
Subdivision J	
Subdivision J.....	ad No 148, 2018
s 34AAA	ad No 148, 2018 renum No 134, 2020
s 34AAD (prev s 34AAA).....	am No 134, 2020
Division 3	
Division 3	ad No 77, 2003 rs No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
Subdivision A	
s 34A.....	ad No 77, 2003

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 54, 2006; No 13, 2013
	rs No 134, 2020
	am No 13, 2021
	exp 7 Sept 2025 (s 34JF)
s 34AA	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34AB	ad No 77, 2003
	am No 13, 2013; No 31, 2018
	rs No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34AC	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34AD	ad No 134, 2020
	am No 38, 2024; No 115, 2024
	exp 7 Sept 2025 (s 34JF)
s 34AE	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34AF	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34AG	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
Subdivision B	
Subdivision B	rs No 54, 2006; No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34B	ad No 77, 2003
	am No 31, 2018
	rs No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34BA	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34BB	ad No 134, 2020

Endnote 4—Amendment history

Provision affected	How affected
	exp 7 Sept 2025 (s 34JF)
s 34BC	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34BD	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34BE.....	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34BF	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34BG	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34BH	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
Subdivision C	
Subdivision C	rs No 54, 2006; No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34C	ad No 77, 2003
	am No 128, 2005
	rs No 54, 2006
	am No 126, 2015; No 31, 2018
	rs No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34CA	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34CB	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34CC	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34CD	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34CE.....	ad No 134, 2020

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	exp 7 Sept 2025 (s 34JF)
Subdivision D	
Subdivision D heading.....	ad No 54, 2006 rs No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34D.....	ad No 77, 2003 rs No 54, 2006 am No 54, 2006; No 116, 2014; No 31, 2018 rs No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DA.....	ad No 77, 2003 rep No 54, 2006 ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DB.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DC.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DD.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DE.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DF.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DG.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DH.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DI.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34DJ.....	ad No 134, 2020

Endnote 4—Amendment history

Provision affected	How affected
	exp 7 Sept 2025 (s 34JF)
s 34DK	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34DL	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34DM	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34DN	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34DO	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34DP	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
Subdivision E	
Subdivision E heading	ad No 54, 2006
	rs No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34E	ad No 77, 2003
	rs No 54, 2006
	am No 54, 2006
	rs No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34EA	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34EB	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34EC	ad No 134, 2020
	am No 134, 2020
	exp 7 Sept 2025 (s 34JF)
s 34ED	ad No 134, 2020
	exp 7 Sept 2025 (s 34JF)

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 34EE.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34EF.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
Subdivision F	
s 34F.....	ad No 77, 2003 am No 143, 2003 rs No 54, 2006 am No 31, 2018 rs No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FA.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FB.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FC.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FD.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FE.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FF.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FG.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FH.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
s 34FI.....	ad No 134, 2020 exp <u>7 Sept 2025 (s 34JF)</u>
Subdivision G	
s 34G.....	ad No 77, 2003

Endnote 4—Amendment history

Provision affected	How affected
	am No 144, 2005
	rs No 54, 2006
	am No 54, 2006; No 84, 2006; No 46, 2011; No 31, 2018
	rs No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34GA	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34GB	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34GC	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34GD	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34GE	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34GF	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
Subdivision H	
s 34H	ad No 77, 2003
	rs No 54, 2006; No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34HAA	ad No 77, 2003
	rep No 54, 2006
s 34HAB	ad No 77, 2003
	rep No 54, 2006
s 34HA	ad No 77, 2003
	rep No 54, 2006
	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34HB	ad No 77, 2003
	am No 143, 2003

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	rep No 54, 2006
	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34HC	ad No 77, 2003
	rep No 54, 2006
	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
Subdivision I	
s 34J	ad No 77, 2003
	rs No 54, 2006
	am No 54, 2006; No 84, 2006
	rs No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34JA	ad No 77, 2003
	rep No 54, 2006
	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34JB	ad No 77, 2003
	rep No 54, 2006
	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>
s 34JBA.....	ad No 125, 2004
	am No 7, 2005
	rep No 54, 2006
s 34JBB.....	ad No 125, 2004
	rep No 54, 2006
s 34JC	ad No 143, 2003
	am No 7, 2005
	rep No 54, 2006
	ad No 134, 2020
	exp <u>7 Sept 2025 (s 34JF)</u>

