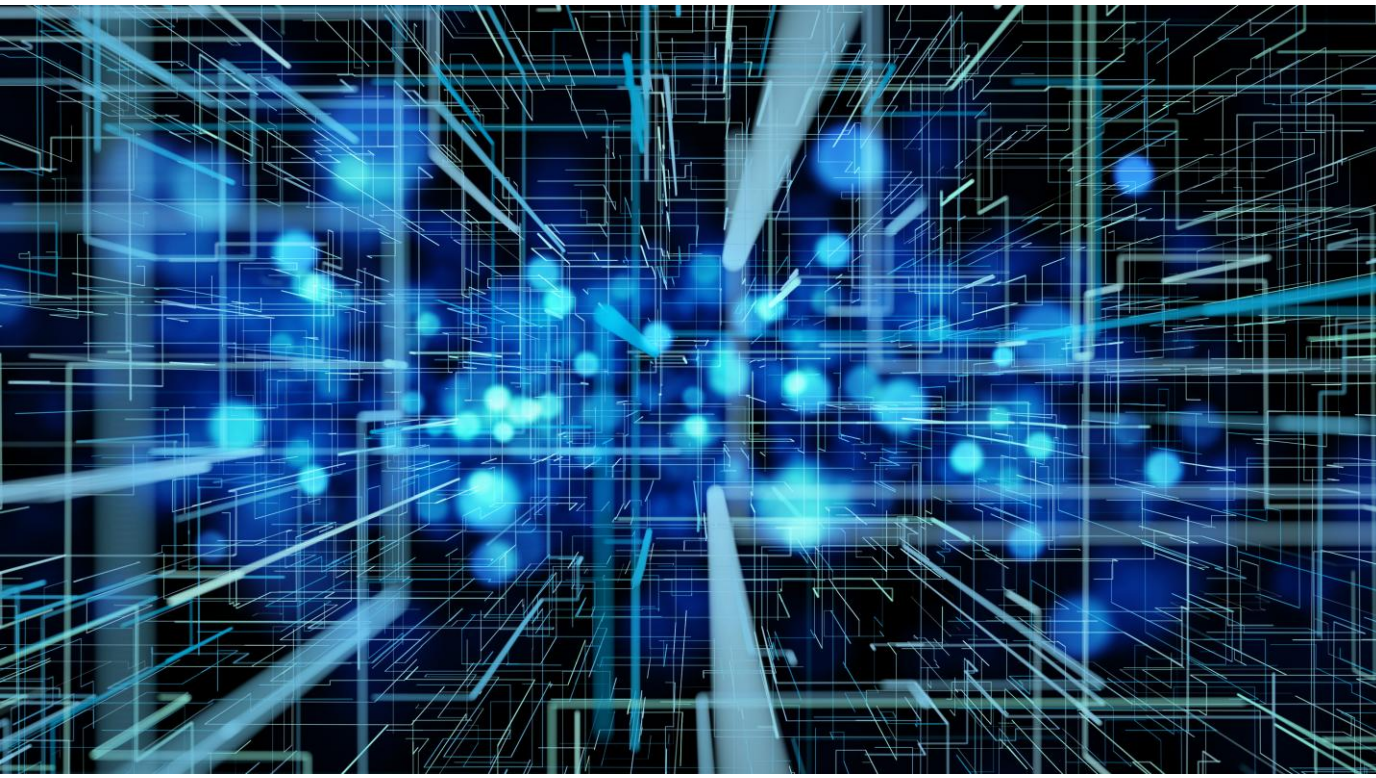
Australian Government
Department of Home Affairs



Telecommunications (Interception and Access) Act 1979 and Part 15 of the *Telecommunications Act 1997*

Annual Report 2024–25

Contact us

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

Office of the Communications Access Coordinator
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Table of Contents

Abbreviations **1**

Key 2024–25 statistics 3

Chapter 1: Introduction **5**

Access to the content of a communication 5

Telecommunications data 5

Chapter 2: Telecommunications interception **7**

Serious offences 7

Eligibility to issue an interception warrant 15

Issuing of interception warrants 16

Applications for interception warrants 16

Warrants that authorise entry onto premises 18

Conditions or restrictions on warrants 19

Effectiveness of interception warrants 19

Named person warrants 25

B-party warrants 29

Duration of warrants 30

Final renewals 32

Eligible warrants 33

Interception without a warrant 34

International assistance 34

Number of interceptions carried out on behalf of other agencies 35

Telecommunications interception expenditure 35

Emergency service facilities 37

Safeguards and reporting requirements on interception powers 38

Ombudsman – Inspection of telecommunications records conducted in 2024–25 39

Overview 39

Good practices 40

What can agencies improve on? 41

Chapter 3: Stored communications **48**

Applications for stored communications warrants 48

Conditions or restrictions on stored communications warrants 50

Effectiveness of stored communications warrants 50

Preservation notices 51

International assistance 53

Ombudsman inspection report 54

Chapter 4: Telecommunications data **55**

Existing data – enforcement of the criminal law 55

Existing data – assist in locating a missing person 57
Existing data – enforcement of a law imposing a pecuniary penalty or protecting public revenue 58
Prospective data – authorisations 58
Data authorisations for foreign law enforcement 60
Offences for which authorisations were made 61
Age of data under disclosure 74
Types of data retained 76
Journalist information warrants 77
Industry estimated cost of implementing data retention 78

Chapter 5: International production orders 79

Agencies report on applications for international production orders 79
Applications for enforcement of the criminal law 79
Applications relating to a Part 5.3 supervisory orders 80
Applications for each designated international agreement 80
The Australian Designated Authority report 81
International production orders given by the Australian Designated Authority 81
International production orders cancelled by the Australian Designated Authority 82
Objections received by the Australian Designated Authority 83
Effectiveness of international production orders 84
Offences for which international production orders were made 85
International production orders revoked by the chief officer 86

Chapter 6: Industry assistance 87

Requests and notices 87
Use of industry assistance 88
Offences enforced through industry assistance 89
Oversight of industry assistance powers 90

Chapter 7: Further information 91

Appendix A: Lists of tables and figures 92

Appendix B: Interception agencies under the TIA Act 96

Appendix C: Categories of serious offences under the TIA Act 96

Appendix D: Updated figures for previous reporting periods 98

ASIC 2023–2024 98
IBAC 2023–2024 99
NT Police 2023–2024 100
TAS Police 2023–2024 103
WA Police 2023–2024 104

Abbreviations

Abbreviation	Term
AAT	Administrative Appeals Tribunal
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACT Integrity Commission	Australian Capital Territory Integrity Commission
AFP	Australian Federal Police
ART	Administrative Review Tribunal
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASIC	Australian Securities and Investments Commission
ASD	Australian Signals Directorate
AGD	Attorney-General's Department
Ombudsman	Commonwealth Ombudsman
CS NSW	Corrective Services New South Wales
CCC (WA)	Corruption and Crime Commission (Western Australia)
Home Affairs	Department of Home Affairs
IBAC	Independent Broad-based Anti-Corruption Commission (Victoria)
ICAC (NSW)	Independent Commission Against Corruption (New South Wales)
ICAC (SA)	Independent Commission Against Corruption (South Australia)
IGIS	Inspector-General of Intelligence and Security
IPO	International Production Order
JIW	Journalist Information Warrant
LECC	Law Enforcement Conduct Commission
NACC	National Anti-Corruption Commission

Abbreviation	Term
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police Force
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PIA	Public Interest Advocate
QLD CCC	Queensland Corruption and Crime Commission
QLD Police	Queensland Police Service
SA Police	South Australia Police
TAS Police	Tasmania Police
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
TCN	Technical Capability Notice
Telecommunications Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
VIC Police	Victoria Police
WA Police	Western Australia Police Force

Key 2024–25 statistics

- There were 2,726 interception warrants issued to 17 interception agencies. This is a decrease of 281 from the 3,007 issued in 2023–24.
- Six applications for interception warrants were refused. This is a decrease of 10 from the 16 refused in 2023–24.
- The majority of serious offences specified in interception warrants issued were serious drug offences (1,088), followed by serious personal injury (503) and murder (278).
- Information obtained under interception warrants was used in 2,156 arrests 1,947 prosecutions and 1,004 convictions.
- There were 706 stored communications warrants issued to 10 criminal law-enforcement agencies. This is a decrease of 32 from the 738 issued in 2024–25.
- Two applications for stored communications warrants were refused. This is an increase of one from 2023–24.
- Information obtained under stored communications warrants was used in 319 arrests, 236 proceedings, and 177 convictions. This is an increase of 36 on the 283 arrests made in 2023–24, an increase of 26 on the 210 proceedings conducted in 2023–24 and an increase of 19 on the 158 convictions obtained in 2023–24.
- There were 364,868 authorisations made by 21 enforcement agencies for the disclosure of existing telecommunications data. This is an increase of 4,920 authorisations on the 359,948 authorisations made in 2023–24.[1] Of these, 357,864 were made to enforce the criminal law.
- Authorisations for existing telecommunications data covered a range of crimes, including 59,076 authorisations for illicit drugs offences, 42,843 for abduction and 38,452 authorisations for unlawful entry.
- There were 49,482 authorisations made by 20 criminal law-enforcement agencies for disclosure of prospective telecommunications data. This is a decrease of 3,381 from the 52,863 authorisations made in 2023–24.
- There were 100 international production order (IPO) applications issued to an issuing authority in relation to stored communications. Five IPO applications were issued to an issuing authority in relation to telecommunications data. These statistics were nil in 2023–24 as work was still on foot to operationalise the IPO framework.
- Protected information obtained under IPOs was used in seven arrests, nine proceedings and two convictions.
- One journalist information warrant was issued to an enforcement agency in 2024–25. This is an increase of one from 2023–24.
- There were 58 technical assistance requests given to designated communications providers by five interception agencies. This is a decrease of two from the 60 given in 2023–24.

[1] This includes adjustments made to the 2023–24 Annual Report (see Appendix D).

- There were no technical assistance notices given in this reporting period. This is a decrease of two from 2023–24. No technical capability notices were given in this reporting period.

Chapter 1: Introduction

The 2024–25 Annual Report under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and Part 15 of the *Telecommunications Act 1997* (Telecommunications Act) sets out the extent to and circumstances in which eligible Commonwealth, state and territory agencies have used the powers available under the TIA Act and Part 15 of the Telecommunications Act between 1 July 2024 and 30 June 2025.

The TIA Act provides a legal framework for national security and law enforcement agencies to access information held by communications providers to investigate criminal offences and other activities that threaten the safety and security of Australians. The access that may be sought under the TIA Act includes access to telecommunications data, stored communications, and the interception of communications. Law enforcement agencies' use of warrants and authorisations related to these powers is independently overseen by the Commonwealth Ombudsman (the Ombudsman) and/or equivalent state bodies.

Part 15 of the Telecommunications Act provides a framework for national security and law enforcement agencies to obtain technical assistance from designated communications providers. The industry assistance framework does not replace the need for agencies to obtain a warrant or authorisation to access information.

Access to the content of a communication

Accessing the content or the substance of a communication — for instance, the message written in an email, the discussion between two parties to a phone call, the subject line of an email or a private social media post — without the knowledge of the person making the communications is highly intrusive. Except in limited circumstances, such as a life-threatening emergency, interception of communications or access to stored communications can only occur under the authority of a warrant. Such access is subject to strict safeguards, including oversight, record-keeping and reporting obligations. This Annual Report is an important part of this accountability framework, as it provides the public with information about how these powers are used.

Accessing communications is an effective investigative tool that supports and complements information obtained by other methods.

Telecommunications data

Another critical tool available under the TIA Act is access to telecommunications data. Telecommunications data is information about a communication (such as the phone numbers of the people who called each other, how long they spoke to each other, the email address from which a message was sent and the time the message was sent) or the telecommunications service to which a person has subscribed, but not the content of the communication.

Telecommunications data is often the first source of lead information for investigations. The data can help eliminate potential suspects and to consider whether more intrusive investigative tools are required. For example, an examination of call charge records can show that an individual may not have had contact with suspects being investigated.

Telecommunications data gives agencies a method for identifying users of a telecommunication service. It can also be used to demonstrate an association between people, or to prove that two or more people contacted each other at a critical point in time.

Enforcement agencies can access existing telecommunications data. Existing data, also known as historic data, is information that is already in existence when an authorisation for disclosure is received by a carrier.

Comparatively, only criminal law-enforcement agencies can access prospective telecommunications data to assist in the investigation of offences punishable by a maximum term of at least three years' imprisonment.[2] Prospective data is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

The Minister for Home Affairs may declare additional agencies in limited circumstances for a period of 40 sitting days of Parliament. In the 2024–25 reporting period, the Australian Capital Territory Integrity Commission (ACT Integrity Commission) was declared as a criminal law-enforcement agency, and Corrective Services NSW, as part of the New South Wales Department of Communities and Justice, was declared as an enforcement agency.

[2] 'Criminal law-enforcement agencies' are set out in section 110A of the TIA Act. These agencies include all interception agencies as well as Home Affairs, ASIC, and the ACCC.

Chapter 2: Telecommunications interception

The interception of communications is regulated by Chapter 2 of the TIA Act. Section 7 of the TIA Act prohibits communications from being intercepted while they are passing over an Australian telecommunications system, except in limited circumstances set out in the TIA Act. This protects the privacy of the communications of people who use the Australian telecommunications network.

Definition

The term **'interception agency'** is defined in section 5 of the TIA Act, and covers the AFP and state and territory police forces, the ACIC and state and territory crime commissions, and the NACC and state and territory integrity agencies. Only interception agencies are eligible to apply under Part 2-5 of the TIA Act for an interception warrant

The TIA Act provides for several types of warrants that enable interception of communications passing over a telecommunications system (for example, a warrant to authorise the interception of a particular telephone number, or a warrant to authorise the interception of multiple services that relate to a named person). During the reporting period, interception warrants were available to 17 Commonwealth, state and territory agencies.

Definition

Section 6 of the TIA Act provides that the **interception** of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

Serious offences

Interception warrants can be obtained to investigate serious offences as set out in section 5D of the TIA Act. Serious offences generally carry a maximum penalty of at least seven years' imprisonment. There are exceptions to this threshold. Interception warrants may be available for offences with a maximum penalty of less than seven years' imprisonment that are of a serious nature, or involve the use of the telecommunications system, such as money laundering. In these circumstances interception of a communication is critical to enable the collection of evidence and its availability may be key to resolving an investigation.

Serious offences for which interception warrants can be obtained under the TIA Act include murder, kidnapping, serious drug offences, espionage, terrorism, and offences involving child abuse, money laundering, and organised crime.

Paragraphs 100(1)(f)–(g) and 100(2)(f)–(g) of the TIA Act provide that this report must set out the categories of serious offences specified in interception warrants issued during the year, and in relation to each of those categories, how many serious offences in that category were so specified.

This information is presented in **Tables 1, 1A, 1B and 1C**. Consistent with previous years, in 2024–25 the majority of warrants obtained were to assist with investigations into serious drug offences (1,088 warrants). Serious personal injury was specified in 503 warrants and 278 warrants related to murder. The total number of offences is typically larger than the total number of warrants issued, as a warrant can be issued to investigate more than one serious offence.

Information about offences covered under each category is set out in **Appendix C**.

Table 1: Categories of serious offences specified in interception warrants – paragraphs100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	Commonwealth Agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Abuse of public office[3]	9	-	-	**9**
Aiding a prisoner to escape/attempt to escape from criminal detention	3	-	-	**3**
Appropriating property of a Commonwealth entity[4]	1	-	-	**1**
Assisting person to escape or dispose of proceeds	-	30	-	**30**
Bribery, corruption and dishonesty offences	2	-	60	**62**
Child abuse offences	4	88	-	**92**
Conspire/aid/abet/serious offence	4	21	1	**26**
Corrupting benefits given to, or received by, a Commonwealth public official[5]	-	1	-	**1**
Cybercrime offences	3	3	-	**6**
False testimony in judicial proceeding	-	-	6	**6**
Foreign incursions and recruitment	4	-	-	**4**
Foreign interference offences	9	-	-	**9**
General dishonesty[6]	2	19	-	**21**
Kidnapping	3	74	-	**77**

[3] Last year all offences listed under subsection 5D(8) (which included abuse of public office, giving or receiving corrupting benefits by Commonwealth public officials, dishonestly appropriating Commonwealth property, general dishonesty, impersonation of an official by another official, and perverting the course of justice in respect of the International Criminal Court) were recorded in a single line item as 'offences against the administration of justice or by government officials'.
[4] Last year all offences under subsection 5D(8) were recorded in a single line item as 'offences against the administration of justice or by government officials'.
[5] Last year all offences under subsection 5D(8) were recorded in a single line item as 'offences against the administration of justice or by government officials'.

[6] Last year all offences under subsection 5D(8) were recorded in a single line item as 'offences against the administration of justice or by government officials'.

