Australian Government

Department of Home Affairs

Surveillance Devices Act 2004

Annual Report 2024–25

Table of Contents

Executive Summary

The *Surveillance Devices Act 2004* (the SD Act) requires that each year the Minister for Home Affairs lay before each House of Parliament a report setting out the information required by section 50 of the SD Act. The Annual Report for 2024–25 describes the extent and circumstances in which eligible Commonwealth, state and territory law enforcement agencies have used the powers available under the SD Act between 1 July 2024 and 30 June 2025.

Objects of the *Surveillance Devices Act 2004*

The SD Act provides a legislative regime for Commonwealth agencies to use surveillance devices and access data held in computers. It also provides a regime for the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to disrupt data held in computers and collect intelligence that relates to criminal networks of individuals.

The SD Act also authorises state and territory law enforcement agencies to use surveillance devices and access data held in computers for certain investigations relevant to Commonwealth offences and state offences with a federal aspect. A state offence with a federal aspect may include, for example, a state offence committed by a constitutional corporation, committed in a Commonwealth place, involving an electronic communication, or involving trade or commerce.

The SD Act also restricts the use, communication, and publication of information that is obtained through the use of powers under the SD Act.

Powers under the SD Act may be used by officers of the following law enforcement agencies:

- ACIC
- AFP
- National Anti-Corruption Commission (NACC)
- State and territory police forces
- Crime and Corruption Commission of Queensland
- Corruption and Crime Commission of Western Australia
- Independent Broad-based Anti-Corruption Commission of Victoria
- Independent Commission Against Corruption of New South Wales
- Independent Commission Against Corruption of South Australia
- New South Wales Crime Commission, and
- New South Wales Law Enforcement Conduct Commission (LECC).

Key statistics

- In 2024–25, five law enforcement agencies were issued 743 surveillance device warrants, an increase of 107 warrants from the 636 issued in 2023–24.
- In 2024–25, no applications for surveillance device warrants were refused by an issuing authority, compared to the 12 applications refused in 2023–24.
- In 2024–25, 42 computer access warrants were issued to law enforcement agencies, an increase of 24 warrants from the 18 issued in 2023–24. No computer access warrants were refused in 2023–24, or in 2024–25.
- In 2024–25, four data disruption warrants were issued, an increase of three warrants from the one issued 2023–24. One data disruption warrant was initially refused in 2024–25 (compared to none in 2023-24), but was then granted after further information was supplied.
- In 2024–25, one network activity warrant was issued, a decrease of one from the two issued in 2023–24. One further network activity warrant was refused in 2024–25, an increase of one from 2023–24.
- In 2024–25, 214 applications to extend surveillance device warrants were granted, representing a decrease of 30 applications from the 244 granted in 2023–24. Applications to extend warrants are often required due to the prolonged nature of investigations for complex and serious crime (where evidence gathering may not have been completed within 90 days).
- In 2024–25, 26 retrieval warrants were issued to law enforcement agencies in order to retrieve lawfully installed surveillance devices, an increase of nine warrants from the 17 issued in 2023–24.
- In 2024–25, 21 tracking device authorisations were issued, an increase of 11 authorisations from the 10 issued in 2023-24. One tracking device retrieval authorisation was issued in 2024-25, an increase of one from 2023–24.
- In 2024–25, information obtained under the SD Act contributed to 271 arrests, 190 prosecutions, and 29 convictions. In 2023–24, information obtained under the SD Act contributed to 148 arrests, 102 prosecutions and 18 convictions.

Chapter 1: Warrants and Oversight

Part 2 of the SD Act allows law enforcement agencies to apply for five types of warrants:

- surveillance device warrants
- retrieval warrants
- computer access warrants
- data disruption warrants, and
- network activity warrants.

Further information on these warrants, including statistics on their use during the 2024–25 reporting period, can be found in Chapters 2, 3, 4 and 5 of this report. Although account takeover warrants were introduced with data disruption and network activity warrants under the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, use of account takeover warrants are reported on in agencies' annual report under the *Crimes Act 1914*.

Arrangements for the issuing of warrants under the SD Act altered following the operational commencement of the Administrative Review Tribunal (ART) on 14 October 2024, replacing the former Administrative Appeals Tribunal (AAT). Previously, nominated members of the AAT were eligible to issue warrants. The SD Act now provides that an eligible Judge or nominated ART member may issue a warrant, with all matters previously dealt with by the AAT now transferred to the ART.

An eligible Judge is a Judge who has consented in writing and been declared by the Attorney-General to be an eligible Judge. During the reporting period, eligible Judges included members of the:

- Federal Court of Australia, and
- Federal Circuit and Family Court of Australia.

A nominated ART member refers to a Deputy President, senior member, or general member of the ART that has been nominated by the Attorney-General to issue warrants under the SD Act.

In the case of part-time senior members and members of the ART, the person must have been enrolled as a legal practitioner of the High Court, another federal court, or Supreme Court of a State or of the Australian Capital Territory for no less than five years to be eligible for nomination to issue warrants.

The total number of eligible Judges and nominated ART members available to issue warrants under the SD Act in the reporting period is presented in **Table 1**.

Table 1: Availability of eligible Judges, and nominated ART members to issue warrants

Issuing authority	Number	
	23/24	24/25
Nominated AAT/ART Members[1]	33	51[2]
Federal Circuit and Family Court of Australia Judges	40	42
Federal Court Judges	16	17
TOTAL	**89**	**110**

Form of applications

Generally, an application for a warrant must be in writing and be accompanied by an affidavit setting out the grounds on which the warrant is sought. Where a law enforcement officer believes that it is impracticable for an application for a warrant to be made in person, remote applications may be made by telephone, fax, email or any other means of communication.