Endnote 4—Amendment history

Provision affected	How affected
s 34JD	ad No 143, 2003 rep No 54, 2006 ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34JE.....	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34JF	ad No 134, 2020 exp 7 Sept 2025 (s 34JF)
s 34K.....	ad No 77, 2003 rs No 54, 2006 am No 54, 2006; No 84, 2006; No 31, 2018 rep No 134, 2020
s 34L	ad No 77, 2003 rs No 54, 2006 am No 116, 2014 rep No 134, 2020
s 34M.....	ad No 77, 2003 rs No 54, 2006 rep No 134, 2020
s 34N.....	ad No 77, 2003 am No 144, 2005 rs No 54, 2006 rep No 134, 2020
s 34NA.....	ad No 77, 2003 rep No 54, 2006
s 34NB.....	ad No 77, 2003 rep No 54, 2006
s 34NC	ad No 77, 2003 rep No 54, 2006
s 34P	ad No 77, 2003 rs No 54, 2006

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	rep No 134, 2020
s 34Q.....	ad No 77, 2003
	rs No 54, 2006
	am No 54, 2006
	rep No 134, 2020
s 34QA.....	ad No 77, 2003
	rep No 54, 2006
s 34R.....	ad No 77, 2003
	rs No 54, 2006
	am No 54, 2006; No 84, 2006
	rep No 134, 2020
s 34S.....	ad No 77, 2003
	rs No 54, 2006
	rep No 134, 2020
s 34SA.....	ad No 77, 2003
	rep No 54, 2006
s 34T.....	ad No 77, 2003
	rs No 54, 2006
	rep No 134, 2020
s 34TA.....	ad No 77, 2003
	rep No 54, 2006
s 34TB.....	ad No 77, 2003
	rep No 54, 2006
s 34U.....	ad No 77, 2003
	am No 143, 2003
	rs No 54, 2006
	rep No 134, 2020
s 34V.....	ad No 77, 2003
	am No 143, 2003
	rs No 54, 2006
	am No 116, 2014

Endnote 4—Amendment history

Provision affected	How affected
	rep No 134, 2020
s 34VAA	ad No 143, 2003
	rep No 54, 2006
s 34VA	ad No 77, 2003
	rep No 54, 2006
s 34W	ad No 77, 2003
	rs No 54, 2006
	am No 122, 2015; No 31, 2018
	rep No 134, 2020
s 34WA	ad No 77, 2003
	rep No 54, 2006
s 34X	ad No 77, 2003
	rs No 54, 2006
	am No 31, 2018
	rep No 134, 2020
s 34Y	ad No 77, 2003
	rs No 54, 2006
	am No 122, 2015
	rep No 134, 2020
s 34Z	ad No 54, 2006
	rep No 134, 2020
s 34ZA	ad No 54, 2006
	rep No 134, 2020
s 34ZB	ad No 54, 2006
	rep No 134, 2020
s 34ZC	ad No 54, 2006
	am No 108, 2014
	rep No 134, 2020
s 34ZD	ad No 54, 2006
	rep No 134, 2020
s 34ZE	ad No 54, 2006

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	am No 54, 2006; No 108, 2014; No 31, 2018
	rep No 134, 2020
s 34ZF	ad No 54, 2006
	am No 54, 2006; No 84, 2006; No 108, 2014
	rep No 134, 2020
s 34ZG	ad No 54, 2006
	rs No 84, 2006
	rep No 134, 2020
s 34ZH	ad No 54, 2006
	am No 31, 2018; No 148, 2018
	rep No 134, 2020
s 34ZI	ad No 54, 2006
	am No 31, 2018
	rep No 134, 2020
s 34ZJ	ad No 54, 2006
	am No 62, 2014; No 31, 2018
	rep No 134, 2020
s 34ZK	ad No 54, 2006
	am No 31, 2018
	rep No 134, 2020
s 34ZL	ad No 54, 2006
	rep No 134, 2020
s 34ZM	ad No 54, 2006
	rep No 134, 2020
s 34ZN	ad No 54, 2006
	am No 84, 2006
	rep No 134, 2020
s 34ZO	ad No 54, 2006
	am No 54, 2006
	rep No 134, 2020
s 34ZP	ad No 54, 2006