Categories of offences	Commonwealth Agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Loss of life	7	123	-	**130**
Money laundering	53	39	16	**108**
Murder	17	258	3	**278**
Offences involving planning and organisation	17	127	-	**144**
Organised crime	6	38	3	**47**
People smuggling and related offences	4	-	-	**4**
Serious arson	-	109	-	**109**
Serious damage to property	-	1	-	**1**
Serious drug offences	340	732	16	**1,088**
Serious fraud	11	57	4	**72**
Serious loss of revenue	5	5	-	**10**
Serious personal Injury	17	486	-	**503**
Telecommunications offences	-	4	-	**4**
Terrorism offences	59	2	-	**61**
TOTAL	**580**	**2,217**	**109**	**2,906**

Table 1A: Commonwealth agencies – Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	ACIC[7]	AFP	NACC	TOTAL
Abuse of public office[8]	-	-	9	**9**
Aiding a prisoner to escape/attempt to escape from criminal detention	-	3	-	**3**
Appropriating property of a Commonwealth entity[9]	-	1	-	**1**
Bribery, corruption and dishonesty offences	-	2	-	**2**
Child abuse offences	-	4	-	**4**
Conspire/aid/abet/serious offence	-	-	4	**4**
Cybercrime offences	-	3	-	**3**
Foreign incursions and recruitment	-	4	-	**4**
Foreign interference offences	-	9	-	**9**
General dishonesty[10]	-	-	2	**2**
Kidnapping	-	3	-	**3**
Loss of life	-	7	-	**7**
Money laundering	-	53	-	**53**
Murder	-	17	-	**17**
Offences involving planning and organisation	-	17	-	**17**

[7] The ACIC has commenced reporting authorisations against specific offence categories, rather than the broader 'special ACIC investigation' category, to achieve a more precise background.
[8] Last year all offences under subsection 5D(8) (which included abuse of public office, giving or receiving corrupting benefits by Commonwealth public officials, dishonestly appropriating Commonwealth property, general dishonesty, impersonation of an official by another official, and perverting the course of justice in respect of the International Criminal Court) were recorded in a single line item as 'offences against the administration of justice or by government officials'.
[9] Last year all offences under subsection 5D(8) were recorded in a single line item as 'offences against the administration of justice or by government officials'.
[10] Last year all offences under subsection 5D(8) were recorded in a single line item as 'offences against the administration of justice or by government officials'.

Categories of offences	ACIC[7]	AFP	NACC	TOTAL
Organised crime	-	6	-	**6**
People smuggling and related offences	-	4	-	**4**
Serious drug offences	2	338	-	**340**
Serious fraud	-	7	4	**11**
Serious loss of revenue	-	5	-	**5**
Serious personal Injury	-	17	-	**17**
Terrorism offences	-	59	-	**59**
TOTAL	**2**	**559**	**19**	**580**

Table 1B: State and Territory Police – Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Assisting person to escape or dispose of proceeds	30	-	-	-	-	-	-	**30**
Child abuse offences	70	-	-	7	1	6	4	**88**
Conspire/aid/abet serious offence	19	-	-	-	-	-	2	**21**
Corrupting benefits given to, or received by, a Commonwealth public official[11]	-	-	-	-	-	1	-	**1**
Cybercrime offences	3	-	-	-	-	-	-	**3**
General dishonesty[12]	-	-	-	-	-	-	19	**19**

[11] Last year all offences under subsection 5D(8) (which included abuse of public office, giving or receiving corrupting benefits by Commonwealth public officials, dishonestly appropriating Commonwealth property, general dishonesty, impersonation of an official by another official, and perverting the course of justice in respect of the International Criminal Court) were recorded in a single line item as 'offences against the administration of justice or by government officials'.
[12] Last year all offences under subsection 5D(8) were recorded in a single line item as 'offences against the administration of justice or by government officials.

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Kidnapping	74	-	-	-	-	-	-	**74**
Loss of life	66	1	28	-	1	20	7	**123**
Money laundering	26	-	2	-	-	5	6	**39**
Murder	175	-	12	13	-	37	21	**258**
Offences involving planning and organisation	121	-	6	-	-	-	-	**127**
Organised crime	37	-	-	-	-	1	-	**38**
Serious arson	92	-	-	7	1	6	3	**109**
Serious damage to property	-	-	-	-	-	1	-	**1**
Serious drug offences	418	23	142	10	7	27	105	**732**
Serious fraud	47	-	1	-	-	4	5	**57**
Serious loss of revenue	-	1	-	-	-	4	-	**5**
Serious personal Injury	416	-	27	1	-	18	24	**486**
Telecommunications offences	4	-	-	-	-	-	-	**4**
Terrorism offences	2	-	-	-	-	-	-	**2**
TOTAL	**1,600**	**25**	**218**	**38**	**10**	**130**	196	**2,217**

Table 1C: State and Territory Integrity Agencies – Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Bribery, corruption and dishonesty offences	8	13	6	8	15	-	10	**60**
Conspire/aid/abet serious offence	-	1	-	-	-	-	-	**1**
False testimony in judicial proceeding	-	-	-	-	6	-	-	**6**
Money laundering	-	2	-	-	-	11	3	**16**

Categories of offences	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Murder	-	-	-	-	-	3	-	**3**
Organised crime	-	-	-	-	-	3	-	**3**
Serious drug offences	-	-	-	-	-	13	3	**16**
Serious fraud	-	4	-	-	-	-	-	**4**
TOTAL	**8**	**20**	**6**	**8**	**21**	**30**	**16**	**109**

Eligibility to issue an interception warrant

The Administrative Review Tribunal (ART) commenced on 14 October 2024, replacing the former Administrative Appeals Tribunal (AAT). Previously, eligible judges or nominated members of the AAT were eligible to issue warrants. The TIA 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. In the reporting period, eligible judges were members of the:

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

Persons who hold one of the following appointments to the ART may be nominated by the Attorney-General to issue warrants under Part 2-5 of the TIA Act:

- Deputy President
- senior member (of any level), or
- general member.

Before issuing an interception warrant the issuing authority must take into account matters including:

- the gravity of the conduct of the offence/s being investigated
- how the privacy of any person would be interfered with
- how much the interception would be likely to assist with the investigation, and
- the extent to which other methods of investigating the offence are available to the agency.

Paragraph 103(ab) of the TIA Act provides that this report must contain information about the availability of judges to issue warrants under Part 2-5 and the extent to which nominated ART members have been used for that purpose.

This information is presented in **Table 2**. Over the 2024–25 reporting period, there were 117 issuing authorities for interception warrants.

Table 2: Federal Court judges, Federal Circuit and Family Court judges, and nominated ART member eligible to Issue interception warrants – paragraph 103(ab)

Issuing authority	Number eligible
Federal Court judges	21
Federal Circuit and Family Court judges	44
Nominated AAT/ART members	52
TOTAL	**117**

Issuing of interception warrants

Table 3 states which issuing authorities considered applications for warrants made by each interception agency during 2024–25. In 2024–25, nominated ART members considered 78 per cent of total interception warrant applications made.

Table 3: Interception warrant applications considered by Federal Court judges, Federal Circuit and Family Court judges, and nominated ART members[13]

Agency	Issuing authority			
	Federal Court judges	Federal Circuit and Family Court judges	Nominated ART members	TOTAL
ACIC	-	-	1	**1**
AFP	-	120	346	**466**
CCC (WA)	-	8	-	**8**
IBAC	-	-	11	**11**
ICAC (NSW)	-	-	6	**6**
ICAC (SA)	-	-	9	**9**
LECC	-	-	21	**21**
NACC	9	-	-	**9**
NSW CC	-	-	22	**22**
NSW Police	-	54	1,548	**1,602**
NT Police	-	25	-	**25**
QLD CCC	-	10	-	**10**
QLD Police	-	184	34	**218**
SA Police	-	-	22	**22**
TAS Police	-	-	10	**10**
VIC Police	-	-	110	**110**
WA Police	-	182	-	**182**
TOTAL	**9**	**583**	**2,140**	**2,732**

Applications for interception warrants

Paragraphs 100(1)(a)–(c) and 100(2)(a)–(c) of the TIA Act provide that this report must set out the relevant statistics about standard applications, telephone applications and renewal applications for interception warrants made by agencies during the year.

This information is presented in **Table 4**. In 2024–25, agencies were issued 2,726 interception warrants, a decrease of 281 from 2023–24, where 3,007 interception warrants were issued. In 2024–25, five telephone applications for warrants were issued. This was a

[13] The telephone and renewal applications made for interception warrants are a subset of the total warrant applications made for each agency.

decrease of six from the 11 issued in 2023–24. In 2024–25, 400 renewals of interception warrants were issued. This is a decrease of 130 from the 530 issued in 2023–24.

Table 4: Applications, telephone applications and renewal applications for interception warrants[14] – paragraphs 100(1)(a)–(c)

Agency	Status of Application	Applications for warrants		Telephone applications for warrants		Renewal applications	
		23/24	24/25	23/24	24/25	23/24	24/25
ACIC	Made	11	1	-	-	3	-
	Refused	1	-	-	-	-	-
	Issued	10	1	-	-	3	-
AFP	Made	466	466	-	-	137	111
	Refused	3	-	-	-	-	-
	Issued	463	466	-	-	137	111
CCC (WA)	Made	4	8	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	4	8	-	-	1	-
IBAC	Made	8	11	-	-	-	6
	Refused	-	-	-	-	-	-
	Issued	8	11	-	-	-	6
ICAC (NSW)	Made	-	6	-	-	-	4
	Refused	-	-	-	-	-	-
	Issued	-	6	-	-	-	4
ICAC (SA)	Made	-	9	-	-	-	1
	Refused	-	1	-	-	-	-
	Issued	-	8	-	-	-	1
LECC	Made	19	21	-	-	12	10
	Refused	-	-	-	-	-	-
	Issued	19	21	-	-	12	10
NACC	Made	13	9	2	-	2	2
	Refused	-	-	-	-	-	-
	Issued	13	9	2	-	2	2
NSW CCC	Made	10	22	-	-	3	4
	Refused	-	-	-	-	-	-
	Issued	10	22	-	-	3	4

[14] The telephone applications and renewal applications made, refused and issued for interception warrants are a subset of the total warrants made, refused and issued for each agency.

Agency	Status of Application	Applications for warrants		Telephone applications for warrants		Renewal applications	
		23/24	24/25	23/24	24/25	23/24	24/25
NSW Police	Made	1,786	1,602	9	5	306	202
	Refused	4	2	-	-	-	-
	Issued	1,782	1,600	9	5	306	202
NT Police	Made	27	25	-	-	-	2
	Refused	-	-	-	-	-	-
	Issued	27	25	-	-	-	2
QLD CCC	Made	20	10	-	-	9	5
	Refused	1	-	-	-	-	-
	Issued	19	10	-	-	9	5
QLD Police	Made	231	218	-	-	36	21
	Refused	6	3	-	-	1	-
	Issued	225	215	-	-	35	21
SA Police	Made	20	22	-	-	3	5
	Refused	-	-	-	-	-	-
	Issued	20	22	-	-	3	5
TAS Police	Made	7	10	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	7	10	-	-	-	-
VIC Police	Made	127	110	-	-	19	16
	Refused	1	-	-	-	-	-
	Issued	126	110	-	-	19	16
WA Police	Made	274	182	-	-	-	11
	Refused	-	-	-	-	-	-
	Issued	274	182	-	-	-	11
TOTAL	**Made**	**3,023**	**2,732**	**11**	**5**	**531**	**400**
	Refused	**16**	**6**	**-**	**-**	**1**	**-**
	Issued	**3,007**	**2,726**	**11**	**5**	**530**	**400**

Warrants that authorise entry onto premises

The TIA Act provides that an issuing authority can issue an interception warrant that authorises entry on premises. An issuing authority can only issue such a warrant if satisfied that it would be impracticable or inappropriate to intercept communications other than by use of equipment installed on those premises.

Paragraphs 100(1)(d) and 100(2)(d) of the TIA Act provide that this report must set out the relevant statistics about applications for interception warrants made by an agency during the year that included a request to authorise entry onto premises.

In 2024–25, no warrants authorising entry on premises were issued. This is consistent with 2023–24.

Conditions or restrictions on warrants

Issuing authorities can place conditions or restrictions on an interception warrant. For example, a condition or restriction may limit the ability for the agency to use or communicate the information obtained under the warrant, or restrict when interceptions may occur.

Paragraphs 100(1)(e) and 100(2)(e) of the TIA Act provide that this report must set out how many interception warrants issued during the reporting period specified conditions or restrictions relating to interceptions under the warrants.

This information is presented in **Table 5**. In 2024–25, 6 interception warrants were issued with a condition or restriction. This is a decrease of two compared to the eight issued in 2023–24.

Table 5: Interception warrants issued with specific conditions or restrictions – paragraphs 100(1)(e) and 100(2)(e)

Agency	Telecommunications interception warrants issued specifying conditions or restrictions	
	23/24	24/25
AFP	-	2
ICAC (SA)	-	1
NACC	1	-
NSW CC	-	1
NSW Police	7	-
TAS Police	-	1
WA Police	-	1
TOTAL	**8**	**6**

Effectiveness of interception warrants

Paragraphs 102(1)(a) and 102(2)(a) of the TIA Act provide that this report must set out for each agency how many arrests were made during that year in connection with the performance of the agency's functions, and on the basis of information that was, or included, lawfully intercepted information.

Agencies also separately report on the number of times lawfully intercepted information derived from their warrants culminated in an arrest by another agency. This removed the

risk that arrest numbers will be duplicated due to multiple agencies reporting on the same arrest. This also shows the outcomes from agencies that do not have arrest powers, but lawfully intercepted information derived from their warrants ultimately leads to an arrest by another agency.

Paragraphs 102(1)(b)–(c) and 102(2)(b)–(c) of the TIA Act provide that this report must set out the categories of prescribed offences proceeding by way of prosecutions which ended during that year.

This information is provided in **Tables 6, 7 and 8**. In 2024–25, there were 2,156 arrests made as a result of lawfully intercepted information (comprising 1,685 arrests by the agency to whom the warrant was issued, and 471 arrests by another agency). There were also 1,947 prosecutions and 1,004 convictions where lawfully intercepted material was given in evidence.

The information provided in this section should be interpreted with some caution, particularly in presuming a relationship between the number of arrests, prosecutions and convictions in a reporting period. An arrest recorded in one reporting period may not result in a prosecution until a later reporting period. Any resulting conviction could be recorded in that, or a subsequent reporting period. Additionally, one arrest may result in prosecution or conviction for a number of offences, some or all of which may occur at a later time.

The statistics may also understate the effectiveness of interception, as prosecutions may be initiated or convictions entered without the need to give intercepted information in evidence. In particular, agencies continue to report that telecommunications interception effectively enables investigators to identify persons involved in, and the infrastructure of, organised criminal activities. In some cases, the weight of evidence obtained through telecommunications interception results in defendants entering guilty pleas, eliminating the need for intercepted information to be admitted into evidence.

For Tables 7 and 8, the total number of offences is typically larger than the total number of warrants issued, as a warrant can be issued to investigate more than one serious offence.

Table 6: Arrests on the basis of lawfully intercepted information – paragraphs 102(1)(a) and 102(2)(a)

Agency	23/24		24/25	
	Number of arrests on the basis of lawfully obtained information provided by the agency	Number of times lawfully intercepted information culminated in arrest by another agency	Number of arrests on the basis of lawfully obtained information provided by the agency	Number of times lawfully intercepted information culminated in arrest by another agency
AFP	91	91	158	298
IBAC	-	-	-	2
NACC	1	1	-	-
NSW CC	-	78	-	39
NSW Police	749	27	1,127	49
NT Police	43	13	**-**	**-**
QLD CCC	3	-	4	1
QLD Police	255	-	211	-
SA Police	19	1	12	-
TAS Police	4	4	6	**-**
VIC Police	174	38	144	82
WA Police	-	-	23	-
TOTAL	**1,339**	**253**	**1,685**	**471**

Table 7: Prosecutions per offence category in which lawfully intercepted information was given in evidence – paragraphs 102(1)(b)–(c) and 102(2)(b)–(c)

Category	ACIC	AFP	ICAC (NSW)	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Abuse of public office	-	1	-	-	-	-	-	-	-	-	-	**1**
Ancillary offences	-	-	-	-	-	-	-	-	-	1	-	**1**
Assisting to escape or dispose of proceeds	-	3	-	-	-	-	-	-	-	-	-	**3**
Bribery, corruption or dishonesty offences	-	3	-	-	-	-	2	-	-	-	-	**5**
Cartel offences	-	4	-	-	-	-	-	-	-	-	-	**4**
Child abuse offences	-	3	-	-	50	-	-	-	-	-	-	**53**
Conspire/aid/abet serious offence	-	13	-	3	3	-	-	-	-	3	-	**22**
Corrupting benefits given to, or received by, a Commonwealth public official	-	2	-	-	-	-	-	-	-	-	-	**2**
Destroying evidence	-	2	-	-	-	-	-	-	-	-	-	**2**
Espionage	-	2	-	-	-	-	-	-	-	-	-	**2**
General dishonesty	-	-	-	-	-	-	-	3	-	2	-	**5**
Kidnapping	-	-	-	-	4	-	-	-	3	-	-	**7**
Loss of life	-	3	-	-	-	-	-	-	-	1	-	**4**
Money laundering	-	13	-	16	34	-	-	1	2	-	-	**66**
Murder	-	1	-	2	56	-	-	-	3	23	-	**85**
Offences involving planning and organisation	-	8	-	-	36	-	-	-	-	-	-	**44**
Organised crime	-	21	-	3	-	-	-	-	-	29	-	**53**
Other offences punishable by three years to life	-	13	1	23	375	-	-	51	-	-	-	**463**

Category	ACIC	AFP	ICAC (NSW)	NSW CC	NSW Police	NT Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
People smuggling and related offences	-	2	-	1	-	-	-	-	-	-	-	**3**
Serious arson	-	3	-	-	17	-	-	-	-	2	1	**23**
Serious damage to property	-	2	-	-	2	-	-	-	-	24	-	**28**
Serious drug offences	1	99	-	18	659	1	-	-	16	-	19	**813**
Serious fraud	-	-	-	-	57	-	-	2	-	-	1	**60**
Serious loss of revenue	-	2	-	-	-	-	-	-	-	-	-	**2**
Serious personal injury	-	4	-	-	143	-	-	-	3	5	1	**156**
Telecommunication offences	-	2	-	-	-	-	-	-	-	-	-	**2**
Trafficking in prescribed substances	-	20	-	-	1	-	-	16	-	-	1	**38**
TOTAL	**1**	**226**	**1**	**66**	**1,437**	**1**	**2**	**73**	**27**	**90**	**23**	**1,947**