Offences and matters for which warrants are available

A law enforcement agency may apply for a warrant under the SD Act to assist in the investigation or disruption of a 'relevant offence', or collection of intelligence in relation to a 'relevant offence. 'Relevant offence' is defined in section 6 of the SD Act as including:

- Commonwealth offences which carry a maximum penalty of at least three years imprisonment
- state offences with a federal aspect (which is defined in section 7 of the SD Act) and carry a maximum penalty of at least three years imprisonment
- specific offences under the:
  - *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
  - *Financial Transaction Reports Act 1988*[3]
  - *Fisheries Management Act 1991*, and

[1] The AAT was replaced with the ART on 14 October 2024.
[2] 23 members were eligible to issue warrants before the ART commenced and 42 were eligible to issue warrants after the ART commenced. 14 were eligible both before and after the ART's commencement.
[3] This Act was repealed by the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024*.

- *Torres Strait Fisheries Act 1984*

- offences against laws of the Commonwealth, states and territories which carry a maximum penalty of at least 12 months imprisonment as part of an integrity operation, and
- offences that are prescribed by the regulations.[4]

The offences specified above that do not carry maximum penalties of at least three years imprisonment either:

- carry pecuniary penalties that are the equivalent of imprisonment terms of at least three years, or
- are generally considered to be serious criminal conduct.

The surveillance device and computer access powers in the SD Act are also available to assist in the safe recovery of a child who is subject to a recovery order made under section 67U of the *Family Law Act 1975,* or an order for a warrant for the apprehension or detention of a child under the *Family Law (Child Abduction Convention) Regulations 1986.*

Duration of warrants

A warrant has effect for the period specified in the warrant, which cannot exceed 90 days (or 21 days, in the case of a warrant issued for the purposes of an integrity operation), unless the warrant is revoked earlier or extended. A warrant may be extended or varied by an eligible Judge or nominated ART member if he or she is satisfied that the grounds on which the warrant was issued continue to exist.

Extraterritorial operation of warrants

Part 5 of the SD Act allows for Commonwealth law enforcement agencies to use surveillance devices or access data held in a computer in the investigation of 'relevant offences' where there is a need for surveillance, or access to data held in a computer outside Australia. However, there is an exception for the investigation of certain offences in Australia's contiguous and fishing zones:

- the consent of an appropriate official of the foreign country must be obtained, or
- if surveillance or access to data is occurring on a vessel or aircraft that is in or above waters beyond the outer limits of the territorial sea of Australia, consent must be obtained from the country for registration of the vessel or aircraft.

Part 5 contains similar provisions in relation to the extraterritorial operation of network activity warrants and data disruption warrants. However, consent from an appropriate official is not required for a computer access, data disruption or network activity warrant, if the person executing the warrant is physically present in Australia and the locations where the data is held is unknown or cannot reasonably be determined.

[4] No offences are currently specified in regulations.

Use of the information obtained

The SD Act restricts the use, communication, and disclosure of information obtained under the SD Act. As a general rule, all information obtained under the SD Act and all information relating to the existence of a warrant or authorisation is 'protected information' and may only be used for the purposes set out in the SD Act. These purposes include:

- the investigation and prosecution of relevant offences, including but not limited to the offence for which surveillance powers in the SD Act were originally used
- information sharing with the Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Australian Geospatial-Intelligence Organisation or Australian Signals Directorate, where the information relates or appears to relate to the functions of those agencies
- disciplinary proceedings for public officers
- the provision of international assistance to other countries, the International Criminal Court, or war crimes tribunals, where such assistance has been authorised under the *Mutual Assistance in Criminal Matters Act 1987*, *International Criminal Court Act 2002* or *International War Crimes Tribunals Act 1995*, respectively, and
- where the use of the information is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property, including protecting the public from a terrorist act.

Information obtained under a network activity warrant can only be used for intelligence related purposes, and will generally not be permitted to be used in evidence in criminal proceedings. Intelligence related purposes include making reports in relation to criminal intelligence or applying for another warrant.

Accountability provisions

The SD Act includes a reporting and inspection regime, which allows the Commonwealth Ombudsman (the Ombudsman), the Inspector-General of Intelligence and Security (IGIS), the Minister for Home Affairs, and the Parliament to scrutinise the exercise of powers under the SD Act.

All law enforcement agencies are required to maintain records relating to each warrant or authorisation, and the use of information obtained through powers in the SD Act. All law enforcement agencies must maintain a register of all warrants and authorisations, and provide the Minister for Home Affairs with a report on all warrants and authorisations issued under the SD Act.

Inspections and report by the Commonwealth Ombudsman

The Ombudsman is required to inspect the records of law enforcement agencies to ensure compliance with the SD Act, except insofar as it relates to network activity warrants which are overseen by the IGIS. The Ombudsman must make a written report to the Minister for Home Affairs at six monthly intervals on the results of each inspection. The Minister for Home Affairs must present a copy of the report before each House of Parliament within 15 sitting days after the Minister receives it.

The Ombudsman's inspection for the period from 1 July to 31 December 2024 was tabled in the Senate on 7 August 2025 and the House of Representatives on 24 August 2025.

The report detailing the Ombudsman's inspections for the period from 1 January 2025 to 30 June 2025 had not been presented before Parliament at the time this report was provided to the Minister for Home Affairs.

Once laid before each House of Parliament, these reports are available at <https://www.ombudsman.gov.au/>.

Agencies are also required to notify the Ombudsman of certain matters within seven days including:

- if anything has been done in relation to a computer to conceal acts done under a computer access warrant more than 28 days after the warrant ceases to be in force
- if anything was done under a data disruption warrant, and
- if anything done under a data disruption warrant has caused material loss or damage to one or more persons lawfully using a computer.

Oversight by the Inspector-General of Intelligence and Security

The IGIS has oversight responsibility of network activity warrants as they are an intelligence collection tool. The IGIS is responsible for inspecting, inquiring, and reporting on the use of network activity warrants by the AFP and the ACIC to ensure both agencies act lawfully, with propriety, and consistently with human rights.