Endnote 4—Amendment history

Provision affected	How affected
	rep No 134, 2020
s 34ZQ	ad No 54, 2006 am No 54, 2006
	rep No 134, 2020
s 34ZR	ad No 54, 2006
	rep No 134, 2020
s 34ZS	ad No 54, 2006 am No 54, 2006; No 84, 2006; No 31, 2018
	rep No 134, 2020
s 34ZT	ad No 54, 2006
	rep No 134, 2020
s 34ZU	ad No 54, 2006 am No 103, 2013
	rep No 134, 2020
s 34ZV	ad No 54, 2006
	rep No 134, 2020
s 34ZW	ad No 54, 2006
	rep No 134, 2020
s 34ZX	ad No 54, 2006 am No 84, 2006; No 31, 2018
	rep No 134, 2020
s 34ZY	ad No 54, 2006 am No 31, 2018
	rep No 134, 2020
s 34ZZ	ad No 54, 2006 am No 54, 2006; No 116, 2014; No 74, 2018; No 61, 2019
	rep No 134, 2020
Division 4	
Division 4	ad No 108, 2014
s 35A	ad No 108, 2014

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 35B	ad No 108, 2014 am No 31, 2018; No 24, 2024
s 35C	ad No 108, 2014 am No 31, 2018
s 35D.....	ad No 108, 2014
s 35E	ad No 108, 2014
s 35F	ad No 108, 2014 am No 31, 2018; No 24, 2024
s 35G.....	ad No 108, 2014
s 35H.....	ad No 108, 2014
s 35J	ad No 108, 2014
s 35K.....	ad No 108, 2014 am No 31, 2018
s 35L	ad No 108, 2014
s 35M.....	ad No 108, 2014
s 35N.....	ad No 108, 2014
s 35P	ad No 108, 2014 am No 82, 2016; No 73, 2023
s 35PA.....	ad No 108, 2014
s 35Q.....	ad No 108, 2014 am No 31, 2018
s 35R	ad No 108, 2014 am No 31, 2018
Part IV	
Division 1	
s 35.....	am No 122, 1986; No 175, 1995; No 161, 1999; No 77, 2003; No 35, 2004; No 141, 2004; No 7, 2005; No 144, 2005; No 21, 2007; No 80, 2011; No 33, 2014; No 108, 2014; No 82, 2016; No 111, 2017; No 25, 2018; No 30, 2018; No 156, 2018; No 131, 2021; No 12, 2022; No 33, 2023; No 96, 2023; No 110, 2023; No 24, 2024; No 26, 2024; No 38, 2024; No 100, 2024
s 36AA.....	ad No 24, 2024

Endnote 4—Amendment history

Provision affected	How affected
s 36.....	am No 122, 1986; No 159, 1989; No 136, 1991; No 175, 1995; No 161, 1999; No 141, 2004; No 80, 2011; No 116, 2014; No 24, 2024; No 26, 2024
s 36A.....	ad No 33, 2023
Division 2	
s 37.....	am No 175, 1995; No 161, 1999
s 38.....	am No 141, 1987; No 161, 1999; No 35, 2004; No 116, 2014; No 82, 2016; No 31, 2018; No 74, 2023; No 100, 2024
s 38A.....	ad No 35, 2004 am No 33, 2014; No 111, 2017; No 30, 2018; No 31, 2018; No 74, 2023 rep No 100, 2024
s 39.....	am No 161, 1999; No 141, 2004; No 24, 2024
s 40.....	am No 161, 1999; No 77, 2003; No 82, 2016; No 24, 2024
s 41.....	rep No 175, 1995 ad No 24, 2024
s 42.....	am No 141, 1987 rep No 175, 1995 ad No 24, 2024
Division 3	rep No 175, 1995
s 43.....	am No 141, 1987 rep No 175, 1995
s 44.....	rep No 175, 1995
s 45.....	am No 141, 1987 rep No 175, 1995
s 46.....	am No 141, 1987 rep No 175, 1995
s 47.....	am No 141, 1987 rep No 175, 1995
s 48.....	am No 141, 1987 rep No 175, 1995
s 49.....	am No 141, 1987

