Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024

No. 99, 2024

An Act to amend the *Intelligence Services Act 2001* and to deal with consequential matters arising from the enactment of the *Cyber Security Act 2024*, and for related purposes

Note: An electronic version of this Act is available on the Federal Register of Legislation (https://www.legislation.gov.au/)

Contents

Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024

No. 99, 2024

An Act to amend the *Intelligence Services Act 2001* and to deal with consequential matters arising from the enactment of the *Cyber Security Act 2024*, and for related purposes

[*Assented to 29 November 2024*]

The Parliament of Australia enacts:

1 Short title

This Act is the *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	29 November 2024
2. Schedules 1 and 2	At the same time as Part 4 of the *Cyber Security Act 2024* commences.	30 November 2024

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Limited use of certain cyber security information

Intelligence Services Act 2001

1 Subsection 3(1)

Insert:

Commonwealth body, for the purposes of Division 1A of Part 6, has the meaning given by subsection 41BA(5).

Commonwealth enforcement body, for the purposes of Division 1A of Part 6, has the meaning given by subsection 41BA(5).

computer has the same meaning as in the *Security of Critical Infrastructure Act 2018*.

coronial inquiry means a coronial inquiry, coronial investigation or coronial inquest under a law of the Commonwealth, or of a State or Territory.

cyber security incident has the meaning given by subsection 41BA(4).

entity, for the purposes of Division 1A of Part 6, has the meaning given by subsection 41BA(5).

limited cyber security information has the meaning given by subsection 41BA(1).

State body, for the purposes of Division 1A of Part 6, has the meaning given by subsection 41BA(5).

2 After Division 1 of Part 6

Insert:

Division 1A—Communication and use of limited cyber security information

41BA Cyber security information for which communication and use is limited by this Division

(1) This Division applies to information (***limited cyber security information***) if:

(a) the information relates to:

(i) a cyber security incident that has occurred or is occurring; or

(ii) a cyber security incident that may potentially occur; and

(b) the information has been acquired or prepared by ASD in a circumstance mentioned in subsection (2); and

(c) the information is not excepted under subsection (3).

(2) This Division only applies to information that ASD has acquired or prepared in one of the following circumstances:

(a) the information has been voluntarily provided to ASD, in the performance of its functions, by, or on behalf of, an entity (the ***impacted entity***) that:

(i) is, was or could reasonably be expected to be directly or indirectly impacted by the cyber security incident; or

(ii) would be or would reasonably be expected to be impacted by the cyber security incident that may potentially occur;

(b) the information has been acquired or prepared by ASD, in the performance of its functions, with the consent of the impacted entity;

(c) the information has been:

(i) acquired by the National Cyber Security Coordinator under subsection 35(2) of the *Cyber Security Act 2024* in relation to the cyber security incident; and

(ii) disclosed to ASD under subsection 38(1), 39(2) or 40(2) of that Act.

(3) This Division does not apply to information if:

(a) the information has been provided to the Commonwealth about the cyber security incident to comply with:
  (i) a requirement in Part 3 of the *Cyber Security Act 2024*; or
  (ii) a requirement in Part 2B of the *Security of Critical Infrastructure Act 2018*; or
  (iii) a requirement under the *Telecommunications Act 1997*; or
  (iv) a requirement under a prescribed law; or
(b) the information has already been lawfully made available to the public; or
(c) the information is about an entity and has been de-identified so that it is no longer about an identifiable entity or an entity that is reasonably identifiable.

(4) A ***cyber security incident*** is:
(a) one or more acts, events or circumstances:
  (i) of a kind covered by the meaning of ***cyber security incident*** in the *Security of Critical Infrastructure Act 2018*; or
  (ii) involving unauthorised impairment of electronic communication to or from a computer, within the meaning of that phrase in that Act, but as if that phrase did not exclude the mere interception of any such communication; or
(b) the discovery of unintended or unexpected vulnerabilities in a computer, computer data or a computer program that, if exploited, would result in a cyber security incident within the meaning of paragraph (a).

(5) For the purposes of this Division:
(a) ***Commonwealth body*** has the same meaning as in the *Cyber Security Act 2024*; and
(b) ***Commonwealth enforcement body*** has the same meaning as in the *Cyber Security Act 2024*; and
(c) ***entity*** has the same meaning as in the *Cyber Security Act 2024*; and
(d) ***State body*** has the same meaning as in the *Cyber Security Act 2024*.