Agencies are also required to notify the IGIS of certain matters within seven days, including if a network activity warrant was issued, and if anything has been done to conceal the use of a network activity warrant after the 28 days after which the warrant ceases to be in force.

The IGIS must include its comments on any inspection conducted in respect of the AFP's and the ACIC's use of network activity warrants in its annual report given to the Minister for Home Affairs under section 46 of the *Public Governance, Performance and Accountability Act 2013*. The Minister for Home Affairs must cause a copy of the report to be laid before each House of Parliament as soon as practicable after the Minister receives it.

The IGIS' annual report for the 2023–24 financial year, which includes its comments on inspections conducted in respect of the AFP and the ACIC's use of network activity warrants, was tabled in the Senate on 16 October 2024, and in the House of Representatives on 4 November 2024.

The report detailing the IGIS' inspections on agency compliance with the SD Act for the period from 1 July 2024 to 30 June 2025 had not been laid before each House of Parliament at the time this report was provided to the Minister for Home Affairs.

Once laid before each House of Parliament, the report is available at <www.igis.gov.au/>.

Chapter 2: Surveillance Devices

Applications for surveillance device warrants

Section 14 of the SD Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for a surveillance device warrant for the investigation of a 'relevant offence'. The use of the surveillance device must be necessary, in the course of an investigation, for the purpose of enabling evidence to be obtained of the commission of that 'relevant offence', or the identity or location of the offenders. A surveillance device warrant may also be issued for the safe recovery of a child, for the purposes of an integrity operation, international assistance applications, and for determining whether to apply for post-sentence orders (such as Part 5.3 and Part 9.10 orders).

Surveillance device warrants may be issued in respect of a single surveillance device, in respect of more than one kind of surveillance device, or in respect of more than one surveillance device of any particular kind. The kinds of surveillance devices available to law enforcement under the SD Act are:

- **data surveillance devices**, meaning any device or program used to record or monitor the input of information into or output of information from a computer.
- **listening devices**, meaning any device capable of being used to hear, record, monitor, or listen to conversations or words spoken but does not include a hearing aid or similar device.
- **optical surveillance devices**, meaning any device used to record visually or observe an activity but does not include spectacles, contact lenses, or similar devices.
- **tracking devices**, meaning any electronic device capable of determining or monitoring the location of a person or an object, or the status of an object.
- **composite devices**, meaning any device that is a combination of two or more of the devices referred to above.

Paragraphs 50(1)(a) and 50(1)(e) of the SD Act provide that this report must set out the number of applications for surveillance device warrants made and refused (including reasons for any refusal), and the number of warrants issued during the reporting period. Subsection 50(2) requires that this report set out a breakdown of these numbers in respect of each kind of surveillance device.

This information is presented in **Table 2**. In 2024–25, law enforcement agencies were issued 743 surveillance device warrants. No applications for surveillance device warrants were refused by an issuing authority, compared to 12 applications refused in 2023–24.

Table 2: Number of surveillance device warrant applications made, issued and refused – paragraphs 50(1)(a) and 50(1)(e) [5]

Agency		Composite/ Multiple[6]		Optical		Listening		Data		Tracking		TOTAL	
		23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25
ACIC	Made	9	3	-	-	-	-	1	-	3	-	**13**	**3**
	Refused	-	-	-	-	-	-	-	-	-	-	**-**	-
	Issued	9	3	-	-	-	-	1	-	3	-	**13**	**3**
AFP	Made	610	709	-	-	-	-	-	-	-	-	**610**	**709**
	Refused	12	-	-	-	-	-	-	-	-	-	**12**	**-**
	Issued	598	709	-	-	-	-	-	-	-	-	**598**	**709**
LECC	Made	4	-	-	-	-	-	-	-	-	-	**4**	**-**
	Refused	-	-	-	-	-	-	-	-	-	-	**-**	**-**
	Issued	4	-	-	-	-	-	-	-	-	-	**4**	**-**
NACC	Made	5	-	-	-	2	-	4	**3**	-	**-**	**11**	**3**
	Refused	-	-	-	-	-	-	-	**-**	-	**-**	**-**	**-**
	Issued	5	-	-	-	2	-	4	**3**	-	**-**	**11**	**3**

[5] Agencies that did not apply for a surveillance device warrant are not included in Table 2.
[6] Applications for the authorisation of multiple kinds of surveillance devices and applications for the use of composite surveillance devices are included in this column.

Agency		Composite/ Multiple[6]		Optical		Listening		Data		Tracking		TOTAL	
		23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25
NT Police	Made	2	-	-	-	-	-	-	-	-	-	**2**	**-**
	Refused	-	-	-	-	-	-	-	-	-	-	**-**	**-**
	Issued	2	-	-	-	-	-	-	-	-	-	**2**	**-**
VIC Police	Made	-	2	-	-	-	-	-	-	-	-	**-**	**2**
	Refused	-	-	-	-	-	-	-	-	-	-	**-**	**-**
	Issued	-	2	-	-	-	-	-	-	-	-	**-**	**2**
WA Police	Made	8	6	-	-	-	-	-	19	-	1	**8**	**26**
	Refused	-	-	-	-	-	-	-	-	-	-	**-**	
	Issued	8	6	-	-	-	-	-	19	-	1	**8**	**26**
TOTAL	**Made**	**638**	**720**	**-**	**-**	**2**	**-**	**5**	**22**	**3**	**1**	**648**	**743**
	Refused	**12**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**12**	**-**
	Issued	**626**	**720**	**-**	**-**	**2**	**-**	**5**	**22**	**3**	**1**	**636**	**743**

Remote applications for surveillance device warrants

Section 15 of the SD Act permits an application for a surveillance device warrant to be made by telephone, fax, email, or other means of communications if the law enforcement officer believes that it is impracticable to make the application in person. Paragraph 50(1)(d) of the SD Act provides that this report must set out the number of remote applications for surveillance device warrants during the reporting period.