Table 8: Convictions per offence category in which lawfully intercepted information was given in evidence – paragraphs 102(1)(b)–(c) and 102(2)(b)–(c)

Category	ACIC	AFP	ICAC (NSW)	ICAC (SA)	NSW CC	NSW Police	QLD Police	SA Police	VIC Police	TOTAL
Ancillary offences	-	-	-	-	-	-	-	-	1	**1**
Bribery, corruption or dishonesty offences	-	2	-	1	-	-	-	-	-	**3**
Child abuse offences	-	2	-	-	-	14	-	-	-	**16**
Conspire/aid/abet serious offence	-	2	-	-	-	2	-	-	-	**4**
General dishonesty	-	-	-	-	-	-	3	-	1	**4**
Kidnapping	-	-	-	-	-	4	-	3	-	**7**
Loss of life	-	-	-	-	-	-	-	-	1	**1**
Money laundering	-	6	-	-	1	31	-	2	-	**40**

Category	ACIC	AFP	ICAC (NSW)	ICAC (SA)	NSW CC	NSW Police	QLD Police	SA Police	VIC Police	TOTAL
Murder	-	-	-	-	-	29	-	3	1	**33**
Offences involving planning and organisation	-	-	-	-	-	19	-	-	4	**23**
Organised crime	-	10	-	-	-	-	-	-	-	**10**
Other offences punishable by three years to life	-	12	1	-	-	285	51	-	2	**351**
Serious arson	-	2	-	-	-	16	-	-	-	**18**
Serious drug offences	1	29	-	-	-	305	-	12	11	**358**
Serious fraud	-	-	-	-	-	56	2	-	-	**58**
Serious loss of revenue	-	-	-	-	-	-	-	-	2	**2**
Serious personal injury	-	1	-	-	-	46	-	3	2	**52**
Trafficking in prescribed substances	-	7	-	-	-	-	16	-	-	**23**
TOTAL	**1**	**73**	**1**	**1**	**1**	**807**	**72**	**23**	**25**	**1,004**

Named person warrants

A named person warrant can authorise the interception of multiple telecommunications services (such as a landline or mobile service), or telecommunications devices (such as a mobile handset) that relate to a particular person. Before issuing a named person warrant, an issuing authority must take into account a number of matters including:

- how much the privacy of any person would be likely to be interfered with
- the gravity of the conduct constituting the offence
- the extent to which the interception would be likely to assist in the investigation, and
- the extent to which less intrusive means other than using a named person warrant are available to the agency.

Paragraphs 100(1)(ea) and 100(2)(ea) of the TIA Act provide that this report must set out the relevant statistics about standard applications, telephone applications and renewal applications for named person warrants, and how many named person warrants issued on applications made by an agency during the reporting period specified conditions or restrictions relating to interceptions under the warrants.

This information is presented in **Tables 9 and 10**. In 2024–25, 433 named person warrants were issued, a decrease of 100 from 2023–24, in which 533 named person warrants were issued. In 2024–25, 118 renewal applications were issued, a decrease of 23 on the 141 issued in 2023–24. In 2024–25, two named person warrants were issued with a condition or restriction, an increase of two from 2023–24.

Table 9: Applications, telephone applications, and renewal applications for named person warrants – paragraphs 100(1)(ea) and 100(2)(ea)[15]

Agency	Relevant statistics	Applications		Telephone applications		Renewal applications	
		23/24	24/25	23/24	24/25	23/24	24/25
ACIC	Made	5	1	-	-	3	-
	Refused	-	-	-	-	-	-
	Issued	5	1	-	-	3	-
AFP	Made	224	234	-	-	74	78
	Refused	-	-	-	-	-	-
	Issued	224	234	-	-	74	78
CCC (WA)	Made	4	-	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	4	-	-	-	1	-
ICAC (SA)	Made	-	1	-	-	-	-

[15] The telephone applications and renewal applications made, refused and issued for named person warrants are a subsection of the total warrants made, refused, and issued for each agency.

Agency	Relevant statistics	Applications		Telephone applications		Renewal applications	
		23/24	24/25	23/24	24/25	23/24	24/25
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
LECC	Made	19	21	-	-	12	10
	Refused	-	-	-	-	-	-
	Issued	19	21	-	-	12	10
NACC	Made	2	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	2	-	-	-	-
NSW CC	Made	-	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	4	-	-	-	-
NSW Police	Made	161	124	-	-	44	23
	Refused	-	-	-	-	-	-
	Issued	161	124	-	-	44	23
NT Police	Made	5	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	5	4	-	-	-	-
QLD CCC	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
QLD Police	Made	16	7	-	-	2	-
	Refused	1	-	-	-	1	-
	Issued	15	7	-	-	1	-
SA Police	Made	1	3	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	1	3	-	-	-	1
VIC Police	Made	33	19	-	-	6	4
	Refused	-	-	-	-	-	-
	Issued	33	19	-	-	6	4
WA Police	Made	63	13	-	-	-	2
	Refused	-	-	-	-	-	-
	Issued	63	13	-	-	-	2
TOTAL	**Made**	**534**	**433**	**-**	**-**	**142**	**118**
	Refused	**1**	**-**	**-**	**-**	**1**	**-**
	Issued	**533**	**433**	**-**	**-**	**141**	**118**

Table 10: Named person warrants issued with specific conditions or restrictions – paragraphs 100(1)(ea) and 100(2)(ea)

Agency	Named person warrants issued specifying conditions or restrictions	
	23/24	24/25
ICAC (SA)	-	1
NSW CC	-	1
TOTAL	**-**	**2**

Paragraphs 100(1)(eb) and 100(2)(eb) of the TIA Act provide that this report must set out, for all named person warrants issued in the reporting period, the number of services intercepted in the categories outlined in the table below. This information is outlined in **Table 11**.

Table 11: Named person warrants by reference to services intercepted under the warrant – paragraphs 100(1)(eb) and 100(2)(eb)

Agency	Named person warrants by number of services intercepted							
	1 service only		2-5 services		6-10 services		10+ services	
	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25
ACIC	3	-	5	2	-	-	-	-
AFP	56	81	129	139	9	13	-	1
ICAC (SA)	-	-	-	1	-	-	-	-
LECC	9	18	10	3	-	-	-	-
NACC	2	-	-	2	-	-	-	-
NSW CC	-	1	-	3	-	-	-	-
NSW Police	68	57	75	59	4	1	-	-
NT Police	1	1	4	3	-	-	-	-
QLD CCC	-	-	1	-	-	-	-	-
QLD Police	5	2	9	5	-	-	-	-
SA Police	-	-	1	3	-	-	-	-
TAS Police	-	-	1	-	-	-	-	-
VIC Police	9	11	20	14	1	-	2	-
WA Police	7	6	56	7	-	-	-	-
TOTAL	**160**	**177**	**311**	**241**	**14**	**14**	**2**	**1**

Under the TIA Act, agencies can apply for a named person warrant in relation to telecommunications services or devices. Subparagraphs 100(1)(ec)(i)–(iii) and 100(2)(ec)(i)–(iii) require the report to include the total number of:

- services intercepted under service based named person warrants
- services intercepted under device based named person warrants, and
- telecommunications devices intercepted under device-based named person warrants.

Definitions

A **'telecommunications service'** is defined in section 5 of the TIA Act and means a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunications.

A **'telecommunications device'** is also defined in section 5 of the TIA Act and means a terminal device that is capable of being used for transmitting or receiving communication over a telecommunications system.

The number of services and devices intercepted under the different types of named person warrants are outlined in **Tables 12 and 13**.

Table 12: Total number of services intercepted under service-based named person warrants Paragraphs 100(1)(ec) and 100(2)(ec)

Agency	Services	
	23/24	24/25
ACIC	18	-
AFP	465	503
ICAC (SA)	-	2
LECC	37	14
NACC	2	7
NSW CC	-	10
NSW Police	256	218
NT Police	-	8
QLD CCC	1	-
QLD Police	33	18
SA Police	2	17
TAS Police	2	-
VIC Police	93	42
WA Police	-	182
TOTAL	**909**	**1,021**

Table 13 : Total number of services and devices intercepted under device-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)

Agency	Devices		Services	
	23/24	24/25	23/24	24/25
AFP	77	85	73	83
NSW Police	47	26	81	37
VIC Police	1	1	-	1
TOTAL	**125**	**112**	**154**	**121**

B-party warrants

Definition

A **'B-party warrant'** is a telecommunications service warrant that enables an interception agency to intercept the communications of a person who is communicating with a person suspected of involvement in a serious offence.

An issuing authority can issue a B-party warrant, but only if the agency has exhausted all other practicable methods of identifying the telecommunications services used by the person involved in the offences, or if the interception of communications from that person's telecommunications services would not otherwise by possible.

Paragraphs 100(1)(ed) and 100(2)(ed) of the TIA Act provide that this report must set out the relevant statistics about standard applications, telephone applications and renewal applications for B-party warrants. This report must also set out how many B-party warrants were issued and the number of applications made by an agency during the year, including requests to authorise entry on premises, and specified conditions or restrictions relating to interception under the warrants.

This information is presented in **Tables 14 and 15**. In 2024–25, 58 B-Party warrants were issued to interception agencies. This represents a decrease of 40 from the 98 B-party warrants issued in 2023–24. There was a decrease of 15 renewal applications, with six issued in 2024–25 and 21 in 2023–24. In 2024–25, no B-party warrants were issued with conditions or restrictions. This is a decrease of two from the B-party warrants issued in 2023–24.

Table 14: Applications for B-party warrants, telephone applications and renewal applications for B-party warrants – paragraphs 100(1)(ed) and 100(2)(ed)[16]

Agency	Relevant statistics	Applications for B-party warrants		Telephone applications for B-party warrants		Renewal applications for B-party warrants	
		23/24	24/25	23/24	24/25	23/24	24/25
AFP	Made	20	8	-	-	11	2
	Refused	-	-	-	-	-	-
	Issued	20	8	-	-	11	2
NACC	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
NSW Police	Made	77	50	4	1	10	4
	Refused	-	-	-	-	-	-
	Issued	77	50	4	1	10	4
TOTAL	**Made**	**98**	**58**	**4**	**1**	**21**	**6**
	Refused	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**98**	**58**	**4**	**1**	**21**	**6**

Table 15: B-party warrants issued with conditions or restrictions – paragraphs 100(1)(ed) and 100(2)(ed)

Agency	B-party warrants specifying conditions or restrictions	
	23/24	24/25
NACC	1	-
NSW Police	1	-
TOTAL	**2**	**-**

In 2024–25, no B-Party warrants were issued authorising entry onto premises. This is the same as the previous year.

Duration of warrants

Under the TIA Act, an interception warrant, other than a B-party warrant, can be in force for up to 90 days. Under section 57, the chief officer of an agency may revoke a warrant at any time and must revoke a warrant if they are satisfied that the grounds on which the warrant was issued no longer exist.

[16] The telephone applications and renewal applications made, refused and issued for B-party warrants are a subset of the total warrants made, refused and issued for each agency.

Paragraphs 101(1)(a)–(d) and 101(2)(a)–(d) of the TIA Act provide that this report must set out for each agency the average length of time for which interception warrants — including renewals, but not including B-party warrants — were issued, and the average length of time they were in force in the reporting period. This information is presented in **Table 16**.

Table 16: Duration of original and renewal interception warrants – paragraphs 101(1)(a)–(d) and 101(2)(a)–(d)

Agency	Duration of original telecommunications warrants		Duration of renewal telecommunications interception warrants	
	Average period specified in warrants (days)	Average period warrants in force (days)[17]	Average period specified in warrants (days)	Average period warrants in force (days)[18]
ACIC	90	90	-	-
AFP	88	63	86	54
CCC (WA)	75	58	-	-
IBAC	90	88	68	63
ICAC (NSW)	90	90	90	45
ICAC (SA)	68	62	30	16
LECC	90	90	90	35
NACC	90	80	90	90
NSW CC	89	79	84	55
NSW Police	80	51	82	66
NT Police	90	89	90	59
QLD CCC	86	85	89	89
QLD Police	74	53	71	45
SA Police	90	59	90	30
TAS Police	75	60	-	-
VIC Police	87	72	88	73
WA Police	85	79	86	86
AVERAGE	**85**	**73**	**81**	**58**

A B-party warrant can be in force for up to 45 days. Paragraphs 101(1)(da) and 101(2)(da) of the TIA Act provide that this report must set out for each agency the average length of time for which B-Party warrants — including renewals — were specified to be in force when issued, and the average length of time they were actually in force during the reporting period. This information is presented in **Table 17**.

[17] This column excludes warrants that did not cease before the end of the reporting period.
[18] This column excludes warrants that did not cease before the end of the reporting period.

Table 17: Duration of original and renewal B-Party warrants – paragraphs 101(1)(da) and 101(2)(da)

Agency	Duration of original B-Party warrants		Duration of renewal telecommunications B-Party warrants	
	Average period specified in warrants (days)	Average period warrants in force (days)[19]	Average period specified in warrants (days)	Average period warrants in force (days)[20]
AFP	45	28	45	45
NSW Police	38	22	15	5
AVERAGE	**42**	**25**	**30**	**25**

Final renewals

A final renewal means an interception warrant that is the last renewal of a warrant. A final renewal is recorded as the number of days after the issue of the original warrant. Paragraphs 101(1)(e) and 101(2)(e) of the TIA Act provide that this report must set out how many renewals ceased to be in force during that year.

Information on the number of final renewals of warrants by agencies is presented in **Table 18**.

Table 18: Final renewals – paragraphs 101(1)(e) and 101(2)(e)

Agency	90 days		150 days		180 days	
	23/24	24/25	23/24	24/25	23/24	24/25
ACIC	-	-	-	-	1	-
AFP	14	2	35	55	35	28
IBAC	-	1	-	-	-	-
ICAC (NSW)	-	4	-	-	-	-
LECC	-	3	3	1	3	-
NACC	-	-	2	2	-	-
NSW CC	1	1	-	-	-	-
NSW Police	88	53	79	61	51	40
NT Police	-	1	-	1	-	-
QLD CCC	-	-	3	5	3	-
QLD Police	13	8	16	4	6	2
SA Police	1	3	-	-	-	-
VIC Police	7	15	5	1	3	-

[19] This column excludes warrants that did not cease before the end of the reporting period.
[20] This column excludes warrants that did not cease before the end of the reporting period.

Agency	90 days		150 days		180 days	
	23/24	24/25	23/24	24/25	23/24	24/25
WA Police	-	165	-	-	-	-
TOTAL	**124**	**256**	**143**	**130**	**102**	**70**

Eligible warrants

Subsections 102(3) and 102(4) of the TIA Act provide that this report must set out for each agency the percentage of eligible warrants against the number of total warrants during the year.

Definition

An **'eligible warrant'** is a warrant that was in force during the reporting period — not necessarily a warrant that was issued during the reporting period — where a prosecution was instituted or was likely to be instituted on the basis of information obtained by interceptions under the warrant.

'Total warrant' means the number of warrants that were issued to an agency and in force during the year to which the report relates.

This information is presented in **Table 19**. In 2024–25, 68% of total warrants were eligible warrants.

Table 19: Percentage of eligible warrants – subsections 102(3) and 102(4)[21]

Agency	Number of eligible warrants	Total number of warrants in force	%
AFP	367	578	63
IBAC	13	16	81
ICAC (NSW)	6	11	55
ICAC (SA)	3	8	38
LECC	2	22	9
NSW CC	20	25	80
NSW Police	1,320	1,732	76
NT Police	11	25	44
QLD CCC	12	16	75
QLD Police	235	250	94
SA Police	18	22	82

[21] Total number of warrants in force is often larger than the number of warrants issued as it includes warrants issued in the previous reporting period but still in force during the current reporting period.

Agency	Number of eligible warrants	Total number of warrants in force	%
TAS Police	2	12	17
VIC Police	32	123	26
WA Police	23	182	13
TOTAL	**2,064**	**3,022**	**68**

Interception without a warrant

Under subsections 7(4) and 7(5) of the TIA Act, an agency can undertake interception without a warrant in the event of an emergency. Section 102A of the TIA Act provides that this report must set out, for each of those agencies, the number of occasions where an officer or staff member of the agency intercepted a communication in reliance on subsections 7(4) or 7(5).

Table 20: Number of occasions on which an officer or staff member of an agency intercepted a communication in reliance on subsection 7(4) or 7(5) – section 102A

Agency	23/24	24/25
AFP	2	2
TOTAL	**2**	**2**

In 2024–25, the AFP intercepted two communications without a warrant. The AFP advised that they were a party to the communication where there were reasonable grounds for suspecting that another party to the communication had committed an act that has resulted, or may result, in loss of life or the infliction of serious personal injury. The AFP advised that in both instances this occurred with the consent of the person to whom the communication was directed.

Subsection 7(6) requires that as soon as practicable after the interception of a communication in reliance on subsection 7(4) or 7(5), an officer of the agency shall cause an application for an interception warrant to be made in relation to the matter.[22] The AFP has complied with all requirements under subsection 7(6).

International assistance

Section 102B of the TIA Act provides that this report must set out the number of occasions where lawfully intercepted information or interception warrant information was provided to:

- a foreign country under paragraph 68(l) or section 68A of the TIA Act in connection with an authorisation under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*

[22] There is an exception where the action has ceased before it is practicable for an application to be made under s 7(6A).