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
	rep No 175, 1995
s 50.....	am No 141, 1987
	rep No 175, 1995
s 51.....	rep No 175, 1995
s 52.....	am No 141, 1987
	rep No 175, 1995
s 53.....	rep No 175, 1995
Division 4	
s 54.....	am No 122, 1986; No 141, 1987
	rs No 175, 1995
	am No 38, 2024; No 100, 2024
s 55.....	rep No 175, 1995
s 56.....	am No 122, 1986
	rep No 175, 1995
s 57.....	rep No 175, 1995
s 58.....	am No 141, 1987
	rep No 175, 1995
s 59.....	am No 141, 1987
	rep No 175, 1995
s 60.....	am No 65, 1985; No 122, 1986; No 141, 1987
	rep No 175, 1995
s 60A.....	ad No 122, 1986
	rep No 175, 1995
s 61.....	am No 122, 1986; No 141, 2004; No 82, 2016
s 62.....	rep No 175, 1995
s 63.....	am No 122, 1986; No 141, 1987; No 136, 1991
	rep No 175, 1995
s 64.....	am No 161, 1999
s 65.....	am No 122, 1986; No 141, 1987; No 175, 1995; No 161, 1999; No 82, 2016; No 31, 2018; No 38, 2024
Division 5	rep No 175, 1995

Endnote 4—Amendment history

Provision affected	How affected
s 66.....	rep No 175, 1995
s 67.....	rep No 175, 1995
s 68.....	rep No 175, 1995
s 69.....	am No 141, 1987 rep No 175, 1995
s 70.....	am No 141, 1987 rep No 175, 1995
s 71.....	rep No 175, 1995
Division 6 heading.....	rep No 175, 1995
s 72.....	am No 141, 1987 rep No 175, 1995
s 72A.....	ad No 122, 1986 rep No 175, 1995
s 73.....	am No 141, 1987 rep No 175, 1995
s 74.....	am No 122, 1986; No 141, 1987 rep No 175, 1995
s 75.....	am No 122, 1986; No 141, 1987 rep No 175, 1995
s 76.....	am No 122, 1986; No 141, 1987 rep No 175, 1995
s 77.....	am No 141, 1987 rep No 175, 1995
s 78.....	am No 157, 1989 rep No 175, 1995
s 79.....	rep No 175, 1995
s 80.....	rep No 175, 1995
s 81.....	am No 122, 1986; No 141, 1987; No 161, 1999; No 33, 2023; No 38, 2024
s 82.....	rep No 175, 1995
s 83.....	rep No 175, 1995

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
Part IVA	
Part IVA.....	ad No 33, 2023
Division 1	
s 82.....	ad No 33, 2023
s 82A.....	ad No 33, 2023
	am No 24, 2024
s 82B.....	ad No 33, 2023
	am No 24, 2024; No 38, 2024
Division 2	
s 82C.....	ad No 33, 2023
	am No 38, 2024
s 82D.....	ad No 33, 2023
s 82E.....	ad No 33, 2023
s 82F.....	ad No 33, 2023
s 82G.....	ad No 33, 2023
s 82GA.....	ad No 24, 2024
s 82GB.....	ad No 24, 2024
Division 3	
Subdivision A	
s 82H.....	ad No 33, 2023
s 82J.....	ad No 33, 2023
s 82K.....	ad No 33, 2023
s 82L.....	ad No 33, 2023
	am No 38, 2024
Subdivision B	
Subdivision B heading.....	am No 38, 2024
s 83.....	ad No 33, 2023
s 83A.....	ad No 33, 2023
	am No 38, 2024
s 83B.....	ad No 33, 2023
	am No 38, 2024