In 2024–25, there were no remote applications for surveillance device warrants. This is the same as in 2023–24.

Extension applications for surveillance device warrants

Section 19 of the SD Act provides that the law enforcement officer to whom a warrant was issued (or another person on the officer's behalf) may apply for an extension of the warrant for a period not exceeding 90 days after the warrant's original expiry date (or 21 days, in the case of a warrant issued for the purposes of an integrity operation). This application may be made any time before the warrant expires.

Paragraph 50(1)(f) of the SD Act provides that the annual report must set out the number of applications for the extension of a surveillance device warrant that were made, and the number of extensions granted and refused (including reasons why applications were granted or refused) during the reporting period.

This information is presented in **Table 3**. In 2024–25, there were 214 extensions of surveillance device warrants granted to law enforcement agencies, a decrease of 30 from the 244 extensions granted in 2023-24.

Table 3: Number of applications for extension of a surveillance device warrant – paragraph 50(1)(f)[7]

Agency		Applications	
		23/24	24/25
ACIC	Made	1	-
	Refused	-	-
	Issued	1	-
AFP	Made	238	211
	Refused	-	-
	Issued	238	211
LECC	Mades	5	-

[7] Agencies that did not apply for an extension of a surveillance device warrant are not included in Table 3.

Agency		Applications	
		23/24	24/25
	Refused	-	-
	Issued	5	-
NACC	Made	-	2
	Refused	-	-
	Issued	-	2
WA Police	Made	-	1
	Refused	-	-
	Issued	-	1
TOTAL	**Made**	**244**	**214**
	Refused	**-**	**-**
	Issued	**244**	**214**

The AFP advised it sought and was granted extensions of surveillance device warrants for the continued use of surveillance devices in the investigation of serious and organised criminal activity. The NACC advised that it sought and was granted extensions of surveillance device warrants in order to support ongoing criminal intelligence collection related to the commission of offences. WA Police advised it sought and was granted an extension of a surveillance device warrant for the continued use of surveillance devices in an ongoing criminal investigation.

International assistance applications for surveillance device warrants

Subsection 14(3A) of the SD Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for a surveillance device warrant when they are authorised by an international assistance authorisation and suspect on reasonable grounds that the use of the surveillance is necessary for the purpose of enabling evidence to be obtained of the commission of an international or foreign offence or the identity or location of such an offender.

The Attorney-General may issue international assistance authorisations under section 15CA of the *Mutual Assistance in Criminal Matters Act 1987*, section 79A of the *International Criminal Court Act 2002* and section 32A of the *International War Crimes Tribunals Act 1995* if satisfied of the following:

- a foreign country, the International Criminal Court, or a war crimes tribunal has requested that the Attorney-General arrange for the use of a surveillance device

- there is an investigation or proceeding underway within their jurisdiction (if the request is being made by a foreign country, the investigation must relate to a criminal matter involving an offence against the law of that foreign country that is punishable by a maximum penalty of at least three years imprisonment), and
- the requesting country, the International Criminal Court, or war crimes tribunal has given undertakings regarding:
  - the information obtained via the use of surveillance devices only being used for the purposes for which it is communicated to that jurisdiction
  - the destruction of the information obtained by the surveillance device, and
  - any other matters the Attorney-General considers appropriate.

Paragraphs 50(1)(aa) and 50(1)(ea) of the SD Act provide that this report must set out the number of international assistance applications made and refused (including the reasons for any refusal), and the number of warrants issued as a result during the reporting period.

Where a surveillance device warrant was issued as a result of an international assistance application, paragraph 50(1)(ia) of the SD Act requires that this report list the offence (if any) under a law of the Commonwealth, a state, or a territory that is of the same or substantially similar nature as the foreign offence being investigated under that surveillance device warrant.

In 2024–25, no applications for a surveillance device warrant were made due to an international assistance authorisation. This is the same as in 2023–24.

Application for retrieval warrants

Section 22 of the SD Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for a retrieval warrant in respect of a surveillance device that was lawfully installed on a premise, or in or on an object, under a surveillance device warrant or a tracking device authorisation. The officer must suspect on reasonable grounds that the device is still on those premises or in or on that object, or on other premises, or in or on another object.

Paragraphs 50(1)(a) and 50(1)(e) of the SD Act provide that this report must set out the number of applications for retrieval warrants made and refused (including reasons for any refusal), and the number of warrants issued during the reporting period. Subsection 50(2) requires that this report set out a breakdown of these numbers in respect of each kind of surveillance device. This information is presented in **Table 4**.

In 2024–25, the AFP was issued 26 warrants to retrieve a surveillance device, an increase of nine warrants from the 17 issued in 2023–24.[8]

[8] A surveillance device warrant may also authorise the retrieval of the surveillance device, removing the need for a law enforcement agency to apply for a retrieval warrant.

Table 4: Number of retrieval warrant applications made, issued and refused – paragraphs 50(1)(a) and 50(1)(e)[9]

Agency		Composite/ Multiple		Optical		Listening		Data		Tracking		TOTAL	
		23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25
AFP	Made	12	16	-	1	2	6	-	-	3	3	**17**	**26**
	Refused	-	-	-	-	-	-	-	-	-	-	**-**	**-**
	Issued	12	16	-	1	2	6	-	-	3	3	**17**	**26**
TOTAL	**Made**	**12**	**16**	**-**	**1**	**2**	**6**	**-**	**-**	**3**	**3**	17	26
	Refused	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**12**	**16**	**-**	**1**	**2**	**6**	**-**	**-**	**3**	**3**	17	26

[9] Agencies that did not apply for retrieval warrant applications are not included in Table 4.