- the International Criminal Court under paragraph 68(la) or section 68A of the TIA Act in connection with an authorisation under section 69A of the *International Criminal Court Act 2002*, and
- a War Crimes Tribunal under paragraph 68(lb) or section 68A of the TIA Act in connection with an authorisation under section 25A of the *International War Crimes Tribunals Act 1995*.

In 2024–25, there were two occasions in which lawfully intercepted information or interception warrant information was provided to a foreign country under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*. This is an increase of one from 2023–24.

In 2024–25, there were no occasions in which lawfully intercepted information or interception warrant information was provided to the International Criminal Court under section 69A of the *International Criminal Court Act 2002*, or to a War Crimes Tribunal under section 25A of the *International War Crimes Tribunal Act 1995*. This is the same as 2023–24.

Number of interceptions carried out on behalf of other agencies

The TIA Act supports the ability of interception agencies to cooperate and work collaboratively by enabling one interception agency to carry out interception on behalf of other interception agencies. Paragraph 103(ac) of the TIA Act provides that this report must set out for each agency the number (if any) of interceptions carried out on behalf of other agencies. In total, 28 interceptions were carried out on behalf of other agencies in the reporting period. This is an increase of four from the 24 interceptions carried out in 2023–24.

Table 21: Interceptions carried out on behalf of other agencies – paragraph 103(ac)

Interception carried out by:	Interception carried out on behalf of	Number of interceptions
VIC Police	Tasmania Police	10
VIC Police	Queensland CCC	10
CCC (WA)	ICAC (SA)	8
TOTAL		28

Telecommunications interception expenditure

Table 22 provides information about the total expenditure (including capital expenditure) incurred by interception agencies in connection with interception warrants and the average expenditure per warrant.

Care should be taken in comparing costs associated with average expenditure as interception agencies employ different interception models, which may result in some costs associated with interception being delineated, and for other agencies, those same costs being included in their average expenditure. The average cost can vary significantly, for instance, due to a capital upgrade program, as well as the number of warrants issued—smaller agencies typically have higher average costs as they apply for fewer warrants.

Table 22: Total expenditure incurred by each agency in connection with the execution of interception warrants and average expenditure per interception warrant – paragraphs 103(a) and 103(aa)

Agency	Total expenditure	Average expenditure
ACIC	$3,708,477	$3,708,477[23]
AFP	$22,648,804	$48,603
CCC (WA)	$191,314	$23,914
IBAC	$1,030,831	$93,712
ICAC (NSW)	$816,580	$136,097
ICAC (SA)	$290,237	$36,280
LECC	$911,807	$43,419
NACC	$280,407	$31,156
NSW CC	$1,465,594	$66,618
NSW Police	$9,578,878	$5,987
NT Police	$1,062,000	$42,480
QLD CCC	$1,207,325	$120,733
QLD Police	$9,059,824	$ 42,139
SA Police	$4,993,917	$226,996
TAS Police	$1,282,954	$128,295
VIC Police	$331,508	$3,014
WA Police	$4,760,000	$15,385
TOTAL / AVERAGE	**$63,620,457**	**$312,755[24]**

The breakdown of the total recurrent costs of interception over the reporting period is provided in **Table 23**. As agencies do not necessarily treat or record particular items of expenditure in the same way, caution should be exercised in comparing costs incurred by individual agencies.

[23] The ACIC had only one interception warrant over the period, meaning that its average and total expenditure in the period are the same.
[24] The total average expenditure for interception warrants represents the average of all the individual average expenditures reported by the agencies.

Table 23: Recurrent interception costs per agency

Agency	Salaries	Administrative support	Capital expenditure	Interception costs	Total ($)
ACIC	$2,251,370	$162,167	$85,728	$1,209,212	**$3,708,477**
AFP	$11,384,657	$531,613	$5,193,230	$5,539,304	**$22,648,804**
CCC (WA)	$150,563	-	-	$40,751	**$191,314**
IBAC	$657,721	$30,747	$52,408	$289,955	**$1,030,831**
ICAC (NSW)	$617,081	$70,285	$128,279	$935	**$816,580**
ICAC (SA)	$189,150	$5,268	$93,500	$2,319	**$290,237**
LECC	$712,090	$1,677	$70,109	$127,931	**$911,807**
NACC	$69,050	-	$208,453	$2,904	**$280,407**
NSW CC	$870,393	-	-	$595,196	**$1,465,589**
NSW Police	$6,966,844	$140,916	-	$2,471,118	**$9,578,878**
NT Police	$501,000	-	$483,000	$126,000	**$1,110,000**
QLD CCC	$743,032	$214,531	-	$249,762	**$1,207,325**
QLD Police	$6,698,042	$564,900	-	$1,796,883	**$9,059,825**
SA Police	$2,733,252	$356,999	$748,280	$1,155,386	**$4,993,917**
TAS Police	$1,017,271	$37,589	$6,539	$221,555	**$1,282,954**
VIC Police	$232,718	$16,766	$16,552	$37,755	**$303,791**
WA Police	$3,823,600	-	$900,000	$36,400	**$4,760,000**
TOTAL	**$39,617,834**	**$2,133,458**	**$7,986,078**	**$13,903,366**	**$63,640,736**

Emergency service facilities

Under the TIA Act, listening to or recording calls to and from a facility declared by the Minister for Home Affairs to be an emergency service facility does not constitute interception. This exemption ensures that emergency service providers can assist emergency callers and respond to critical situations as quickly as possible, without the need to first obtain a caller's consent to the recording of the call. **Table 24** sets out the number of premises that have been declared in 2024–25 under the TIA Act to be emergency service facilities. It does not include facilities that were declared in a previous reporting period, unless the declaration instrument was remade in 2024–25.

Table 24: Emergency service facility declaration – paragraph 103(ad)

State	Police	Fire brigade	Ambulance	Dispatching	Shared facilities	TOTAL
Australian Capital Territory	-	-	-	1	-	**1**
New South Wales	-	1	-	-	-	**1**
Northern Territory	1	-	-	-	1	**2**
Queensland	16	8	9	15	-	**48**[25]
South Australia	-	-	-	-	1	**1**
Victoria	-	-	1	-	-	**1**
TOTAL	**17**	**9**	**10**	**16**	**2**	**54**

Safeguards and reporting requirements on interception powers

The TIA Act contains a number of safeguards, controls, and reporting requirements in relation to interception warrants. These include a requirement for:

- the heads of interception agencies to provide the Secretary of Home Affairs with a copy of each interception warrant
- interception agencies to report to the Minister for Home Affairs, within three months of a warrant ceasing to be in force, detailing the use of information obtained by interception under the warrant
- the Secretary of Home Affairs to maintain a General Register detailing the particulars of all interception warrants. The Secretary of Home Affairs must provide the General Register to the Minister for Home Affairs for inspection every three months, and
- the Secretary of Home Affairs to maintain a Special Register recording the details of interception warrants that do not lead to a prosecution within three months of the warrant expiring. The Special Register is also given to the Minister for Home Affairs to inspect.

Interception agencies' use of interception powers under the TIA Act is independently overseen by the Ombudsman and equivalent state oversight and integrity bodies.

At least twice a year the Ombudsman must inspect the records kept by the ACIC, the NACC, and the AFP relating to interception, and the use, dissemination and destruction of intercepted information. The inspections are retrospective, and for this reason, the Ombudsman inspected relevant telecommunications interception warrants that were expired or revoked in the period between 1 January and 31 December 2024.

[25] The *Telecommunications (Interception and Access) (Emergency Services Facilities – Queensland) Instrument 2015* instrument sunset on 1 October 2025 and was remade.

The Ombudsman is required under the TIA Act to report to the Minister for Home Affairs about these inspections, including information about any deficiencies identified and remedial action. State and territory legislation impose similar requirements on state and territory oversight agencies regarding interception agencies' use of interception powers.

While the Ombudsman is responsible for inspecting the record of the ACIC, the NACC, and the AFP in relation to interception, the relevant state or territory Ombudsman generally undertakes this function for state or territory agencies. The reports of the inspections of the declared state and territory agencies are given to the responsible state or territory minister who provides a copy to the Minister for Home Affairs. The Ombudsman also conducts inspections of records related to enforcement agencies' (including both Commonwealth and state agencies) access to stored communications and telecommunications data.

Ombudsman – Inspection of telecommunications records conducted in 2024–25

Overview

During the 2024–25 financial year (the inspection period), the Ombudsman conducted seven inspections under section 83(1) of the TIA Act. These inspections examined the use of telecommunications interception powers under Chapter 2 of the TIA Act by the following Commonwealth agencies:

- ACIC
- AFP, and
- NACC.

The Ombudsman must inspect and report on agencies' compliance with record keeping and destruction provisions under sections 79, 79AA, 80 and 81 of the TIA Act. Additionally, in accordance with section 85 of the TIA Act, the Ombudsman may also report on any other contravention of the TIA Act.

This report provides a summary of the most significant findings from these inspections and identifies matters, such as the adequacy of their policies, procedures and practices, that will assist agencies to improve their compliance with the law.

The Ombudsman found several key areas of concern across the agencies, including:

- there is a not insignificant risk that the ACIC could not adequately demonstrate it met the necessary legislative thresholds, if challenged in court, when using the telecommunications interception powers in all instances
- the AFP did not destroy records authorised for destruction within appropriate timeframes
- insufficient information was included by the ACIC and NACC in applications and affidavits to renew telecommunications interception warrants, and
- telecommunications interception warrants were not revoked by the AFP when the legislated threshold to use the powers no longer existed.

The Ombudsman did not identify any non-compliance by agencies with their obligation to keep documents connected with the issue of the warrant (section 80 of the TIA Act) or other records in connection with interceptions (section 81 of the TIA Act). Whilst the AFP complied with requirements to destroy material obtained in relation to an interception Part 5.3 warrant under section 79AA, it did not comply with requirement to destroy restricted records that are not likely to be required for a permitted purpose under section 79 of the TIA Act.

Overview of Inspections

The Ombudsman conducted seven telecommunications interception inspections during the inspection period. Five of these inspections were combined with inspections of other covert powers the Ombudsman oversaw and assessed the agencies use of telecommunications interception powers within select operations or investigations. The Ombudsman's December 2024 inspection of the ACIC reviewed records connected with a sample of all ACIC usages of telecommunications interception powers.

Between December 2024 and March 2025, the Ombudsman conducted an additional inspection of the ACIC. The Ombudsman inspected the records in the four ACIC intelligence operations that were reviewed in the 2023–24 inspection period. The Ombudsman concluded its view on whether the ACIC had been able to adequately demonstrate in those operations the connection with the thresholds under the TIA Act.

Good practices

The AFP complied with obligations under section 79AA of the TIA Act to destroy restricted records associated with Part 5.3 telecommunications interception warrants and all three agencies complied with their record keeping obligations under sections 80 and 81 of the TIA Act.

Positively engaging with changes to the Ombudsman's inspection approach

The ACIC, AFP and NACC positively engaged with changes to the Ombudsman's inspection approach. At previous inspections, it examined records connected with a sample of all usages of the telecommunications interception powers by an agency. During the Ombudsman's 2023–24 inspection period, it reviewed records at the ACIC within a selection of intelligence operations. This was the first time the Ombudsman compared the records connected to the use of the powers with the decisions and plans made by investigators for their intended use of telecommunications interception powers.

The Ombudsman broadened this approach during this inspection period to the AFP and NACC (in addition to the ACIC). It reviewed each agency's use of telecommunications interception powers within a selection of agency operations or investigations. Agency staff were receptive to the change in approach and demonstrated flexibility in supporting the Ombudsman's inspection requirements.

ACIC destructions

The Ombudsman's 2019 inspection of the ACIC found a significant number of records dating back to before 2012 that had not yet been reviewed or destroyed. During the 2023–24 inspection period, the Ombudsman was concerned with the ACIC's progress in reviewing and destroying records created between 2012 and 2016 that the agency was not

permitted to retain. The ACIC accepted the Ombudsman's recommendation to dedicate resources to expedite the review and destruction of these records.

During this inspection period, the Ombudsman was pleased to see that the ACIC had taken significant steps to review and destroy records that the agency was no longer permitted to retain. This included the destruction of records from 3,389 warrants dating from 2002 to 2020.

The ACIC also took steps to upgrade its systems that facilitated the destruction of records from telecommunications interception warrants. This resulted in a more streamlined destruction process, which will assist the ACIC in meeting its destruction obligations under the TIA Act.

What can agencies improve on?

There is a not insignificant risk that the ACIC would not be able to adequately demonstrate they met the thresholds when using telecommunications interception powers in all instances.

A law enforcement agency can obtain a warrant to intercept a telecommunication service if there is a reasonable suspicion that the material gathered through interception would likely assist in connection with investigating a serious offence.[26]

The Ombudsman recognises the unique role of the ACIC which encompasses the strategic direction of an intelligence agency while having a legal framework for some powers that is premised on a law enforcement agency. The ACIC primarily exists to perform an intelligence function, providing a range of both focussed and high-level intelligence products to its law enforcement partners. The ACIC generally relies on arrangements with its partners to investigate serious offences or commence proceedings before a court. It is the nature of intelligence that it may or may not lead to or result in a law enforcement outcome. However, the Ombudsman considers there still needs to be a demonstrated link with the threshold for being able to use telecommunications interception powers.

The Ombudsman's last report to the Attorney-General highlighted its observation that the ACIC's demonstration of the link with the threshold for being able to use telecommunications interception powers was not always clear. At that time, the Ombudsman had not yet concluded its views on whether the ACIC had been able to adequately demonstrate a connection between the use of telecommunications intercept powers and the thresholds under the TIA Act. The Ombudsman's observation was based on the records it inspected within four ACIC intelligence operations between April and May 2024.

Between December 2024 and March 2025, the Ombudsman re-examined the records for those four intelligence operations to conclude its view on whether the ACIC had been able to adequately demonstrate the connection with the thresholds under the TIA Act.

---

[26] Section 46 and 46A limits the issuing of a warrant to intercept communications where an eligible judge or nominated ART is satisfied on reasonable grounds that information obtained by intercepting communication under a warrant would be likely to assist in connection with the investigation by the agency of a serious offence(s), in which the particular person is involved or another person is involved with whom the particular person is likely to communicate using the telecommunication service.

The Ombudsman found that there was a not insignificant risk that the ACIC would not be able to adequately demonstrate it met the thresholds if challenged in court when using these powers in all instances. This was not to say that the Ombudsman found evidence to suggest the powers were being used unlawfully. Rather, there was a lack of records to clearly demonstrate that they were be used lawfully.

The Ombudsman observed differences in the way the telecommunications interception powers are accessed by the ACIC in intelligence operations compared to how other law enforcement and integrity agencies use these powers within an investigation. The Ombudsman generally sees law enforcement agencies use a telecommunications interception warrant to investigate and prove an allegation of a crime having been, or being, committed. Admissibility of evidence gathered through a telecommunications interception power is the key priority for any law enforcement investigation. In contrast, during an intelligence operation, the ACIC does not directly contribute evidence from using telecommunications interception powers to support an investigation or prosecution of a person for an offence, but rather, provides what it calls 'actionable intelligence' or potential investigation leads that another agency that may or may not use to gather their own evidence of that offending.

The connection between the ACIC's use of telecommunications interception powers and the purpose of providing assistance in connection with investigating a serious offence (an investigative purpose) is less clear. This connection is particularly strained when the ACIC uses telecommunications interception powers and collects evidence, but it may not ever intend to pass that material to a partner law enforcement agency as evidence or necessarily advise a partner agency of its activities at all.

The ACIC principally relied upon the applications used to seek a warrant as the primary records to demonstrate the use of telecommunications interception powers met the legislated thresholds. However, the Ombudsman considers it important to look at all the surrounding circumstances to determine if there was indeed the requisite investigative purpose when using telecommunications interception powers. Despite the original application providing material connecting the proposed issue of a telecommunications interception warrant to the investigation of an offence, the Ombudsman found limited records to help determine how the use of telecommunications interception powers were regularly monitored and evaluated against the objectives of the ACIC's intelligence operation, or how the information generated through the use of the powers would likely assist in connection with an investigation by the ACIC or a partner agency. With limited records to help re-construct the chronology of the investigation, the value of using telecommunications interception powers to assist the ACIC or a partner's investigation was difficult to determine.

In response to the Ombudsman's findings from the April to May 2024 inspection, the ACIC acknowledged that its records supporting the use of the telecommunications interception powers could be improved. That said, at this inspection the Ombudsman was concerned that unless the ACIC turns its mind to the inherent risks that exist when using law enforcement powers in an intelligence setting, considers how these risks can be mitigated, records those considerations, and can be sure its staff know how to use the powers lawfully, there will continue to be a risk that the link between the ACIC's use of the powers and the relevant legal thresholds will be tenuous or not be able to be demonstrated.

The Ombudsman made five recommendations and three suggestions to assist the ACIC with engaging the legal risks when using telecommunications interception powers in support of its intelligence mandate.

The ACIC accepted two, and accepted in part three, of the Ombudsman's recommendations. The ACIC acknowledged that more can be done to record considerations and decisions throughout the life of covert warrants and authorisations and in considering disclosure of evidence. The ACIC acknowledged the Ombudsman's recommendations and suggestions on how the ACIC can continue to improve its compliance and risk practices. The ACIC appreciated the Ombudsman's Office acknowledging that the ways in which the ACIC uses covert powers differs from other law enforcement and integrity agencies use of the same powers.

Records authorised for destruction were not disposed of within appropriate timeframes

The Ombudsman saw instances at the AFP where records authorised for destruction were not destroyed within an appropriate timeframe.