41BB Limited cyber security information can only be communicated by ASD for permitted cyber security purposes

(1) The Director-General of ASD, or a staff member of ASD, may communicate limited cyber security information to a person who is not the Director-General of ASD, or a staff member of ASD, but only for the purposes of one or more of the following:

(a) the performance of any of ASD's functions under this Act including, for example:

(i) assisting, in the performance of ASD's functions, the impacted entity (referred to in paragraph 41BA(2)(a) or (b)) to respond to, mitigate or resolve the cyber security incident or the cyber security incident that may potentially occur; or

(ii) providing technical advice and assistance, in the performance of ASD's functions, to entities on the prevention of cyber security incidents or cyber security incidents that may potentially occur;

(b) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident or a cyber security incident that may potentially occur;

(c) the performance of the functions of a Commonwealth body (to the extent that it is not a Commonwealth enforcement body) relating to responding to, mitigating or resolving a cyber security incident or a cyber security incident that may potentially occur;

(d) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident (within the meaning of the *Cyber Security Act 2024*);

(e) the performance of the functions of the National Cyber Security Coordinator under Part 4 of the *Cyber Security Act 2024* in relation to a cyber security incident (within the meaning of that Act);

(f) the performance of the functions of ASIS, AGO, the Australian Security Intelligence Organisation, the Defence Intelligence Organisation or the Office of National Intelligence;

(g) the performance of the functions of the Inspector-General of Intelligence and Security;

(h) the performance of the functions of the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*;

(i) the performance of the functions of a Commonwealth enforcement body.

Note: Information must not be communicated to a State body under this Division unless a Minister of the State or Territory has consented to this Division applying to the State body: see subsection 41BD(4).

Restriction on use and communication for civil or regulatory action

(2) However, the Director-General of ASD, or a staff member of ASD, must not communicate the information for the purposes of investigating or enforcing, or assisting the investigation or enforcement, of any contravention of a Commonwealth, State or Territory law that:

(a) is a contravention by the impacted entity that:

(ii) originally voluntarily provided the information to ASD as referred to in paragraph 41BA(2)(a); or

(ii) consented to the information being acquired or prepared by ASD as referred to in paragraph 41BA(2)(b); or

(iii) originally voluntarily provided the information to the National Cyber Security Coordinator under subsection 35(2), or as referred to in subsection 39(1), of the *Cyber Security Act 2024*; and

(b) is not a contravention by the impacted entity of:

(i) this Division; or

(ii) a law that imposes a penalty or sanction for a criminal offence.

Note: See also section 41BF in relation to admissibility of the information in proceedings.

Interaction with this Act

(3) Subsection (1) does not authorise the Director-General of ASD, or a staff member of ASD, to communicate the information to the extent that it is prohibited or restricted by or under this Act.

41BC Limitations on secondary use and communication of limited cyber security information

(1) This section applies to limited cyber security information that:

(a) has been acquired, under subsection 41BB(1) or this section, by:

(i) a Commonwealth body; or

(ii) a State body; or

(iii) an entity that is a corporation to which paragraph 51(xx) of the Constitution applies; and

(b) is held by the Commonwealth body, State body or entity.

Note: This section does not apply to information held by the Commonwealth body, State body or entity, to the extent that it has been otherwise acquired.

(2) The Commonwealth body, State body or entity may use or communicate the limited cyber security information but only for the purposes of one or more of the following:

(a) informing and advising the Minister, and other Ministers of the Commonwealth, about a cyber security incident or a cyber security incident that may potentially occur;

(b) the performance of the functions of a Commonwealth body (to the extent that it is not a Commonwealth enforcement body) relating to responding to, mitigating or resolving a cyber security incident or a cyber security incident that may potentially occur;

(c) the performance of the functions of a State body relating to responding to, mitigating or resolving a cyber security incident (within the meaning of the *Cyber Security Act 2024*);

(d) the performance of the functions of the National Cyber Security Coordinator under Part 4 of the *Cyber Security Act 2024* in relation to a cyber security incident (within the meaning of that Act);

(e) the performance of the functions of ASD, ASIS, AGO, the Australian Security Intelligence Organisation, the Defence Intelligence Organisation or the Office of National Intelligence;

(f) the performance of the functions of the Inspector-General of Intelligence and Security;

(g) the performance of the functions of the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*;

(h) the performance of the functions of a Commonwealth enforcement body.

Note: Information must not be communicated to a State body under this Division unless a Minister of the State or Territory has consented to this Division applying to the State body: see subsection 41BD(4).

Restriction on use and communication for civil or regulatory action

(3) However, the Commonwealth body, State body or entity must not use or communicate the information for the purposes of investigating or enforcing, or assisting the investigation or enforcement of, any contravention of a Commonwealth, State or Territory law that:

(a) is a contravention by the impacted entity that:

(i) originally voluntarily provided the information to ASD as referred to in paragraph 41BA(2)(a); or

(ii) consented to the information being acquired or prepared by ASD as referred to in paragraph 41BA(2)(b); or

(iii) originally voluntarily provided the information to the National Cyber Security Coordinator under subsection 35(2), or as referred to in subsection 39(1), of the *Cyber Security Act 2024*; and

(b) is not a contravention by the impacted entity of:

(i) this Division; or

(ii) a law that imposes a penalty or sanction for a criminal offence.