Remote applications for retrieval warrants

Section 23 of the SD Act permits an application for a retrieval warrant to be made by telephone, fax, email, or other means of communication, if the law enforcement officer believes that immediate retrieval of a surveillance device is necessary, and it is impracticable to make the application in person. Paragraph 50(1)(d) of the SD Act provides that this report must set out the number of remote applications for retrieval warrants during the reporting period.

In 2024–25, no remote applications for a retrieval warrant were made. This is the same as in 2023–24.

Use of surveillance devices in emergency circumstances

An appropriate authorising officer of a law enforcement agency may issue an emergency authorisation enabling the use of surveillance devices without a warrant. An emergency authorisation may only be issued in urgent circumstances when it is not practicable to apply for a warrant, and:

- there is an imminent risk of serious violence to a person or substantial damage to property (section 28)
- a recovery order in relation to a child is in force and the law enforcement officer reasonably suspects that the circumstances are so urgent as to warrant the immediate use of a surveillance device (section 29), or
- there is a risk of loss of evidence for certain serious offences, such as drug offences, terrorism, espionage, sexual servitude, and aggravated people smuggling (section 30).

The appropriate authorising officer who gives an authorisation (or another person on their behalf) must apply to an eligible Judge or ART member for approval of the giving of the emergency authorisation within 48 hours of the authorisation being issued.

Paragraphs 50(1)(b) and 50(1)(e) provide that this report must set out the number of applications for emergency authorisations made and refused (including the reasons for any refusal), and the number of authorisations given during the reporting period. Subsection 50(2) requires that this report set out a breakdown of these numbers, in respect of each different kind of surveillance device.

In 2024–25, the AFP applied for, and was issued, one emergency authorisation to use a composite surveillance device without a warrant. This an increase of one from 2023–24. No other agencies made emergency authorisations.

Tracking device authorisations

Section 39 of the SD Act permits a law enforcement officer to use a tracking device without a warrant in the investigation of a relevant offence or to assist in the location and safe recovery of a child to whom a recovery order relates, where the officer has the written authorisation of an appropriate authorising officer.

A tracking device authorised under subsection 39(8) of the SD Act cannot be used, installed, or retrieved if it involves entry onto premises or an interference with the interior of a vehicle without permission. The permission may come from the owner or occupier. Where such use requires a greater level of intrusion (such as entry onto premises without permission), a surveillance device warrant is required.

Paragraphs 50(1)(c) and 50(1)(e) provide that this report must set out the number of applications for tracking device authorisations made and refused (including reasons for any refusal), and the number of authorisations given during the reporting period. This includes the number of tracking device retrievals, which may be authorised without a warrant in accordance with subsection 39(6) of the SD Act.

This information is presented in **Table 5**. In 2024–25, law enforcement agencies made 21 tracking device authorisations, an increase of 11 from the 10 given in 2023–24. One tracking device retrieval authorisation was given, an increase of one from 2023-24.

Table 5: Number of applications for tracking device authorisation – paragraphs 50(1)(c) and 50(1)(e)

Agency		Tracking Device Authorisations		Tracking Device Retrievals	
		23/24	24/25	23/24	24/25
ACIC	Made	1	-	-	-
	Refused	-	-	-	-
	Issued	1	-	-	-
AFP	Made	9	14	-	1
	Refused	-	-	-	-
	Issued	9	14	-	1
WA Police	Made	-	7	-	-
	Refused	-	-	-	-
	Issued	-	7	-	-
TOTAL	**Made**	**10**	**21**	**-**	**1**
	Refused	**-**	**-**	**-**	**-**
	Issued	**10**	**21**	**-**	**1**

Chapter 3: Computer Access Warrants

Applications for computer access warrants

Section 27A of the SD Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for the issue of a computer access warrant for the investigation of a 'relevant offence', which generally carries a maximum penalty of at least three years imprisonment. Access to data held in a computer must be necessary, in the course of an investigation for the purpose of enabling evidence to be obtained of the commission of that 'relevant offence', or the identity or location of the offenders. A computer access warrant may also be issued for the safe recovery of a child, for the purposes of an integrity operation, and for determining whether to apply for post-sentence orders.

A computer access warrant must specify the things that are authorised under the warrant, which may include:

- entering premises for the purposes of executing the warrant
- using the target computer, a telecommunications facility, electronic equipment or data storage device, in order to access data held in the target computer, to determine whether the relevant data is covered by the warrant
- adding, copying, deleting or altering data in the target computer if necessary to access the data to determine whether the relevant data is covered by the warrant
- using any other computer if necessary to access the data (and adding, copying, deleting or altering data on that computer if necessary)
- removing a computer from premises for the purposes of executing the warrant
- copying data to which access has been obtained that is relevant and covered by the warrant
- intercepting a communication in order to execute the warrant, and
- any other thing reasonably incidental to the above things.

Computer access warrants do not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more of the things specified in the warrant. Computer access warrants do not authorise anything that is likely to cause material loss or damage to other persons lawfully using a computer.

Paragraphs 50(1)(a) and 50(1)(e) of the SD Act provide that this report must set out the number of applications for computer access warrants made and refused (including reasons for any refusal), and the number of warrants issued during the reporting period.

Section 27B of the SD Act permits a remote application for a computer access warrant to be made by telephone, fax, email, or other means of communication if the law

enforcement officer believes that it is impracticable to make the application in person. Paragraph 50(1)(d) of the SD Act provides that this report must set out the number of remote applications made during the reporting period.

Section 27F of the SD Act provides that the law enforcement officer to whom a computer access warrant was issued (or another person on the officer's behalf) may apply for an extension of the warrant for a period not exceeding 90 days after the warrant's original expiry date (or 21 days, in the case of a warrant issued for the purposes of an integrity operation). This application may be made at any time before the warrant expires.