Telecommunications interception records are highly intrusive on an individual's privacy. Agencies should be responsible for regularly reviewing these records and destroying them forthwith when they are not required for a permitted purpose under the TIA Act. Section 79 is a key safeguard in the legislation and requires the chief officer to cause records to be destroyed forthwith if they are likely to not be required for a permitted purpose under the TIA Act. Agencies should have internal guidance on what is an appropriate timeframe to satisfy the destruction requirements. If there is no internal guidance, the Ombudsman considers material authorised for destruction should be disposed of within 28 days of the records being authorised for destruction.

AFP

The Ombudsman identified several instances where the destruction of records had been authorised, but the AFP did not destroy these forthwith as required by the TIA Act. During the March 2025 inspection, the Ombudsman identified 26 warrants across nine operations had not been destroyed forthwith. The AFP advised that some of these operations were permitted a temporary increase to the time to destroy the records from one month to two months. Despite this increase, the records from some of operations were still not destroyed within this amended deadline.

The Ombudsman's Office was also concerned that this temporary change to AFP's definition of forthwith had not been shared with its Office during previous inspections. The Ombudsman encourages agencies at the beginning of each inspection to share any policy changes that impact on the agencies use of the powers it inspects. The AFP advised that it did not consider this to be significant change in policy and would work with the Ombudsman's Office to clarify when policy changes should be notified to the Ombudsman's Office.

The failure to destroy records forthwith is a repeat finding for the AFP. The Ombudsman recommended the AFP conduct a comprehensive review of its destruction process to ensure records no longer required for a permitted purpose are destroyed at the earliest opportunity. The Ombudsman also recommended that the AFP must destroy any records authorised for destruction within the legislated timeframe under the TIA Act, and for staff to ensure accurate records confirming the destructions are kept.

The AFP accepted the Ombudsman's recommendations and suggestion. The AFP completed a review of its destruction process and is working towards ensuring records that are no longer required for a permitted purpose under the TIA Act are destroyed.

Suspending the destruction of telecommunications interception records

In March 2025, the AFP advised that it had suspended the destruction of telecommunications interception records due to technical issues limiting its ability to dispose of the records. Despite not being able to facilitate the record's destruction, the AFP was continuing to identify and review records that are no longer required for a permitted purpose under the TIA Act. The AFP advised that these records had been quarantined from further use or communication and would be destroyed once the technical issues were resolved.

Insufficient consideration of privacy impacts on third parties

The Ombudsman found the ACIC and NACC did not sufficiently outline the extent to which privacy of persons would likely be impacted when renewing certain telecommunications interception warrants. Both agencies relied upon considerations made within the original affidavit used to obtain the warrant and did not sufficiently outline changes in the investigation or any privacy intrusion from the use of the telecommunications interception powers authorised by the original warrant.

Affidavits for any renewal of a telecommunications interception warrant should accurately reflect the circumstances of the investigation, any changes to those circumstances, the likely impacts on the privacy of any person, and any steps the agency will take to limit unnecessary intrusion on privacy of a person. When issuing a telecommunications interception warrant, sections 46(2) or 46A(2) of the TIA Act require the eligible judge or nominated Administrative Review Tribunal (ART) member to consider how much the privacy of any person or persons would be likely to be interfered with under a warrant.

While the Ombudsman does not consider the merits of a decision to issue a warrant, it does assess whether affidavits provided to the judge or ART member contain sufficient details specific to the investigation, allowing them to consider the matters which they must have regard. This includes whether the affidavits and any subsequent renewal, contain sufficient detail about the privacy impacts on any person to enable the judge or ART member to have regard to the use of powers they are authorising.

ACIC

At the ACIC, the Ombudsman identified three affidavits that were used to renew a named person telecommunications interception warrant that did not contain sufficient information to address the privacy considerations under section 46A(2) of the TIA Act. This warrant was in effect for 314 days.

The affidavit relied upon to issue the original warrant documented the privacy considerations, the ACIC's considerations of other means to investigate the serious offence, and the extent to which the interception would likely assist in the investigation of a serious offence. However, each of the subsequent affidavits used to renew the warrant continued to rely on the conditions set out in the original affidavit and did not review or re-assess the impacts on privacy. This included providing insufficient information to explain how the interception of the communications had assisted in the investigation of the serious

offence or details of any other less intrusive or other means of investigation that had been considered by the ACIC before applying to renew the warrant.

The Ombudsman suggested the ACIC ensures there is sufficient and up to date information in affidavits to renew telecommunications interception warrants to accurately address all the requirements under section 46A of the TIA Act.

The ACIC's acceptance of the Ombudsman's suggestion was qualified. The ACIC did not agree with the information relied upon by the Ombudsman's Office to support its suggestion and believed the affidavit met the legislative thresholds under the TIA Act. The ACIC, acknowledged that the drafting of the warrants could have been clearer. Following the Ombudsman's inspection, the ACIC reviewed its process and was satisfied that the ACIC's process for preparing and reviewing affidavits were sufficient. The ACIC is confident that it meets the legislative thresholds under section 46A of the TIA Act and that all warrants were considered and authorised by relevant issuing authorities.

NACC

The Ombudsman identified one instance where the affidavit to renew a telecommunications interception warrant did not sufficiently outline the extent to which the privacy of persons would likely be impacted.

While the affidavit used to apply for the initial warrant provided sufficient consideration of impacts on the privacy of persons, the affidavit relied upon to renew this warrant for an additional 90 days did not reassess these privacy considerations, or confirm whether the circumstances in the original affidavit remained the same.

The Ombudsman suggested that the NACC ensures any applications or affidavit to renew a warrant include any information related to, or assessment of, the impacts on privacy of a person or third party gathered through the preceding warrant(s).

The NACC accepted this suggestion and has discussed privacy impacts with staff to ensure further consideration is given when drafting affidavits for renewal of warrant applications. Staff have also been instructed to complete relevant eLearning modules.

Warrants not being revoked when they were no longer required to assist with the investigation of a serious offence

The Ombudsman was informed of instances where the AFP did not revoke a telecommunications interception warrant when the grounds on which the warrant was issued had ceased to exist.

The Ombudsman encourages agencies to continually monitor and evaluate the use of telecommunications interception powers throughout an investigation to ensure the circumstances in which a warrant was issued under either section 46 or 46A of the TIA Act continue to exist. Section 57 of the TIA Act requires the chief officer, or their delegate, to revoke a warrant where they are satisfied that the ground under which the warrant was issued to the agency have ceased to exist.

At the March 2025 inspection, the AFP disclosed four instances where warrants were not revoked when no longer required for an investigation. On two occasions, documentation to revoke the warrants had been prepared but not progressed to the chief officer or their delegate due to failures in administrative oversight.

In the other two instances, the Ombudsman observed practices of 'parking' warrants, meaning the warrants remained in force, but no services or devices were being actively intercepted. Despite being in force, the AFP did not revoke these warrants and allowed them to expire. The Ombudsman understands there are circumstances where it may be necessary to reconnect the warrants for operational reasons. Where this is the case, it expects to see records demonstrating regular consideration of the reasons why warrants remain in force and the need to retain the warrant. The Ombudsman located no records of any considerations or decisions to retain these warrants, or revoke the warrants if they were no longer required for the investigation.

The Ombudsman suggested the AFP review its practice of 'parking' telecommunications interception warrants and ensure that any decisions and/or considerations to retain or revoke a warrant is recorded. The Ombudsman also suggested the AFP revoke a warrant under section 57 of the TIA Act where the thresholds to use the powers under sections 46 and 46A of the TIA Act have ceased to exist.

In response, the AFP accepted this suggestion and has reviewed its practice of 'parking' warrants. The AFP will update systems to send automated reminders to case officers to review a warrant and record any requirement to continue or revoke the warrant. The AFP advised it will implement a manual process as an interim measure to remind case officers every two weeks once a warrant is parked to review and document the need to retain or revoke the warrant.

Minor non-compliance with Part 5.3 supervisory order telecommunications interception warrants

The Ombudsman identified minor non-compliance with the AFP's use of Part 5.3 supervisory order telecommunications interception warrants.

During the Ombudsman's August 2024 inspection, the Ombudsman found an isolated instance where a warrant for monitoring a Part 5.3 supervisory order stated it was issued to monitor compliance with an interim control order. However, at the time the warrant was issued the interim control order had been confirmed by a Court and consequentially became a confirmed control order.

This was the first time the Ombudsman had observed non-compliance with the AFP's use of Part 5.3 supervisory order telecommunication interception warrants. The Ombudsman suggested the AFP ensure applications for warrants issued for monitoring powers reference the correct Part 5.3 supervisory order for which the warrant is being sought to monitor. The AFP accepted this suggestion and has reminded staff to update warrants if the status of an order changes between vetting and issuing the warrant.

At the March 2025 inspection, the Ombudsman also identified an isolated instance of the AFP failing to notify the Ombudsman's Office within six months of a Part 5.3 supervisory order telecommunication interception warrant being issued. This is a requirement under section 59B(1) of the TIA Act. The Ombudsman suggested that the AFP ensure its Office is notified of any Part 5.3 supervisory order telecommunications interception warrant issued under section 46 of the TIA Act within six months of the warrant being issued.

The AFP accepted the Ombudsman's suggestion and reminded its members of their notification obligations under the TIA Act. The AFP advised that it updated their warrant checklists to ensure notification to the Ombudsman occurs within six months of the warrant being issued.

Delays or errors in reports to the Minister

The Ombudsman observed instances at the AFP and ACIC where reports to the Minister were either delayed, did not contain certain information or were inconsistent with the records of the agency.

Reports to the Minister serve as an important transparency mechanism of the use of telecommunications interception powers. Agencies must ensure that reports accurately include all details as required by sections 94 and 94B of the TIA Act, as to provide the Minister with an accurate assessment of the action that took place under a telecommunications interception warrant. These reports must be provided to the Minister within three months after a telecommunications interception warrant ceases to be in force.

AFP

At the Ombudsman's March 2025 inspection, the AFP advised of two separate instances where reports required to be provided under sections 94 and 94B of the TIA Act were not submitted to the Minister within three months. There were several reasons for delay, including failures by staff to follow established AFP processes, failures in workflows to update a warrant status, incorrect dates being recorded and other internal administrative errors. Although the AFP identified and remedied these breaches, including providing a copy of the reports to the Minister, the Ombudsman was concerned with the failings in the AFP workflows and staff's adherence to AFP processes.

The Ombudsman suggested the AFP review its internal guidance and remind investigators at the cessation of a warrant to ensure reports under sections 94 and 94B of the TIA Act are submitted to the Minister within three months of the warrant ceasing.

In response, the AFP accepted the Ombudsman's suggestion and has reviewed the existing controls for compliance with sections 94 and 94B of the TIA Act. The AFP advised it will implement system updates to send automated emails to remind case officers that their reports are incomplete. Until this system is updated, the AFP will introduce a process to follow up with case officers after 21 days if their sections 94 or 94B reports have not been completed.

ACIC

At the ACIC, the Ombudsman identified an instance where lawfully intercepted information communicated to an external agency was not recorded in the reports to the Minister for this warrant. The ACIC explained that it provided the Ombudsman's Office with the incorrect warrant number and the disclosures had in fact occurred under an earlier warrant. The Ombudsman suggested to the ACIC that it should provide the Minister with an updated report in relation to the earlier warrant which accurately recorded the communication of the lawfully intercepted information to the external agency. The ACIC did not agree with this suggestion because the earlier warrant had ceased to be in force for longer than 90 days. In the ACIC's view, this falls outside of the notification period to the Minister. However, the Ombudsman's view is that this is contrary to the intention of the reporting provisions, and it remains that the ACIC did not accurately report to the Minister about the communication within the 90 day time period as required under the legislation.

Chapter 3: Stored communications

Applications for stored communications warrants

Access to stored communications is regulated by Chapter 3 of the TIA Act. Chapter 3 of the TIA Act makes it an offence to access stored communications except in limited circumstances. Authorities and bodies that are criminal law-enforcement agencies under the TIA Act can apply to an issuing authority for a stored communications warrant to investigate a 'serious contravention' as defined in the TIA Act.

Stored communications include communications such as email, SMS, or voice messages stored on a carrier's equipment.

Definition

An **'issuing authority'** is defined at section 6DB of the TIA Act and means a judge, magistrate or an ART member who is enrolled as a legal practitioner for at least five years, and who has been appointed by the Attorney-General.

'Criminal law-enforcement agencies' are set out in section 110A of the TIA Act, being all interception agencies as well as Home Affairs, ASIC, ACCC, or a body for which a declaration is in force. A declaration remains in force for 40 Parliamentary sitting days.

During the reporting period, the ACT Integrity Commission was declared to be a criminal law-enforcement agency.

A **'serious contravention'** includes:

- offences punishable by imprisonment for a period of at least three years
- serious offences (offences for which a telecommunications interception warrant can be obtained), and
- offences or contraventions of the law punishable by a fine of at least 180 penalty units ($59,400 at the end of the reporting period) for individuals or 900 penalty units ($297,000 at the end the reporting period) if the offence cannot be committed by an individual, such as a corporation.

Paragraphs 162(1)(a)–(b) and 162(2)(a)–(b) and (c) of the TIA Act provide that this report must set out the relevant statistics about applications, telephone applications and renewal applications for stored communications warrants that criminal law-enforcement agencies made during the year.

This information is presented in **Table 25**. In 2024–25, 706 stored communications warrants were issued, representing a decrease of 32 from the 738 stored communications warrants issued in 2023–24.

Table 25: Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 162(1)(a)–(b), 162(2)(a)–(b) and 162(2)(c)

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		23/24	24/25	23/24	24/25	23/24	24/25
AFP	Made	27	23	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	27	23	-	-	-	-
IBAC	Made	3	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	-	-	-	-	-
LECC	Made	-	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	2	-	-	-	-
NACC	Made	-	4	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	4	-	-	-	-
NSW Police	Made	357	383	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	357	383	-	-	-	-
NT Police	Made	8	5	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	8	5	-	-	-	-
QLD Police	Made	121	67	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	121	67	-	-	-	-
SA Police	Made	2	13	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	13	-	-	-	-
TAS Police	Made	31	29	-	-	-	-
	Refused	-	2	-	-	-	-
	Issued	31	27	-	-	-	-
VIC Police	Made	113	120	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	113	120	-	-	-	-
WA Police	Made	77	62	-	-	-	-

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		23/24	24/25	23/24	24/25	23/24	24/25
	Refused	1	-	-	-	-	-
	Issued	76	62	-	-	-	-
TOTAL	**Made**	**739**	**708**	**-**	**-**	**-**	**-**
	Refused	**1**	**2**	**-**	**-**	**-**	**-**
	Issued	**738**	**706**	**-**	**-**	**-**	**-**

Conditions or restrictions on stored communications warrants

Paragraph 162(2)(d) of the TIA Act provides that this report must set out how many stored communications warrants issued during the reporting period specified conditions or restrictions relating to access to stored communications under warrants.

This information is presented in **Table 26**. In 2024–25, 448 stored communications warrants were subject to conditions or restrictions, this is an increase of 30 warrants compared to 2023–24.

Table 26: Stored communications warrants subject to conditions or restrictions – paragraph 162(2)(d)

Agency	23/24	24/25
AFP	24	22
NACC	-	1
NSW Police	357	383
SA Police	2	13
TAS Police	31	27
VIC Police	4	-
WA Police	-	2
TOTAL	**418**	**448**

Effectiveness of stored communications warrants

Section 163 of the TIA act provides that this report must set out how many arrests were made during the year on the basis of information that was, or included, lawfully accessed information. This report must also set out how many proceedings, in which lawfully accessed information was given in evidence, ended during the reporting period.

This information is presented in **Table 27**. In 2024–25, lawfully accessed information:

- contributed to 319 arrests
- was given in evidence in 236 proceedings, and
- resulted in 177 convictions in proceedings where such information had been given in evidence.

This is an increase of 36 arrests, 26 proceedings and 19 convictions from 2023–24.

Table 27: Arrests, proceedings and convictions made on the basis of lawfully accessed information – paragraphs 163(a)–(b)

Agency	Arrests		Proceedings		Convictions	
	23/24	24/25	23/24	24/25	23/24	24/25
AFP	39	84	12	21	3	7
NSW Police	111	127	76	110	38	76
NT Police	-	2	-	-	-	1
QLD Police	70	45	4	69	4	69
SA Police	-	5	1	5	-	4
TAS Police	5	2	-	2	-	-
VIC Police	58	45	117	29	113	20
WA Police	-	9	-	-	-	-
TOTAL	**283**	**319**	**210**	**236**	**158**	**177**

Care should be taken in interpreting **Table 27**, as an arrest recorded in one reporting period may not result in a prosecution until a later reporting period (if any). Any conviction may be recorded in that period, or a later period. In some cases, the weight of evidence obtained through stored communication warrants results in defendants entering guilty pleas, eliminating the need for lawfully accessed information to be admitted into evidence.

Preservation notices

Under Part 3-1A of the TIA Act, criminal law-enforcement agencies can give a preservation notice to a carrier. A preservation notice requires a carrier to preserve stored communications that a carrier holds. The carrier is required to keep the stored communications while the notice is in force. The TIA Act provides for three types of preservation notices:

- *Historic domestic preservation notice* — requires the preservation of all stored communications held by the carrier from the time it receives the notice until the end of that day. The carrier must preserve this data for up to 90 days.
- *Ongoing domestic preservation notice* — requires the preservation of all stored communications held by the carrier from the time the notice is received until the end of the 29th day after the day the notice is received. The carrier must preserve this data for

up to 90 days. Only interception agencies may give an ongoing domestic preservation notice.