Note: See also section 41BF in relation to admissibility of the information in proceedings.

Interaction with this Act

(4) Subsection (2) does not authorise the Commonwealth body, State body or entity to use or communicate the information to the extent that it is prohibited or restricted by or under this Act.

Information not covered by the prohibitions in this section

(5) Subsection (2) does not prohibit:

(a) use or communication of the limited cyber security information, by the Commonwealth body, State body or entity, with the consent of the impacted entity that:

(i) originally voluntarily provided the limited cyber security information to ASD as referred to in paragraph 41BA(2)(a); or

(ii) consented to the limited cyber security information being acquired or prepared by ASD as referred to in paragraph 41BA(2)(b); or

(iii) originally voluntarily provided the limited cyber security information to the National Cyber Security Coordinator under subsection 35(2), or as referred to in subsection 39(1), of the *Cyber Security Act 2024*; or

(b) use or communication of information for the purposes of carrying out a State's constitutional functions, powers or duties.

Civil penalty for contravention of this section

(6) An entity is liable to a civil penalty if:

(a) the entity contravenes subsection (2); and

(b) the entity is not a Commonwealth officer (within the meaning of Part 5.6 of the *Criminal Code*); and

(c) any of the following applies:

(i) the information is sensitive information (within the meaning of the *Privacy Act 1988*) about an individual and the individual has not consented to the use or communication of the information;

(ii) the information is confidential or commercially sensitive;

(iii) the use or communication of the information would, or could reasonably be expected to cause, damage to the security, defence or international relations of the Commonwealth.

Note 1: See the *Criminal Code* for offences for Commonwealth officers.

Note 2: This section does not make the Crown (other than an authority of the Crown) liable to a civil penalty, see section 41BD.

Note 3: For the application of provisions of the *Regulatory Powers (Standard Provisions) Act 2014* to this Division, see Part 6 of the *Cyber Security Act 2024*.

Civil penalty: 60 penalty units.

41BD Application of section 41BC to the Crown

(1) Section 41BC binds the Crown in right of each of its capacities.

(2) Subsection (1) does not make the Crown liable to be prosecuted for an offence.

Note: The Crown (other than a Crown authority) is not liable to a pecuniary penalty for the breach of a civil penalty provision or to be given an infringement notice: see subsections 79(8) and 82(7) of the *Cyber Security Act 2024*.

(3) The protection in subsection (2) does not apply to an authority of the Crown.

(4) Despite any other provision of this Division, information that may be communicated to a State body under this Division must not be communicated to the State body under this Division unless:

(a) a Minister of the State or Territory has informed the responsible Minister for ASD, in writing, that the State or Territory gives consent to the provisions of this Division applying to the State body; and

(b) a Minister of the State or Territory has not informed the responsible Minister for ASD, in writing, that the State or Territory withdraws that consent.

(5) For the purposes of paragraph (4)(a), a Minister of a State or Territory may give consent in relation to all State bodies, a class of State bodies, or particular State bodies, of that State or Territory.

41BE Legal professional privilege

(1) The fact that an entity provided information to ASD, as referred to in paragraph 41BA(2)(a), does not otherwise affect a claim of legal

professional privilege that anyone may make in relation to that information in any proceedings:

(a) under any Commonwealth, State or Territory law (including the common law); or

(b) before a tribunal of the Commonwealth, a State or a Territory.

(2) Despite subsection (1), this section does not apply to the following:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(b) proceedings in a federal court exercising original jurisdiction in which a writ of mandamus or prohibition or an injunction is sought against an officer or officers of the Commonwealth.

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

(3) This section does not limit or affect any right, privilege or immunity that the impacted entity has, apart from this section, as a defendant in any proceedings.

41BF Admissibility of limited cyber security information voluntarily given by impacted entity

(1) This section applies to limited cyber security information that:

(a) either:

(i) has been voluntarily provided to ASD by, or on behalf of, an entity (the ***impacted entity***), as referred to in paragraph 41BA(2)(a); or

(ii) has been acquired or prepared by ASD with the consent of an entity (the ***impacted entity***), as referred to in paragraph 41BA(2)(b); and

(b) has been prepared by, as referred to in paragraph 41BA(2)(b), acquired by, as referred to in paragraph 41BA(2)(a) or (b), or acquired, under subsection 41BB(1) or section 41BC, by a Commonwealth body or a State body; and

(c) is held by the Commonwealth body or State body.

Note 1: This section does not apply to information held by the Commonwealth body or State body to the extent that it has been otherwise prepared or acquired.

Note 2: ASD is a Commonwealth body: see the definition of ***Commonwealth body*** in subsection 41BA(5) and section 8 of the *Cyber Security Act 2024*.