Paragraph 50(1)(f) of the SD Act provides that this report must set out the number of applications for the extension of a computer access warrant that were made, and the number of extensions granted and refused (including reasons why applications were granted or refused) during the reporting period.

This information is presented in **Table 6**. In 2024–25, law enforcement agencies were issued 42 computer access warrants, an increase of 24 warrants on the 18 issued in 2023-24. No applications for a computer access warrants were refused by an issuing authority.

Table 6 also shows that 11 warrants were extended in 2024–25, compared to 16 warrants in 2023–24. The AFP advised that extensions were sought and granted for the continued and proportionate access to data held in target computers to investigate relevant offences.

Table 6: Number of computer access warrants issued, remote applications made, and extensions granted –paragraphs 50(1)(a), 50(1)(d), 50(1)(e) and 50(1)(f)[10]

Agency		Warrant Applications		Remote Applications		Extension of Warrants	
		23/24	24/25	23/24	24/25	23/24	24/25
ACIC	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
AFP	Made	13	22	-	-	11	11
	Refused	-	-	-	-	-	-
	Issued	13	22	-	-	11	11
LECC	Made	2	-	-	-	5	-
	Refused	-	-	-	-	-	-

[10] Agencies that did not apply for any computer access warrants are not included in Table 6.

Agency		Warrant Applications		Remote Applications		Extension of Warrants	
		23/24	24/25	23/24	24/25	23/24	24/25
NACC	Issued	2	-	-	-	5	-
	Made	2	3	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	3	-	-	-	-
NSW CC	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
WA Police	Made	-	16	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	16	-	-	-	-
TOTAL	**Made**	**18**	**42**	**-**	**-**	**16**	**11**
	Refused	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**18**	**42**	**-**	**-**	**16**	**11**

International assistance applications for computer access warrants

Subsection 27A(4) of the SD Act provides that a law enforcement officer (or another person on the officer's behalf), may apply for a computer access warrant when authorised under an international assistance authorisation, and the law enforcement officer suspects on reasonable grounds, that access to data held in a computer is necessary for the purpose of enabling evidence to be obtained of the commission of an international or foreign offence or the identity or locations of such an offender.

The Attorney-General may issue international assistance authorisations under section 15CC of the *Mutual Assistance in Criminal Matters Act 1987*, section 79B of the *International Criminal Court Act 2002* and section 32AA of the *International War Crimes Tribunals Act 1995*, if satisfied of the following:

- a foreign country, the International Criminal Court, or a war crimes tribunal has requested that the Attorney-General arrange for access to data held on a computer
- there is an investigation or proceeding underway within their jurisdiction (if the request is being made by a foreign country, the investigation must relate to a criminal matter involving an offence against the law of that foreign country that is punishable by a maximum penalty of at least three years imprisonment), and
- the requesting foreign country, the International Criminal Court, or a war crimes tribunal has given undertakings regarding:

- the information obtained via a computer access warrant only being used for the purposes for which it is communicated to the jurisdiction
- the destruction of the information obtained under the computer access warrant, and
- any other matter the Attorney-General considers appropriate.

Paragraphs 50(1)(aa) and 50(1)(ea) of the SD Act provide that this report must set out the number of international assistance applications made and refused (including the reasons for any refusal), and the number of warrants issued during the reporting period.

Where a computer access warrant was issued as a result of an international assistance application, paragraph 50(1)(ia) of the SD Act requires that this report list the offence (if any) under a law of the Commonwealth, a state or a territory that is of the same or substantially similar nature as the foreign offence being investigated under that computer access warrant.

In 2024–25, no law enforcement agencies applied for a computer access warrant as a result of an international assistance application. This is the same as in 2023–24.

Access to data in emergency circumstances

An appropriate authorising officer of a law enforcement agency may issue an emergency authorisation to authorise access to data held in a computer. An emergency authorisation may only be issued in urgent circumstances when it is not practicable to apply for a warrant and:

- there is an imminent risk of serious violence to a person or substantial damage to property (section 28)
- a recovery order in relation to a child is in force and the law enforcement order reasonably suspects that the circumstances are so urgent as to warrant the immediate use of a surveillance device (section 29), or
- there is a risk of loss of evidence for certain serious offences, such as drug offences, terrorism, espionage, sexual servitude, and aggravated people smuggling (section 30).

The appropriate authorising officer (or another person on their behalf) who gives an authorisation must apply to an eligible Judge or ART member for approval of the giving of the emergency authorisation within 48 hours of the authorisation being issued.

Paragraphs 50(1)(b) and 50(1)(e) provide that this report must set out the number of applications for emergency authorisations made and refused (including the reasons for any refusal) and the number of authorisations given during the reporting period.

In 2024–25, no law enforcement agencies made an emergency authorisation application for access to data held in a computer. This is the same as in 2023–24.

Chapter 4: Data Disruption Warrants

Applications for data disruption warrants

Section 27KA of the SD Act provides that a law enforcement officer of the AFP or the ACIC (or another person on the law enforcement officer's behalf) may apply for the issue of a data disruption warrant for the investigation of a 'relevant offence', which generally carry a maximum penalty of at least three years imprisonment. An application for a data disruption warrant must be endorsed by a senior officer within the agency with the relevant skills, knowledge and experience to make applications for the issue of a warrant and who has completed relevant internal training requirements.

A data disruption warrant must specify the things that are authorised under the warrant, which may include:

- entering premises for the purposes of executing the warrant
- using the target computer, a telecommunications facility, electronic equipment or data storage device in order to access data held in the target computer to determine whether the relevant data is covered by the warrant or to disrupt the relevant data, if doing so is likely to assist in frustrating the commission of the relevant offence
- adding, copying, deleting or altering data in the target computer if necessary to access the data to determine whether the relevant data is covered by the warrant or to disrupt the relevant data, if doing so is likely to assist in frustrating the commission of the relevant offence
- using any other computer if necessary to access or disrupt the data (and adding, copying, deleting or altering data on that computer if necessary)
- removing a computer from premises for the purposes of executing the warrant
- copying data to which access has been obtained that is relevant and covered by the warrant
- intercepting a communication in order to execute the warrant, and
- any other thing reasonably incidental to the above things.