- *Foreign preservation notice* — requires the preservation of all stored communications that a carrier holds from the time they receive the notice until the end of the day where the stored communication relates to the specified person and is in connection with a serious contravention of foreign laws. Only the AFP may give a foreign preservation notice.

An issuing agency that has given a domestic preservation notice may revoke the notice at any time, but must revoke the notice if the grounds on which the notice was issued ceases to exist. Revocation is achieved through giving notice of revocation to the carrier.

The AFP must revoke a foreign preservation notice if either the foreign entity did not make a request for access to stored communications within 180 days, or a request is made but the Attorney-General refuses access to the communication.

Subsection 161A(1) of the TIA Act provides that this report must set out the relevant statistics about domestic preservation notices and revocation notices that were given by the agency during the year.

This information is in **Table 28**. In 2024–25, 1,637 domestic preservation notices were given. This is an increase of 80 notices on the 1,557 given in 2023–24.

Table 28: Domestic preservation notices – subsection 161A(1)

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	23/24	24/25	23/24	24/25
AFP	141	194	-	43
CCC (WA)	3	2	-	-
Home Affairs	2	-	-	-
IBAC	10	1	5	1
ICAC (SA)	-	3	-	3
LECC	-	3	-	-
NACC	1	7	1	3
NSW CC	1	-	1	-
NSW Police	595	692	163	136
NT Police	96	72	63	45
QLD CCC	11	7	1	4
QLD Police	239	211	61	86
SA Police	39	51	33	36
TAS Police	70	94	27	49
VIC Police	147	163	27	32
WA Police	202	137	123	65
TOTAL	**1,557**	**1,637**	**505**	**503**

Subsection 161A(2) of the TIA Act provides that this report must set out the relevant statistics about foreign preservation notices and revocation notices given by the AFP during the year.

In 2024–25, no foreign preservation notices or revocation notices were given. This is the same as in 2023–24.

International assistance

International assistance applications for stored communications must relate to international offences and are made as a result of an authorisation under:

- section 15B of the *Mutual Assistance in Criminal Matters Act 1987*
- section 78A of the *International Criminal Court Act 2002*, or
- section 34A of the *International War Crimes Tribunals Act 1995*.

An 'international offence' is:

- an offence against a law of a foreign country
- a crime within the jurisdiction of the International Criminal Court, or
- a War Crimes Tribunal Offence.

Paragraphs 162(1)(c) and 162(2)(ba) provide that this report must set out the number of stored communications warrant applications made as a result of international assistance applications.

Paragraphs 162(1)(d) and 162(2)(e) provide that this report must list, for each international offence in respect of which a stored communications warrant application was made as a result of an international assistance application made by the agency during the year — the offence under a law of the Commonwealth, or of a State or Territory that is of the same, or substantially similar nature to, the international offence.

In 2024–25, no applications were made for stored communications warrants as a result of an international assistance application. This is the same as in 2023–24.

Paragraph 163A of the TIA Act provides that this report must detail information regarding the number of occasions in which lawfully accessed information or stored communications warrant information was provided to:

- a foreign country
- the International Criminal Court, and
- a War Crimes Tribunal.

In 2024–25, there were no occasions in which lawfully accessed information or stored communications warrant information was provided to a foreign country, the International Criminal Court or a War Crimes Tribunal. This is the same as in 2023–24.

Ombudsman inspection report

The Ombudsman inspects the preservation notice and stored communications access records of all criminal law-enforcement agencies. Under section 186J of the TIA Act, the Ombudsman is required to report on the results of these inspections to the Minister for Home Affairs.

The Minister for Home Affairs must cause a copy of the Ombudsman's inspection reports to be laid before each House of Parliament within 15 sitting days of that House after the inspection report is received.

The Ombudsman's inspection reports on agency compliance with Chapters 3 and 4 of the TIA Act can be found at www.ombudsman.gov.au.

Chapter 4: Telecommunications data

Definition

‘Telecommunications data’ includes:

- information about a communication, such as the phone numbers of the people who called each other, how long they talk to each other, the email address from which a message was sent and the time the message was sent; and
- customer information about a service, such as customer name, address or billing details.

Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits ‘enforcement agencies’ to authorise carriers to disclose telecommunications data where the disclosure is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, the protection of the public revenue, or to locate a missing person.

Telecommunications data is often the first source of lead information for an investigation, helping to eliminate potential suspects and to support applications for more privacy intrusive investigative tools, including search warrants and interception warrants.

Definition

‘Enforcement agency’ is defined as a criminal law-enforcement agency or an authority or body for which a declaration is in force. A declaration remains in force for 40 Parliamentary sitting days.

During the reporting period, Corrective Services NSW, as part of the New South Wales Department of Communities and Justice, was declared as an enforcement agency.

Definitions

‘Existing data’, also known as ‘historical data’, is information that is already in existence when an authorisation for disclosure is received by a carrier.

‘Prospective data’ is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

Existing data – enforcement of the criminal law

Section 178 of the TIA Act provides that an authorised officer of an enforcement agency can authorise the disclosure of telecommunications data if the officer is satisfied the disclosure is reasonably necessary for the enforcement of the criminal law.

Paragraph 186(1)(a) and subsection 186(2) of the TIA Act provide that this report must set out the number of authorisations made under section 178 of the TIA Act by agencies during the year.

This information is provided in **Table 29**. In 2024–25, there were 357,864 authorisations made by agencies under section 178 of the TIA Act. This is an increase of 4,496 from the 353,368[27] authorisations made in 2023–24.

Table 29: Authorisations made by an enforcement agency for access to existing information or documents for the enforcement of the criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	23/24	24/25
ACCC	45	42
ACIC	3,811	2,560
AFP	11,711	13,015
ASIC	301[28]	282
CS NSW	10	12
CCC (WA)	49	47
Home Affairs	2,706	2,464
IBAC	182	166
ICAC (NSW)	198	330
ICAC (SA)	47	92
LECC	395	283
NACC[29]	332	287
NSW CC	2,104	1,780
NSW Police	124,079	126,775
NT Police	2,334[30]	2,162
QLD CCC	443	484[31]
QLD Police	31,125	31,767
SA Police	6,562	5,756

[27] This includes adjustments made to the 2023–24 Annual Report (see Appendix D).
[28] The figure for ASIC for the 2023–24 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).
[29] From 1 July 2023 ACLEI was subsumed into the NACC. While ACLEI is no longer operational, information about the use of TIA Act powers between 1 July 2022 and 30 June 2023 by ACLEI is provided in this table.
[30] The figure for NT Police for the 2023–24 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).
[31] QLD CCC reported that one authorisation was inadvertently submitted on a section 179 internal template and the notice was issued to the carrier under the correct s178 authorisation. This information was quarantined once identified and a new request was issued and authorised under the correct section 178 internal form.

Agency	Authorisations	
	23/24	24/25
TAS Police	3,089[32]	3,624
VIC Police	129,561[33]	136,155
WA Police	34,284	29,781
TOTAL	**353,368**[34]	**357,864**

Existing data – assist in locating a missing person

Section 178A of the TIA Act provides that an authorised officer of the AFP or the police force of a state or territory can authorise the disclosure of telecommunications data if the officer is satisfied the disclosure is reasonably necessary for the purposes of finding a person that has been reported missing.

Paragraph 186(1)(aa) and subsection 186(2) of the TIA Act provides that this report must set out the number of authorisations made under section 178A by agencies during the reporting period. This information is presented in **Table 30**.

In 2024–25, there were 6,507 authorisations made by agencies under section 178A of the TIA Act. This is an increase of 622 from the 5,885 authorisations made in 2023–24.

Table 30: Authorisations made for access to existing information or documents for the location of missing persons – paragraph 186(1)(aa)

Agency	Authorisations	
	23/24	24/25
AFP	48	37
NSW Police	3,641	4,052
NT Police	28	7
QLD Police	635	435
SA Police	150	80
TAS Police	116	40
VIC Police	973	1,661
WA Police	294	195
TOTAL	**5,885**	**6,507**

[32] The figure for TAS Police for the 2023–24 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).
[33] Victoria Police has reported that 520 of these authorisations were inadvertently given for missing persons.
[34] This reflects amendments made to the figures for ASIC, NT Police and Tas Police for the 2023–24 reporting period due to errors (refer to Appendix D of this Annual Report).

Existing data – enforcement of a law imposing a pecuniary penalty or protecting public revenue

Section 179 of the TIA Act provides that an authorised officer of an enforcement agency can authorise the disclosure of telecommunications data if the officer is satisfied the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Paragraph 186(1)(b) and subsection 186(2) of the TIA Act provide that this report must set out the number of authorisations made under section 179 by agencies during the reporting period.

This information is presented in **Table 31**. In 2024–25, there were 497 authorisations made by agencies under section 179 of the TIA Act. This is a decrease of 198 from the 695[35] authorisations made in 2023–24.

Table 31: Authorisations made for access to existing information or documents for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(b)

Agency	Authorisations	
	23/24	24/25
ACCC	21	17
AFP	17	11
ASIC	3[36]	20
Home Affairs	36	15
NSW Police	598	412
NT Police	-	13
SA Police	-	1
TAS Police	2	4
WA Police	18	4
TOTAL	**695[37]**	**497**

Prospective data – authorisations

Section 180 of the TIA Act provides that an authorised officer of a criminal law-enforcement agency may authorise the disclosure of prospective data if they are satisfied the disclosure is reasonably necessary for the investigation of a serious offence or an offence against a law of the Commonwealth, a State or a Territory that is punishable by

[35] This includes adjustments made to the 2023–24 Annual Report (see Appendix D).
[36] The figure for ASIC for the 2023–24 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).
[37] This reflects amendments made to the figures for ASIC for the 2023–24 reporting period due to an error (refer to Appendix D of this Annual Report).

imprisonment for at least three years. Prospective data authorisations may also authorise the disclosure of historical data.

Paragraph 186(1)(c) and subsection 186(2) of the TIA Act provides that this report must set out the number of authorisations made under section 180 of the TIA Act by agencies during the reporting period.

This information is presented in **Table 32**. In 2024–25, there were 49,482 prospective data authorisations made by agencies under section 180 of the TIA Act. This is a decrease of 3,381 from the 52,863 authorisations made in 2023–24.

Table 32: Total number of prospective data authorisations made – paragraph 186(1)(c)

Agency	Number of authorisations made	
	23/24	24/25
ACCC	7	27
ACIC	1,042	710
AFP	12,613	7,623
ASIC	50	53
CCC (WA)	19	14
Home Affairs	372	341
IBAC	77	93
ICAC (NSW)	41	61
ICAC (SA)	-	30
LECC	171	70
NACC	44	38
NSW CC	1,300	1,284
NSW Police	3,788	4,870
NT Police	568	500
QLD CCC	111	108
QLD Police	6,391	7,563
SA Police	497	644
TAS Police	212	332
VIC Police	19,181[38]	18,166
WA Police	6,379	6,955
TOTAL	**52,863**	**49,482**

[38] Victoria Police has reported that 35 of these authorisations were inadvertently given for missing persons.

Data authorisations for foreign law enforcement

Division 4A of Part 4-1 of the TIA Act provides that the AFP may authorise the disclosure of telecommunications data where the disclosure is reasonably necessary for:

- the enforcement of the criminal law of a foreign country
- an investigation or prosecution of a crime within the jurisdiction of the International Criminal Court, or
- an investigation or prosecution of a War Crimes Tribunal offence.

However, for the disclosure of prospective telecommunications data, the Attorney-General must first give an authorisation under:

- section 15D of the *Mutual Assistance in Criminal Matters Act 1987*
- section 78B of the *International Criminal Court Act 2002*, or
- section 34B of the *International War Crimes Tribunal Act 1995*.

The AFP may authorise the disclosure of telecommunications data obtained under an authorisation for foreign law enforcement for the performance by the Australian Security Intelligence Organisation (ASIO) of its functions, the enforcement of the criminal law or a law imposing a pecuniary penalty, the protection of the public revenue, or the purpose of Division 105A of the *Criminal Code*, relating to post-sentence orders.

Paragraph 186(1)(ca) and subsection 186(2) of the TIA Act provide that this report must set out the number of authorisations made by the AFP under sections 180A, 180B, 180C and 180D of the TIA Act during the year.

In 2024–25, the AFP made the following authorisations under section 180A, 180B, 180C, and 180D of the TIA Act:

- 95 authorisations under section 180A
- no authorisations under section 180B
- four authorisations under section 180C, and
- no authorisations under section 180D.

The AFP made 29 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: Bangladesh (one disclosure), Bhutan (one disclosure), Bulgaria (one disclosure), Canada (two disclosures), France (one disclosure), Germany (two disclosures), India (two disclosures), Japan (two disclosures), New Zealand (one disclosure), Philippines (four disclosures), Poland (one disclosure), Romania (one disclosure), Switzerland (two disclosures), Taiwan Province (one disclosure), the United Kingdom (one disclosure) and the United States of America (six disclosures).

Offences for which authorisations were made

Paragraph 186(1)(e) and subsection 186(2) of the TIA Act provide that this report must set out the offences and other matters for which authorised officers of each agency made authorisations under sections 178, 178A, 179 and 180 of the TIA Act. Information relating to sections 178, 179 and 180 are presented in **Tables 33, 33A, 33B, 33C, 34, 35, 35A, 35B and 35C**.

Authorisations for existing telecommunications data covered a range of crimes, including 59,076 authorisations for illicit drugs offences, 42,843 for abduction and 38,452 authorisations for unlawful entry.

Under section 178A of the TIA Act, 6,310 requests were made in relation to missing persons.

The total number of offences is typically larger than the total number of authorisations issued, as an authorisation can be issued to investigate more than one offence.

Table 33: Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Category of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Abduction	196	42,568	79	**42,843**
Acts – injury	150	19,241	13	**19,404**
Bribery or corruption	346	188	835	**1,369**
Cartel offences	42	8	-	**50**
Conspire/aid/abet serious offence	27	1,014	-	**1,041**
Cybercrime and telecommunications	548	5,461	5	**6,014**
Dangerous acts	49	6,661	9	**6,719**
Fraud	2,227	21,620	401	**24,248**
Homicide	352	32,665	237	**33,254**
Illicit drug offences	6,853	51,159	1,064	**59,076**
Loss of life	15	1,064	3	**1,082**
Miscellaneous	880	11,575	284	**12,739**
Justice procedures	120	2,419	36	**2,575**
Organised crime	418	4,506	18	**4,942**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	10	976	1	**987**
Public revenue	21	796	-	**817**
People smuggling	392	3	-	**395**
Weapons	240	6,985	104	**7,329**
Property damage	44	2,461	-	**2,505**
Public order offences	4	1,078	-	**1,082**
Robbery, extortion and related offences	150	20,349	4	**20,503**

Category of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Serious damage	5	8,567	-	**8,572**
Sexual assault	3,732	23,614	-	**27,346**
Terrorism offences	1,662	666	2	**2,330**
Theft	147	29,122	95	**29,364**
Traffic	11	2,923	3	**2,937**
Unlawful entry	111	38,340	1	**38,452**
TOTAL	**18,752**	**336,029**	**3,194**	**357,975**

Table 33A: Commonwealth agencies – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	ACCC	ACIC[39]	AFP	ASIC	Home Affairs	NACC	TOTAL
Abduction	-	-	196	-	-	-	**196**
Acts – injury	-	-	150	-	-	-	**150**
Bribery or corruption	-	-	36	-	-	310	**346**
Cartel offences	42	-	-	-	-	-	**42**
Conspire/aid/abet serious offence	-	-	27	-	-	-	**27**
Cybercrime and telecommunications	-	-	539	9	-	-	**548**
Dangerous acts	-	-	49	-	-	-	**49**
Fraud	-	1,329	522	276	59	41	**2,227**
Homicide	-	-	352	-	-	-	**352**
Illicit drug offences	-	1,191	4,068	-	1,594	-	**6,853**

[39] The ACIC has commenced reporting authorisations against specific offence categories, rather than the broader 'special ACIC investigation' category, to achieve a more precise background.