Endnote 4—Amendment history

Provision affected	How affected
s 83C	ad No 33, 2023 am No 38, 2024
s 83CA	ad No 38, 2024
s 83D	ad No 33, 2023 am No 38, 2024
s 83E	ad No 33, 2023 am No 38, 2024
Subdivision C	
s 83EA	ad No 33, 2023
s 83EB	ad No 33, 2023
s 83EC	ad No 33, 2023
s 83ED	ad No 33, 2023
s 83EE	ad No 33, 2023
s 83EF	ad No 33, 2023
Division 4	
Division 4 heading	am No 38, 2024
s 83F	ad No 33, 2023 am No 38, 2024
Part V	
Part V heading	am No 161, 1999 rs No 108, 2014
s 84	am No 141, 1987; No 161, 1999 rs No 108, 2014
s 85	am No 122, 1986 (as am by No 137, 1988); No 137, 1988; No 161, 1999 rs No 108, 2014
s 86	am No 122, 1986 (as am by No 137, 1988); No 137, 1988; No 146, 1999; No 161, 1999 rs No 108, 2014
s 87	am No 141, 1987; No 161, 1999 rs No 108, 2014

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 88.....	rep No 65, 1985 ad No 108, 2014
s 89.....	am No 141, 1987; No 161, 1999 rs No 108, 2014
s 90.....	am Nos 146 and 161, 1999; No 108, 2014
s 90A.....	ad No 182, 1994 rep No 146, 1999
s 91.....	am No 161, 1999; No 108, 2014 rs No 108, 2014
s 92.....	am No 122, 1986; No 161, 1999; No 108, 2000; No 153, 2001; No 128, 2005; No 108, 2014; No 31, 2018 rs No 24, 2024
s 92A.....	ad No 122, 1986 am No 161, 1999 rep No 153, 2001 ad No 24, 2024
s 92B.....	ad No 122, 1986 am No 161, 1999 rep No 153, 2001 ad No 24, 2024
s 92C.....	ad No 122, 1986 am No 161, 1999 rep No 153, 2001 ad No 24, 2024
s 92D.....	ad No 122, 1986 rep No 153, 2001 ad No 24, 2024
Part VA heading.....	am No 161, 1999 rep No 153, 2001
Part VA.....	ad No 122, 1986 rep No 153, 2001

Endnote 4—Amendment history

Provision affected	How affected
s 92E	ad No 122, 1986 rep No 153, 2001
s 92F	ad No 122, 1986 rep No 153, 2001
s 92G.....	ad No 122, 1986 am No 115, 1990; No 161, 1999 rep No 153, 2001
s 92H.....	ad No 122, 1986 am No 161, 1999 rep No 153, 2001
s 92J	ad No 122, 1986 am No 161, 1999 rep No 153, 2001
s 92K.....	ad No 122, 1986 rep No 153, 2001
s 92L	ad No 122, 1986 rep No 153, 2001
s 92M.....	ad No 122, 1986 am No 161, 1999; No 24, 2001 rep No 153, 2001
s 92N.....	ad No 122, 1986 am No 161, 1999 rep No 153, 2001
s 92P	ad No 122, 1986 rs No 115, 1990 rep No 153, 2001
s 92Q.....	ad No 122, 1986 am No 161, 1999 rep No 153, 2001

Endnotes

Endnote 4—Amendment history

Provision affected	How affected
s 92R	ad No 122, 1986 am No 115, 1990 rep No 153, 2001
s 92S	ad No 122, 1986 am No 161, 1999 rep No 153, 2001
s 92T	ad No 122, 1986 rep No 153, 2001
Part VI	
s 93A	ad No 38, 2024
s 93	rs No 122, 1986 am No 161, 1999; No 5, 2015
s 93A	ad No 11, 1990 am No 161, 1999 rep No 155, 2000
s 94	am No 122, 1986; No 161, 1999; No 77, 2003; No 54, 2006 rs No 62, 2014 am No 108, 2014; No 39, 2015; No 148, 2018; No 134, 2020; No 78, 2021
s 95	am No 24, 2024