Data disruption warrants do not authorise the addition, deletion or alteration of data, or anything that is likely to materially interfere with, interrupt, or obstruct, a communication in transit, or the lawful use by other persons of a computer, unless it is necessary to do things specified in the warrant. Data disruption warrants do not authorise material loss or damage to other persons lawfully using a computer unless the loss or damage is reasonably necessary, and proportionate, to do the things specified in the warrant. If the person executing the warrant becomes aware that a thing done under the warrant has caused material loss or damage to one or more persons lawfully using a computer, the chief officer must notify the Ombudsman within seven days after the person executing the warrant becomes aware.

Paragraphs 50(1)(a) and 50(1)(e) of the SD Act provide that this report must set out the number of applications for data disruption warrants made and refused (including reasons for any refusal), and the number of warrants issued during the reporting period.

Section 27KB of the SD Act permits a remote application for a data disruption warrant to be made by telephone, fax, email, or other means of communication if the law enforcement officer believes that it is impracticable to make the application in person. Paragraph 50(1)(d) of the SD Act provides that this report must set out the number of remote applications made during the reporting period.

Section 27KF of the SD Act provides that the law enforcement officer to whom a data disruption warrant was issued (or another person on the officer's behalf) may apply for an extension of the warrant for a period not exceeding 90 days after the warrant's original expiry date. This application may be made at any time before the warrant expires.

Paragraph 50(1)(f) of the SD Act provides that this report must set out the number of applications for the extension of a data disruption warrant that were made, and the number of extensions granted and refused (including reasons why applications were granted or refused) during the reporting period.

Paragraph 50(1)(eb) of the SD Act provides that this report must set out the kinds of offences targeted by data disruption warrants issued during the reporting period. This information is presented in **Table 7**.

In 2024–25, the AFP made four applications for data disruption warrants, compared to one in 2023-24. The AFP advised that the ART member refused one data disruption warrant on the basis that further information was required. The AFP then remade this application with the further information included, and the ART member subsequently issued the warrant.

The offences targeted by data disruption warrants included dishonestly obtaining or dealing in personal financial information, dealing in the proceeds of crime, and the unauthorised access, modification or impairment of data with the intent to commit fraud and espionage.

Table 7: Number of data disruption warrants issued, remote applications made, and extensions granted – paragraphs 50(1)(a), 50(1)(d), 50(1)(e) and 50(1)(f)

Agency		Warrant		Remote Applications		Extension of warrants	
		23/24	24/25	23/24	24/25	23/24	24/25
AFP	Made	1	5[11]	-	-	-	-
	Refused	-	1[12]	-	-	-	-
	Issued	1	4	-	-	-	-
TOTAL	**Made**	**1**	**5**	**-**	**-**	**-**	**-**
	Refused	**-**	**1**	**-**	**-**	**-**	**-**
	Issued	**1**	**4**	**-**	**-**	**-**	**-**

Data disruption in emergency circumstances

An appropriate authorising officer of the AFP or the ACIC may issue an emergency authorisation for disruption of data held in a computer. An emergency authorisation may only be issued in urgent circumstances when it is not practicable to apply for a warrant and there is an imminent risk of serious violence to a person or substantial damage to property (section 28).

The officer who gave the emergency authorisation must apply to an eligible Judge or ART member for approval of the giving of the emergency authorisation within 48 hours of the authorisation being issued.

Paragraphs 50(1)(b) and 50(1)(e) provide that this report must set out the number of applications for emergency authorisations made and refused (including the reasons for any refusal), and the number of authorisations given during the reporting period.

In 2024–25, no law enforcement agencies made an emergency authorisation application for disruption of data held in a computer. This is the same as in 2023–24.

[11] This includes two applications relating to the same offence and circumstances as one application was remade after initially being refused.
[12] A warrant relating to this offence was subsequently issued after the application was remade with further information.

Chapter 5: Network Activity Warrants

Applications for network activity warrants

Section 27KK of the SD Act provides that the chief officer of the AFP or the ACIC may apply for the issue of a network activity warrant in respect of a criminal network of individuals. A criminal network of individuals is an electronically linked group of individuals and can include individuals who use the same electronic service or communicate by electronic communications. Access to data must substantially assist in the collection of intelligence and be relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

A network activity warrant must specify the things that are authorised under the warrant, which may include:

- entering premises for the purposes of executing the warrant
- using the target computer, a telecommunications facility, electronic equipment or data storage device in order to access data held in the target computer to determine whether the relevant data is covered by the warrant
- adding, copying, deleting or altering data in the target computer if necessary to access the data to determine whether the relevant data is covered by the warrant
- using any other computer if necessary to access the data (and adding, copying, deleting or altering data on that computer if necessary)
- removing a computer from premises for the purposes of executing the warrant
- copying data to which access has been obtained that is relevant and covered by the warrant
- intercepting a communication in order to execute the warrant
- using a surveillance device for the purposes of doing any things specified in the warrant, and
- any other thing reasonably incidental to the above things.

Network activity warrants do not authorise the addition, deletion or alteration of data, or anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer, unless it is necessary to do the things specified in the warrant. Network activity warrants do not authorise anything that is likely to cause material loss or damage to other persons lawfully using a computer.

Section 27KL of the SD Act permits a remote application for a network activity warrant to be made by telephone, fax, email, or other means of communication if the chief officer of the AFP or the ACIC believes that it is impracticable to make the application in person.

Section 27KQ of the SD Act provides that the chief officer of the AFP or the ACIC may apply for an extension of the warrant for a period not exceeding 90 days after the warrant's original expiry date. This application may be made at any time before the warrant expires.