Categories of offences	ACCC	ACIC[39]	AFP	ASIC	Home Affairs	NACC	TOTAL
Loss of life	-	-	15	-	-	-	**15**
Miscellaneous	-	2	402	21	455	-	**880**
Justice procedures	-	-	120	-	-	-	**120**
Organised crime	-	-	418	-	-	-	**418**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	-	-	-	10	-	-	**10**
Public revenue	-	19	-	2	-	-	**21**
People smuggling	-	-	392	-	-	-	**392**
Weapons	-	-	65	-	175	-	**240**
Property damage	-	-	44	-	-	-	**44**
Public order offences	-	-	4	-	-	-	**4**
Robbery, extortion and related offences	-	-	150	-	-	-	**150**
Serious damage	-	-	5	-	-	-	**5**
Sexual assault	-	-	3,560	-	172	-	**3,732**
Terrorism offences	-	-	1,662	-	-	-	**1,662**
Theft	-	21	117	-	9	-	**147**
Traffic	-	-	11	-	-	-	**11**
Unlawful entry	-	-	111	-	-	-	**111**
TOTAL	**42**	**2,562**	**13,015**	**318**	**2,464**	**351**	**18,752**

Table 33B: State and Territory Police – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	17,147	181	3,626	253	416	17,958	2,987	**42,568**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Acts – injury	10,462	38	977	273	163	5,197	2,131	**19,241**
Bribery or corruption	-	3	16	54	1	74	40	**188**
Cartel offences	8	-	-	-	-	-	-	**8**
Conspire/aid/abet serious offence	356	4	10	6	6	603	29	**1,014**
Cybercrime and telecommunications	3,602	29	948	23	350	348	161	**5,461**
Dangerous acts	1,054	70	596	116	43	4,456	326	**6,661**
Fraud	7,923	40	1,612	511	142	9,912	1,480	**21,620**
Homicide	18,497	201	1,781	930	157	10,248	851	**32,665**
Illicit drug offences	17,302	1,007	7,716	1,771	882	16,247	6,234	**51,159**
Loss of life	551	13	116	1	12	371	-	**1,064**
Miscellaneous	6,762	178	3,553	70	71	659	282	**11,575**
Justice procedures	588	2	70	67	209	633	850	**2,419**
Organised crime	3,848	9	113	60	10	36	430	**4,506**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	856	1	106	4	3	6	-	**976**
Public revenue	-	1	1	-	-	794	-	**796**
People smuggling	-	1	2	-	-	-	-	**3**
Weapons	2,665	7	545	122	118	3,498	30	**6,985**
Property damage	1,948	7	367	93	15	31	-	**2,461**
Public order offences	142	-	26	2	3	803	102	**1,078**
Robbery, extortion and related offences	6,793	56	1,889	186	68	9,338	2,019	**20,349**
Serious damage	1,714	16	484	53	89	5,779	432	**8,567**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Sexual assault	9,498	225	3,291	574	225	7,197	2,604	**23,614**
Terrorism offences	380	1	10	-	10	249	16	**666**
Theft	9,814	34	1,983	114	273	13,607	3,297	**29,122**
Traffic	792	4	188	6	27	1,357	549	**2,923**
Unlawful entry	4,073	34	1,741	476	331	26,754	4,931	**38,340**
TOTAL	**126,775**	**2,162**	**31,767**	**5,765**	**3,624**	**136,155**	**29,781**	**336,029**

Table 33C: State and Territory Integrity Agencies – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	CS NSW	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Abduction	-	-	-	-	-	-	79	-	**79**
Acts – injury	-	-	-	-	-	4	9	-	**13**
Bribery or corruption	-	45	121	308	92	201	-	68	**835**
Cybercrime and telecommunications	-	-	-	-	-	1	-	4	**5**
Dangerous acts	-	-	-	-	-	7	2	-	**9**
Fraud	-	2	33	22	-	27	205	112	**401**
Homicide	-	-	-	-	-	-	237	-	**237**
Illicit drug offences	-	-	-	-	-	17	989	58	**1,064**
Loss of life	-	-	-	-	-	-	3	-	**3**
Miscellaneous	12	-	-	-	-	1	29	242	**284**
Justice procedures	-	-	12	-	-	24	-	-	**36**
Organised crime	-	-	-	-	-	-	18	-	**18**
Other offences relating to the enforcement of a law	-	-	-	-	-	-	1	-	**1**

Categories of offences	CS NSW	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
imposing a pecuniary penalty									
Weapons	-	-	-	-	-	-	104	-	**104**
Robbery, extortion and related offences	-	-	-	-	-	-	4	-	**4**
Sexual assault	-	-	-	-	-	1	1	-	**2**
Terrorism offences	-	-	-	-	-	-	95	-	**95**
Theft	-	-	-	-	-	-	3	-	**3**
Unlawful entry	-	-	-	-	-	-	1	-	**1**
TOTAL	**12**	**47**	**166**	**330**	**92**	**283**	**1,780**	**484**	**3,194**

Table 34: Matters for which authorisations were made under section 179 for access to existing data for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(e)

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NSW Police	NT Police	SA Police	TAS Police	WA Police	TOTAL
Abduction	-	-	1	-	53	-	-	-	-	**54**
Acts – injury	-	-	-	-	12	-	-	-	-	**12**
Cartel offences	1	-	-	-	-	-	-	-	-	**1**
Cybercrime and telecommunications	-	-	-	-	25	-	-	-	-	**25**
Dangerous acts	-	-	-	-	2	-	-	-	-	**2**
Fraud	-	-	19	-	35	-	-	-	-	**54**
Homicide	-	-	-	-	4	-	-	-	-	**4**
Illicit drug offences	-	-	-	-	13	1	-	-	-	**14**
Loss of life	-	-	-	-	17	-	-	-	-	**17**
Miscellaneous	-	-	6	7	50	10	1	-	-	**74**

Categories of offences	ACCC	AFP	ASIC	Home Affairs	NSW Police	NT Police	SA Police	TAS Police	WA Police	TOTAL
Justice procedures	-	-	-	-	2	-	-	3	-	**5**
Organised crime	-	-	-	-	7	-	-		-	**7**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	16	10	4	-	108	-	-	1	-	**139**
Public revenue	-	1	-	-	-	2	-	-	-	**3**
Weapons	-	-	-	1	2	-	-	-	-	**3**
Property damage	-	-	-	-	2	-	-	-	3	**5**
Robbery, extortion and related offences	-	-	1	-	8	-	-	-	-	**9**
Sexual assault	-	-	-	-	31	-	-	-	-	**31**
Terrorism offences	-	-	-	7	-	-	-	-	-	**7**
Theft	-	-	-	-	20	-	-	-	-	**20**
Traffic offences	-	-	-	-	16	-	-	-	1	**17**
Unlawful entry	-	-	-	-	5	-	-	-	-	**5**
TOTAL	**17**	**11**	**31**	**15**	**412**	**13**	**1**	**4**	**4**	**508**

Table 35: Offences against which authorisations were made under section 180 for access to specified information or documents that came into existence during the period for which an authorisation is in force – paragraph 186(1)(e)

Categories of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Abduction	65	3,719	17	**3,801**
Acts – injury	17	2,897	2	**2,916**
Bribery or corruption	55	21	238	**314**
Cartel offences	27	2	-	**29**

Categories of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Conspire/aid/abet serious offence	39	173	-	**212**
Cybercrime and telecommunications	222	155	-	**377**
Dangerous acts	23	773	1	**797**
Fraud	668	1,093	199	**1,960**
Homicide	104	828	33	**965**
Illicit drug offences	3,184	11,064	865	**15,113**
Loss of life	20	383	6	**409**
Miscellaneous	242	875	48	**1,165**
Justice procedures	25	395	14	**434**
Organised crime	2,812	229	24	**3,065**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	-	10	-	**10**
Public revenue	83	26	-	**109**
People smuggling	233	-	-	**233**
Weapons	157	1,159	189	**1,505**
Property damage	6	145	-	**151**
Public order offences	-	125	-	**125**
Robbery, extortion and related offences	61	1,952	6	**2,019**
Serious damage	2	739	-	**741**
Sexual assault	485	2,226	1	**2,712**
Terrorism offences	386	35	15	**436**
Theft	119	3,533	2	**3,654**
Traffic	10	238	-	**248**
Unlawful entry	52	6,200	-	**6,252**
TOTAL	**9,097**	**38,995**	**1,660**	**49,752**

Table 35A: Commonwealth agencies – Offences against which authorisations were made under section 180 for access to specified information or documents that came into existence during the period for which an authorisation is in force – paragraph 186(1)(e)

Categories of offences	ACCC	ACIC[40]	AFP	ASIC	Home Affairs	NACC	TOTAL
Abduction	-	-	65	-	-	-	**65**
Acts – injury	-	-	17	-	-	-	**17**
Bribery or corruption	-	-	21	-	-	34	**55**
Cartel offences	27	-	-	-	-	-	**27**
Conspire/aid/abet serious offence	-	-	39	-	-	-	**39**
Cybercrime and telecommunications	-	-	222	-	-	-	**222**
Dangerous acts	-	-	23	-	-	-	**23**
Fraud	-	297	296	53	13	9	**668**
Homicide	-	-	104	-	-	-	**104**
Illicit drug offences	-	423	2,611	-	150	-	**3,184**
Loss of life	-	-	20	-	-	-	**20**
Miscellaneous	-	-	165	4	73	-	**242**
Justice procedures	-	-	25	-	-	-	**25**
Organised crime	-	-	2,812	-	-	-	**2,812**
Public revenue	-	14	69	-	-	-	**83**
People smuggling	-	-	233	-	-	-	**233**
Weapons	-	-	83	-	74	-	**157**
Property damage	-	-	6	-	-	-	**6**
Robbery, extortion and related offences	-	-	61	-	-	-	**61**

[40] The ACIC has commenced reporting authorisations against specific offence categories, rather than the broader 'special ACIC investigation' category, to achieve a more precise background.

Categories of offences	ACCC	ACIC[40]	AFP	ASIC	Home Affairs	NACC	TOTAL
Serious damage	-	-	2	-		-	**2**
Sexual assault	-	-	454	-	31	-	**485**
Terrorism offences	-	-	386	-	-	-	**386**
Theft	-	37	82	-	-	-	**119**
Traffic	-	-	10	-	-	-	**10**
Unlawful entry	-	-	52	-	-	-	**52**
TOTAL	**27**	**771**	**7,858**	**57**	**341**	**43**	**9,097**

Table 35B: State and Territory Police – Offences against which authorisations were made under section 180 for access to specified information or documents that came into existence during the period for which an authorisation is in force – paragraph 186(1)(e)

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	428	29	778	58	20	2,042	364	**3,719**
Acts – injury	753	7	47	32	1	1,490	567	**2,897**
Bribery or corruption	-	-	3	-	-	15	3	**21**
Cartel offences	1	-	-	1	-	-	-	**2**
Conspire/aid/abet serious offence	36	2	4	-	-	119	12	**173**
Cybercrime and telecommunications	101	10	27	2	2	6	7	**155**
Dangerous acts	10	2	78	9	-	647	27	**773**
Fraud	116	7	164	14	-	679	113	**1,093**
Homicide	132	2	214	34	2	401	43	**828**
Illicit drug offences	1,388	345	3,528	257	238	2,654	2,654	**11,064**
Loss of life	25	2	35	2	-	319	-	**383**
Miscellaneous	225	33	45	6	21	447	98	**875**
Justice procedures	91	7	48	10	1	58	180	**395**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Organised crime	42	4	22	9	-	14	138	**229**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	10	-	-	-	-	-	-	**10**
Public revenue	-	-	-	-	-	26	-	**26**
Weapons	282	2	329	22	5	512	7	**1,159**
Property damage	85	4	51	2	-	2	1	**145**
Public order offences	1	-	-	-	-	95	29	**125**
Robbery, extortion and related offences	150	16	409	13	4	958	402	**1,952**
Serious damage	53	3	98	6	-	479	100	**739**
Sexual assault	152	14	477	80	14	978	511	**2,226**
Terrorism offences	1	-	-	-	-	34	-	**35**
Theft	211	5	702	12	20	1,840	743	**3,533**
Traffic	23	-	-	1	1	171	42	**238**
Unlawful entry	554	6	504	39	3	4,180	914	**6,200**
TOTAL	**4,870**	**500**	**7,563**	**609**	**332**	**18,166**	**6,955**	**38,995**

Table 35C: State and Territory Integrity Agencies – Offences against which authorisations were made under section 180 for access to specified information or documents that came into existence during the period for which an authorisation is in force – paragraph 186(1)(e)

Categories of offences	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Abduction	-	-	-	-	-	17	-	**17**
Acts – injury	-	-	-	-	-	2	-	**2**
Bribery or corruption	13	87	59	30	47	-	2	**238**
Dangerous acts	-	-	-	-	1	-	-	**1**
Fraud	1	6	2	-	8	149	33	**199**

Categories of offences	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Homicide	-	-	-	-	-	33	-	**33**
Illicit drug offences	-	-	-	-	-	828	37	**865**
Loss of life	-	-	-	-	-	6	-	**6**
Miscellaneous	-	-	-	-	-	12	36	**48**
Justice procedures	-	-	-	-	14	-	-	**14**
Organised crime	-	-	-	-	-	24	-	**24**
Weapons	-	-	-	-	-	189	-	**189**
Robbery, extortion and related offences	-	-	-	-	-	6	-	**6**
Sexual assault	-	-	-	-	-	1	-	**1**
Terrorism offences	-	-	-	-	-	15	-	**15**
Theft	-	-	-	-	-	2	-	**2**
TOTAL	**14**	**93**	**61**	**30**	**70**	**1,284**	**108**	**1,660**

Age of data under disclosure

Paragraph 186(1)(f) and subsection 186(2) of the TIA Act provide that this report must set out the lengths of time for which information or documents covered by data authorisations had been held by a service provider before the authorisations for that information were made.

This information is provided in **Table 36**. The statistics are split into successive periods of three months and include the total number of authorisations made for data held for lengths of time specified, in accordance with subsection 180(1C) of the TIA Act.

In 2024–25, there were 272,692 authorisations for data 0–3 months old. This includes authorisations for 'point in time' information without an identifiable age, such as current subscriber information and current information held in the Integrated Public Number Database, which have been recorded as '0' months old and are included in the 0–3 month field.[41]

[41] The Integrated Public Number Database is an industry-wide database, managed by Telstra, containing all listed and unlisted public telephone numbers.

Table 36: Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)

Agency	Age of disclosure									
	0–3 months	3–6 months	6–9 months	9–12 months	12–15 months	15–18 months	18–21 months	21–24 months	Over 24 months	TOTAL
ACCC	15	1	3	2	-	1	4	6	27	**59**
ACIC	2,001	236	88	59	52	47	35	11	68	**2,597**
AFP	5,017	2,992	1,791	965	875	295	175	150	803	**13,063**
ASIC	71	34	15	16	6	3	8	2	34	**189**
CS NSW	2	8	1	1	-	-	-	-	-	**12**
CCC (WA)	31	1	5	4	3	-	-	-	3	**47**
Home Affairs	1,708	280	159	72	42	47	45	54	72	**2,479**
IBAC	221	4	2	1	4	-	1	4	22	**259**
ICAC (NSW)	92	15	16	7	12	6	4	5	173	**330**
ICAC (SA)	54	13	2	2	-	1	-	3	17	**92**
LECC	303	25	12	4	-	-	2	5	2	**353**
NACC	188	20	10	9	18	2	5	26	47	**325**
NSW CC	564	138	23	36	40	25	6	69	48	**949**
NSW Police	75,280	2,132	1,853	1,725	804	640	376	451	1,045	**84,306**
NT Police	1,849	39	10	14	7	3	1	9	250	**2,182**
QLD CCC	292	52	54	24	5	3	6	13	35	**484**
QLD Police	27,600	1,669	889	530	382	235	178	133	580	**32,196**
SA Police	4,370	388	259	159	60	67	50	92	392	**5,837**
TAS Police	2,804	316	120	96	68	47	32	51	134	**3,668**
VIC Police	126,650	3,614	1,712	1,061	743	509	373	258	596	**135,516**
WA Police	23,580	2,371	1,048	676	693	308	234	161	-	**29,071**
TOTAL	**272,692**	**14,348**	**8,072**	**5,463**	**3,814**	**2,239**	**1,535**	**1,503**	**4,348**	**314,014**

Types of data retained

Paragraphs 186(1)(g)–(h) and subsection 186(2) of the TIA Act provide that this report must set out the number of occasions during the reporting period that agencies made authorisations for retained data which included information from the data subsets identified in subsection 187AA(1). The data subsets in subsection 187AA(1) can be broadly grouped into two categories:

- 'Subscriber data' which includes information about a telecommunications service[42], and
- 'Traffic data' which includes information such as the time, duration, and source of a communication[43].

This information is presented in **Table 37**. Subscriber information and other customer identification information constitute the majority of authorisations. This type of information is commonly used at the beginning of an investigation to identify and eliminate suspects.

Table 37: Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)[44]

Agency	Subscriber data	Traffic data
ACCC	42	17
ACIC	1,619	977
AFP	10,371	2,692
ASIC	142	177
CS NSW	11	4
CCC (WA)	20	27
Home Affairs	2,030	1,149
IBAC	138	63
ICAC (NSW)	94	236
ICAC (SA)	43	49
LECC	205	78
NACC	177	180
NSW CC	860	906
NSW Police	85,338	45,901
NT Police	1,571	609
QLD CCC	356	128
QLD Police	23,712	5,984
SA Police	4,409	1,496
TAS Police	2,443	1,225

[42] Subscriber data is covered by item 1 of the table in subsection 187AA(1).
[43] Traffic data is covered by items 2 to 6 of the table in subsection 187AA(1).
[44] An agency can request both types of data in a single request.

Agency	Subscriber data	Traffic data
VIC Police	76,942	60,245
WA Police	23,177	13,758
TOTAL	**233,700**	**135,901**

Journalist information warrants

The journalist information warrant (JIW) scheme requires agencies to obtain a JIW prior to authorising the disclosure of telecommunications data relating to a journalist or their employer, for the purpose of identifying a journalist's source.

Paragraphs 186(1)(i)–(j) of the TIA Act provide that this report must set out the number of JIWs issued to agencies during the reporting period and the number of authorisations made under JIWs issued to those agencies.

This information is presented in **Table 38** and **Table 39**. In 2024–25 one historical data authorisation was made under one JIW issued to SA Police for the enforcement of the criminal law. This is an increase of one from 2023–24.

Table 38: Journalist information warrants issued – paragraph 186(1)(j)

Agency	Warrants issued	
	23/24	24/25
SA Police	-	1
TOTAL	**-**	**1**

Table 39: Number of authorisations made under journalist information warrants – paragraph 186(1)(i)

Agency	Authorisations made				
	S178	S178A	S179	S180	TOTAL
SA Police	1		-	-	**1**
TOTAL	**1**		**-**	**-**	**1**

To issue a JIW, the issuing authority must, amongst other things, have regard to any submissions made by a Public Interest Advocate (PIA). The Prime Minister may declare the following persons to be PIAs:

- a King's Counsel or Senior Counsel who has been cleared for security purposes to a level the Prime Minister considers to be appropriate, or
- a former Judge.