Note 3: For admissibility of information acquired by ASD as referred to in paragraph 41BA(2)(c), see section 42 of the *Cyber Security Act 2024*.

(2) The limited cyber security information is not admissible in evidence against the impacted entity in any of the following proceedings:

(a) criminal proceedings for an offence against a Commonwealth, State or Territory law, other than:

(i) proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* (which deal with false or misleading information or documents) that relates to this Act; or

(ii) proceedings for an offence against section 149.1 of the *Criminal Code* (which deals with obstruction of Commonwealth public officials) that relates to this Act;

(b) civil proceedings for a contravention of a civil penalty provision of a Commonwealth, State or Territory law, other than a civil penalty provision of this Division;

(c) proceedings for a breach of any other Commonwealth, State or Territory law (including the common law);

(d) proceedings before a tribunal of the Commonwealth, a State or a Territory.

(3) Despite subsection (2), subsection (2) does not apply to the following proceedings:

(a) the proceedings of a coronial inquiry or a Royal Commission in Australia;

(b) proceedings in a federal court exercising original jurisdiction in which a writ of mandamus or prohibition or an injunction is sought against an officer or officers of the Commonwealth.

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

(4) This section does not limit or affect any right, privilege or immunity that the impacted entity has, apart from this section, as a defendant in any proceedings.

41BG Director-General of ASD and staff members of ASD not compellable as witnesses in relation to limited cyber security information

(1) A person who is, or has been, the Director-General of ASD or a staff member of ASD:

(a) is not obliged to comply with a subpoena or similar direction of a federal court or a court of a State or Territory to attend and answer questions relating to limited cyber security information; and

(b) is not compellable to give an expert opinion in any civil or criminal proceedings in a federal court or a court of a State or Territory in relation to limited cyber security information.

(2) This section does not apply to a coronial inquiry.

41BH How this Division applies in relation to non-legal persons

How permissions and rights are conferred and exercised

(1) If this Division purports to confer a permission or right on an entity that is not a legal person, the permission or right:

(a) is conferred on each person who is an accountable person for the entity at the time the permission or right may be exercised; and

(b) may be exercised by:

(i) any person who is an accountable person for the entity at the time the permission or right may be exercised; or

(ii) any person who is authorised by a person referred to in subparagraph (i) to exercise the permission or right.

How obligations and duties are imposed and discharged

(2) If this Division purports to impose an obligation or duty on an entity that is not a legal person, the obligation or duty:

(a) is imposed on each person who is an accountable person for the entity at the time the obligation or duty arises or is in operation; and

(b) may be discharged by:

(i) any person who is an accountable person for the entity at the time the obligation or duty arises or is in operation; or

(ii) any person who is authorised by a person referred to in subparagraph (i) to discharge the obligation or duty.

How non-legal persons contravene this Division

(3) A provision of this Division (including a civil penalty provision) that is purportedly contravened by an entity that is not a legal person is instead contravened by each accountable person for the entity who:

(a) did the relevant act or made the relevant omission; or

(b) aided, abetted, counselled or procured the relevant act or omission; or

(c) was in any way knowingly concerned in, or party to, the relevant act or omission.

*Meaning of **accountable person***

(4) For the purposes of this section, a person is an ***accountable person*** for an entity at a particular time if:

(a) in the case of a partnership in which one or more of the partners is an individual—the individual is a partner in the partnership at that time; or

(b) in the case of a partnership in which one or more of the partners is a body corporate—the person is a director of the body corporate at that time; or

(c) in the case of a trust in which the trustee, or one or more of the trustees, is an individual—the individual is a trustee of the trust at that time; or

(d) in the case of a trust in which the trustee, or one or more of the trustees, is a body corporate—the person is a director of the body corporate at that time; or

(e) in the case of an unincorporated association—the person is a member of the governing body of the unincorporated association at that time.

41BI Contravening a civil penalty provision of this Division

(1) This section applies if a provision of this Division provides that an entity contravening another provision of this Division (the ***conduct provision***) is liable to a civil penalty.

(2) For the purposes of this Division, and the *Regulatory Powers (Standard Provisions) Act 2014* to the extent that it relates to this Division, a reference to a contravention of a civil penalty provision includes a reference to a contravention of the conduct provision.

Note: For the application of provisions of the *Regulatory Powers (Standard Provisions) Act 2014* to this Division, see Part 6 of the *Cyber Security Act 2024*.

Schedule 2—Other amendments

Freedom of Information Act 1982

1 After subsection 7(2G)

Insert:

(2H) A Minister and an agency are exempt from the operation of this Act in relation to a document given to, or received by, the National Cyber Security Coordinator, for the purposes of the performance of a function, or the exercise of a power, under Part 4 of the *Cyber Security Act 2024*.

[*Minister's second reading speech made in—*
House of Representatives on 9 October 2024
Senate on 25 November 2024]

(118/24)