Subsection 50(1) of the SD Act provide that this report must set out, for the period:

- the number of applications for network activity warrants made and refused (including reasons for any refusal) (paragraphs 50(1)(a) and 50(1)(e))
- the number of warrants issued (paragraph 50(1)(a))
- the number of remote applications made (paragraph 50(1)(d))
- the number of applications for the extension of a network activity warrant that were made, and the number of extensions granted and refused (including reasons for any refusals) (paragraph 50(1)(f)), and
- the kinds of offences in relation to which information was obtained under a network activity warrant (paragraph 50(1)(ec)).

Table 8 shows the number of network activity warrants issued and refused, and the number of extensions. One warrant was issued in 2024–25, a decrease of one from the previous year. One warrant was refused in 2024–25, compared to zero in 2023–24.

In 2024–25, the AFP and the ACIC were granted seven extensions of network activity warrants. The AFP advised that its network activity warrant targeted serious organised criminal activity and drug offences. The ACIC advised that its network activity warrants targeted serious drug and money laundering offences.

Table 8: Number of network activity warrants issued, remote applications made, and extensions granted – paragraphs 50(1)(a), 50(1)(d), 50(1)(e) and 50(1)(f)

Agency		Warrant		Remote Applications		Extension of warrants[13]	
		23/24	24/25	23/24	24/25	23/24	24/25
ACIC	Made	-	-	-	-	4	4
	Refused	-	-	-	-	-	-
	Issued	-	-	-	-	4	4
AFP	Made	2	2	-	-	3	3
	Refused	-	1	-	-	-	-
	Issued	2	1	-	-	3	3
TOTAL	**Made**	**2**	**2**	**-**	**-**	**7**	**7**
	Refused	**-**	**1**	**-**	**-**	**-**	**-**
	Issued	**2**	**1**	**-**	**-**	**7**	**7**

[13] A warrant can be extended more than once.

Chapter 6: Effectiveness of the Surveillance Devices Act

Paragraph 50(1)(g) of the SD Act provides that this report must set out the number of arrests made during the reporting period, wholly or partly, on the basis of information obtained under a surveillance device or computer access warrant, an emergency authorisation, or a tracking device authorisation.

Paragraph 50(1)(i) of the SD Act requires that this report set out the number of prosecutions commenced during the reporting period, in which information obtained under a surveillance device or computer access warrant, emergency authorisation, or tracking device authorisation was given in evidence and the number of those prosecutions in which a person was found guilty (convictions).

Paragraph 50(1)(h) of the SD Act provides that this report must set out the number of instances during the reporting period in which the location and safe recovery of a child, to whom a recovery order related, was assisted, wholly or partly, on the basis of information obtained under a surveillance device or computer access warrant, emergency authorisation, or tracking device authorisation.

Collectively, this information can provide an indication of the effectiveness of the use of surveillance powers in the SD Act as a law enforcement tool.

This information is presented in **Table 9**. In 2024–25, information obtained through the use of these powers contributed to 271 arrests, 190 prosecutions, and 29 convictions.

Table 9: Number of arrests, safe recoveries, prosecutions, and convictions – paragraphs 50(1)(g), 50(1)(h) and 50(1)(i)[14]

Agency	Arrests		Safe recovery		Prosecutions		Convictions	
	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25
AFP	147	271	-	-	101	190	18	29
NACC	1[15]	-	-	-	1	-	-	-
TOTAL	**148**	**271**	**-**	**-**	**102**	**190**	**18**	**29**

Interpretive note

The information presented in **Table 9** should be interpreted with caution, particularly presuming a relationship between the number of arrests, prosecutions (which include committal proceedings), and convictions in a reporting period. An arrest recorded in one reporting period may not result in a prosecution or committal (if at all) until a later reporting period. Moreover, the number of arrests may not equate to the number of

[14] Agencies that did not make any arrests, safe recoveries, prosecutions or convictions under these provisions are not included in Table 9.
[15] This arrest was undertaken by the AFP. The arrest was made on the basis of information obtained by the use of a surveillance device warrant issued to the Commission.

charges laid (some or all of which may be prosecuted at a later time) as an arrested person may be prosecuted and convicted for a number of offences.

Further, the table may understate the effectiveness of these powers.

- In some cases, prosecutions may be initiated and convictions recorded without the need to give information obtained through use of these powers in evidence. In many cases, the weight of evidence obtained through use of these powers results in defendants entering guilty pleas, thereby removing the need for the information to be introduced into evidence.
- Data disruption warrants are intended for circumstances where a prosecution is not feasible and do not lead to arrest, prosecutions or convictions. The AFP has nevertheless reported that these warrants are effective and that they have allowed them to successfully frustrate the commission of serious offences online.
- The intelligence obtained by using a network activity warrant cannot generally be used by the prosecution in evidence, and does not directly lead to convictions. Nevertheless, agencies report that the use of these powers effectively enabled investigators to identify persons involved in, and the infrastructure of, organised criminal activities.

The Independent National Security Legislation Monitor, in its review of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, found that network activity warrants and data disruption warrants were effective but recommended that the public annual reporting requirements be amended to provide further evidence of their effectiveness. For example, by including a statement that describes how the use of data disruption and network activity warrants has enhanced agencies' ability to investigate, disrupt and prosecute serious crimes (recommendation 20). The Government is considering its response to the Review.

Chapter 7: Further Information

Further information about the *Surveillance Devices Act 2004* can be obtained by contacting the Department of Home Affairs:

Electronic Surveillance Section

Department of Home Affairs

PO Box 25

Belconnen ACT 2616

ElectronicSurveillance@homeaffairs.gov.au

Previous *Surveillance Devices Act 2004* Annual Reports can be accessed online at: www.homeaffairs.gov.au.

Appendix A: List of Tables

Notes