A PIA may make a submission to an issuing authority (or the Attorney-General in the case of ASIO) about matters relevant to a decision to issue, refuse, or specify conditions in a JIW. In the case of oral applications, they can attend the hearing of the application.

Table 40 sets out information about the number of PIAs, their location and qualification as of 30 June 2024 in accordance with the recommendations of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press.

Table 40: Public interest advocates

Public interest advocates	Location	Qualification
1	Queensland	Former Judge
2	Victoria	Former Judge
3	Northern Territory	Senior Counsel
4	Western Australia	Former Judge
5	South Australia	Former Judge

Industry estimated cost of implementing data retention

Carriers and carriage service providers must comply with the data and data retention obligations in Part 5-1A of the TIA Act. Section 187P of the TIA Act provides that this report must include information about the costs to service providers of complying with the data retention scheme and the use of data retention implementation plans.

Table 41 shows the cost of complying with the data retention obligations, based on information collected from industry by the Australian Communications and Media Authority, and the costs recovered from criminal law-enforcement agencies.

Table 41: Industry capital cost of data retention – section 187P

Financial year	Data retention compliance cost (GST inclusive) (*exclusive of data retention industry grants*)	Costs recovered from criminal law-enforcement agencies (GST inclusive)
2023–24	$29,729,879.35	$17,111,920.00
2024–25	$37,106,182.52	$18,742,142.50

Chapter 5: International production orders

Schedule 1 to the TIA Act enables Australian agencies to obtain international production orders for interception, stored communications, and telecommunications data from prescribed communications providers in countries with which Australia has a designated international agreement.

There is only one designated international agreement under the International Production Order framework, namely, the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (the Agreement) which entered into force on 31 January 2024.

Definition

'Prescribed communication provider' is defined in clause 2 of Schedule 1 to the TIA Act as a network entity, a transmission service provider, a message/call application service provider, a storage/back-up service provider, or a general electronic service provider.

Agencies that are eligible to apply for stored communications and interception warrants under Chapters 2 and 3 of the TIA Act can apply for international production orders for the equivalent information. Similarly, agencies that can authorise the disclosure of telecommunications data under Chapter 4 of the TIA Act may apply for international production orders seeking telecommunications data.

During the reporting period, the AFP and NSW Police were the only two agencies certified to use the International Production Order Framework.

Agencies report on applications for international production orders

Applications for enforcement of the criminal law

Paragraphs 128(a)–(c) of Schedule 1 to the TIA Act provides that this report must set out for each relevant agency how many international production order applications were submitted to an issuing authority relating to interception, stored communications and telecommunications data for the enforcement of the criminal law.

This information is provided in **Table 42**. In 2024–25, there were 100 international production orders issued in response to applications relating to stored communication, five orders issued in response to applications relating to telecommunications data and no applications relating to interception.[45] There were no international production orders in 2023–24 as work was still on foot to put the Agreement into practical operation.

[45] There was a technical issue in Schedule 1 to the TIA Act which prevented US prescribed communications providers from producing prospective content data where they do not have the

Table 42: Applications for international production orders relating to interception, stored communications and telecommunications data for the enforcement of the criminal law – paragraphs 128(a)–(c) of Schedule 1

Agency	Relevant statistics	Applications relating to interception		Applications relating to Stored Communications		Applications relating to Telecommunications data	
		23/24	24/25	23/24	24/25	23/24	24/25
AFP	Made	-	-	-	90	-	4
	Withdrawn	-	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	-	-	90	-	4
NSW Police	Made	-	-	-	10	-	1
	Withdrawn	-	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	-	-	10	-	1
TOTAL	**Made**	**-**	**-**	**-**	**100**	**-**	**5**
	Withdrawn	**-**	**-**	**-**	**-**	**-**	**-**
	Refused	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**-**	**-**	**-**	**100**	**-**	**5**

Applications relating to a Part 5.3 supervisory orders

Paragraphs 128(d)–(f) of Schedule 1 to the TIA Act provides that this report must set out for each relevant agency how many international production order applications were submitted to an issuing authority relating to interception, stored communications and telecommunications data for Part 5.3 supervisory orders.

In 2024–25, no international production orders were submitted to an issuing authority for Part 5.3 supervisory orders. This is the same as 2023–24.

Applications for each designated international agreement

Paragraph 128(g) of Schedule 1 to the TIA Act provides that this report must also set out the number of international production order applications submitted to an issuing authority by an agency during the financial year, for each designated international agreement. As the only designated international agreement in place is the *Agreement between the Government of Australia and the Government of the United States of America on Access*

technical capability to do this in real-time. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2025*, which entered into force on 5 November 2025, contains amendments to rectify this issue. The amendments enable US providers to comply with international production orders where they do not have the capability to produce information in real time.

to Electronic Data for the Purpose of Countering Serious Crime, these figures are reported above in **Table 42**. In 2024–25, there were 105 international production orders applications.

The Australian Designated Authority report

Under clause 130, the Australian Designated Authority must report to the Minister for Home Affairs information and statistics relating to the functions of the Australian Designated Authority. That information must be included in this report.

International production orders given by the Australian Designated Authority

Subparagraphs 130(1)(a)(i) and 130(1)(a)(ii) of Schedule 1 to the TIA Act provide that this report must set out the number, and type, of international production orders given by the Australian Designated Authority to prescribed communications providers in response to applications made by the relevant agency. This information is provided in **Table 43**.

The statistics from the Australian Designated Authority in **Table 43**, relating to the total number of international production orders given to a prescribed communication provider in the 2024–25 period, differ marginally from the statistics from agencies in **Table 42** relating to the number of international production orders issued to the agency in response to applications made in 2024–25. This could result from:

- timing differences — for example, an international production order may be given to the Australian Designated Authority at the end of a reporting period but not given to a prescribed communications provider until the beginning of the next reporting period, or
- revocations or cancellations — an international production order issued to an agency could be revoked by the agency or cancelled by the Australian Designated Authority before it is given to the relevant prescribed communications provider

Table 43 shows that 91 international production orders were given to prescribed communications providers by the Australian Designated Authority in 2024–25. This number is lower than the number of applications made by agencies in 2024–25 (and the number of orders issued in respect of these applications) as reported in **Table 42**. This is due to orders issued to agencies being revoked or cancelled before being given to the relevant prescribed communications provider.

Table 43: Number of international production orders given by the Australian Designated Authority to prescribed communications providers – subparagraphs 130(1)(a)(i) and 130(1)(a)(ii) of Schedule 1

Agency	Interception[46]		Stored Communications		Telecommunications data		TOTAL	
	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25
AFP	-	-	-	76	-	4	**-**	**80**
NSW Police	-	-	-	10	-	1	**-**	**11**
TOTAL	**-**	**-**	**-**	**86**	**-**	**5**	**-**	**91**

Subparagraph 130(1)(a)(iii) of Schedule 1 to the TIA Act provides that this report must set out the number of international production orders given by the Australian Designated Authority that invoked the designated international agreement.

In 2024–25, 91 international production orders given by the Australian Designated Authority invoked the Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime.

In 2024–25, there were no IPOs given by the Australian Designated Authority to prescribed communications providers that were issued for the enforcement of the criminal law pursuant to paragraphs 30(2)(g)(ii) or 30(2)(h)(ii) of the TIA Act (which cover orders relating to another person).

In 2024–25 there were no IPOs given by the Australian Designated Authority to prescribed communications providers that were issued in relation to a Part 5.3 supervisory order pursuant to 60(2)(g)(ii) or 60(2)(h)(ii) of the TIA Act (which cover orders relating to another person).

International production orders cancelled by the Australian Designated Authority

Paragraphs 130(1)(d) and 130(1)(e) of Schedule 1 to the TIA Act provides that this report must set out the number of international production orders issued by a relevant agency and subsequently cancelled by the Australian Designated Authority under clause 111 and clause 122 of Schedule 1 to the TIA Act.

[46] There is a technical issue in Schedule 1 to the TIA Act which prevented US prescribed communications providers from producing prospective content data where they do not have the technical capability to do this in real-time. The *Telecommunications and Other Legislation Amendment Act 2025*, which commenced on 5 November 2025, contains amendments to rectify this issue.

This information is provided in **Table 44**. In 2024–25, the Australian Designated Authority cancelled three international production orders under clause 111 of Schedule 1 to the TIA Act. These international production orders were cancelled as they were purported to be issued by a judge that was not authorised to issue international production orders.

Table 344: Number of IPOs cancelled by the Australian Designated Authority under clause 111 – paragraph 130(1)(d) of Schedule 1

Agency	International production orders cancelled under clause 111	International production orders cancelled under clause 122
AFP	3	-
NSW Police	-	-
TOTAL	**3**	**-**

In 2024–25, there were no revocation instruments given by the Australian Designated Authority to prescribed communications providers.[47]

Objections received by the Australian Designated Authority

Objections to international productions orders are regulated by Part 7 of Schedule 1 to the TIA Act. Part 7 of Schedule 1 to the TIA Act provides that if an international production order is given to a prescribed communications provider, the provider may object to the international production order on the grounds that the international production order does not comply with the designated international agreement.

Paragraph 130(1)(g) and 130(1)(e) of Schedule 1 to the TIA Act provides that this report must set out any objections received by the Australian Designated Authority under clause 121 and the number of international production orders to which those objections relate to. This refers only to instances where a provider objected based on grounds listed in the designated international agreement.

This report must also set the number of each type of international production order.

This information is presented in **Table 45.** In 2024–25, two objections were received by the Australian Designated Authority for international production orders for purported non-compliance of the Agreement. One objection was received relating to telecommunications data and one objection was received for stored communications data. The Australian Designated Authority advised that both objections related to concerns raised by the prescribed communications providers that the target was a United States Receiving-Party Person, which is not permitted under the Agreement. The Australian Designated Authority advised that this was resolved in both instances following discussions with the prescribed communications provider and by providing further information from the relevant agency to

[47] The Australian Designated Authority advised that during the 2024–25 financial year, one revocation instrument was required to be given to the prescribed communications provider, but due to an administrative delay, this was given after the reporting period. This information will be included in the 2025–26 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

satisfy the prescribed communications provider that the target was not a US person.

Table 45: Number of international production orders issued that relate to objections received by the Australian Designated Authority under clause 121 – subparagraph 130(1)(g)(i) of Schedule 1

Agency	Stored communications		Telecommunications data		Interception		TOTAL	
	23/24	24/25	23/24	24/25	23/24	24/25	23/24	24/25
AFP	-	1	-	1	-	-	-	**2**
TOTAL	**-**	**1**	**-**	**1**	**-**	**-**	**-**	**2**

Effectiveness of international production orders

Paragraph 128(h) of Schedule 1 to the TIA Act provides this report must set out how many arrests were made during the year on the basis of protected information obtained through an international production order. This report must also set out how many proceedings, in which protected information was given in evidence, ended during the reporting period.

This information is presented in **Table 46.** In 2024–25, protected information:

- contributed to seven arrests
- was given in evidence in nine proceedings, and
- resulted in two convictions in proceedings where such information had been given in evidence.

The information in Table 46 should be interpreted with some caution, particularly in presuming a relationship between the number of arrests, prosecutions and convictions in a reporting period. For example, an arrest recorded in one reporting period may not result in a prosecution until a later reporting period. The statistics may also understate the effectiveness of international production orders, as prosecutions may be initiated or convictions entered without the need to give protected information in evidence.

All of these statistics were nil in the 2023–24 reporting period as there were no international production orders issued and work was still on foot to put the Agreement into practical operation.

Table 46: Arrests, prosecutions and convictions made on the basis of obtained protected information obtained – paragraphs 128(h) of Schedule 1

Agency	Arrests		Prosecutions		Convictions	
	23/24	24/25	23/24	24/25	23/24	24/25
AFP	-	2	-	9	-	2
NSW Police	-	5	-	-	-	-
TOTAL	**-**	**7**	**-**	**9**	**-**	**2**

Paragraph 128(h) of Schedule 1 to the TIA Act also provides that this report must set out the number of occasions during the financial year that protected information obtained through an international production order was shared with other relevant agencies.

In 2024–25, there was one occasion in which protected information obtained by the AFP under an IPO was shared with a relevant agency.

Offences for which international production orders were made

Paragraphs 128(i)–(k) of Schedule 1 to the TIA Act provides that this report must set out the offences for the international production orders were issued under clauses 30, 39, or 48 of Schedule 1 to the TIA Act during the financial year.

Information relating to clauses 39 and 48 are presented in **Tables 47 and 48.** International productions orders for enforcement of the criminal law covered a range of crimes, including a total of 47 international production orders for terrorism offences, 46 international production orders for organised crime and 35 international production orders for child abuse offences.

Table 47: Offences for which international production orders were made under clause 39 of Schedule 1 relating to stored communications – paragraphs 128(j) of Schedule 1[48]

Categories of offences	AFP	NSW Police	TOTAL
Bribery or corruption	-	1	**1**
Child abuse offences	29	5	**34**
Cybercrime and telecommunications	5	-	**5**
Espionage	12	-	**12**
Fraud	2	1	**3**
Foreign incursions and recruitment	8	-	**8**
Foreign interference	17	-	**17**
General dishonesty	1	-	**1**
Illicit drug offences	29	-	**29**
Murder	12	3	**15**
Organised crime	45	-	**45**
Serious arson	8	-	**8**
Terrorism offences	47	-	**47**
Trafficking in prescribed substances	12	-	**12**
TOTAL	**227**	**10**	**237**

[48] A single international production order can relate to multiple offences.

Table 48: Offences for which international production orders were made under clause 48 of Schedule 1 relating to telecommunications data – paragraphs 128(k) of Schedule 1

Categories of offences	AFP	NSW Police	TOTAL
Child abuse offences	-	1	**1**
Cybercrime and telecommunications	2	-	**2**
Espionage	2	-	**2**
Foreign interference	2	-	**2**
Illicit drug offences	1	-	**1**
Organised crime	1	-	**1**
TOTAL	**8**	**1**	**9**

International production orders revoked by the chief officer

Paragraph 128(l) of Schedule 1 to the TIA Act provides that this report must set out the number of international production orders where a chief officer of an agency has invoked clause 114 of Schedule 1 to the TIA Act which allows the chief officer to revoke an order, either at their discretion or because the grounds on which the order was issued have ceased to exist. This information is provided at **Table 49**.

An international production order must be revoked if the grounds for which the original international production order was issued no longer exist, a breach has occurred or the international production order is no longer required. International production orders were revoked due to a change of circumstances (for example, the order no longer being required) and/or the identification of errors in the order which necessitated it being revoked (for example, typographical errors in the identifier used to target the relevant account).

Table 49: Applications revoked by the chief officer under section 114 – paragraph 128(l) of Schedule 1

Agency	Applications revoked by the chief officer	
	23/24	**24/25**
AFP	-	13
TOTAL	**-**	**13**

Chapter 6: Industry assistance

Part 15 of the Telecommunications Act provides a framework through which Australian agencies and the communications industry[49] can work together to address technological obstacles to investigations into serious crime and national security threats.

Requests and notices

Part 15 of the Telecommunications Act provides a graduated approach for agencies to receive assistance from industry:

- **Technical Assistance Request (TAR):** Agencies can request voluntary help from designated communications providers.
- **Technical Assistance Notice (TAN):** Agencies can require designated communication providers to give help where they already have the technical capability to do so.
- **Technical Capability Notice (TCN):** Agencies can require designated communications providers to give help in circumstances where they may not have the technical capability to do so.

Table 50: Eligible agencies under Part 15 of the Telecommunications Act

Agency	Industry assistance powers available to agencies		
	TAR	TAN	TCN
Interception agencies[50]	✓	✓	✓
ASD	✓	×	×
ASIO	✓	✓	✓
ASIS	✓	×	×

Definition

'Interception agency' for the purposes of Part 15 of the Telecommunications Act means the AFP, the ACIC, and the police force of a state or the Northern Territory.

The industry assistance framework provides that:

- any assistance or capability requested must be reasonable, proportionate, practicable and technically feasible, and
- assistance may only be sought by law enforcement agencies in the course of enforcing the criminal law or assisting to enforce foreign laws that are in force overseas where

[49] Categories of designated communications providers and their eligible activities are at section 317C of the Telecommunications Act.
[50] In contrast to the TIA Act, this does not include anti-corruption and integrity commissions.

those laws carry penalties of three or more years imprisonment. This threshold does not apply to intelligence agencies.

Definition

'Serious Australian offence' is an offence against a law of the Commonwealth, a state or a territory that is punishable by a maximum term of imprisonment of three years or more, or for life.

'Serious foreign offences' are offences against a law in force in a foreign country punishable by a maximum term of imprisonment of three years or more, or for life.

The framework contains numerous limitations and safeguards including:

- prohibiting assistance that creates 'systemic weaknesses' in encrypted devices and communications systems
  - this includes a prohibition on requesting or requiring providers to refrain from fixing vulnerabilities or making their systems more secure, building a decryption capability, or reducing the broader security of their systems
- prohibiting the doing of things that could otherwise require agencies to obtain a warrant or authorisation under the relevant law of the Commonwealth, state or territory to authorise that act (such as a warrant under the TIA Act), and
- assistance cannot compel providers to build a capability to remove electronic protection or extend existing data retention and interception obligations to new providers.

Definition

'Systemic weakness' means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

Use of industry assistance

Paragraphs 317ZS(1)(a)-(c) of the Telecommunications Act provide that this report must set out the number of TARs and TANs given by the interception agencies during the reporting period, and the number of TCNs given during the reporting period that were directed towards ensuring designated communications providers were capable of giving help to interception agencies.

This information is presented in **Table 51**. In 2024–25, 58 TARs were given by interception agencies to designated communications providers. This represented a decrease of two from the previous year. No TANs were issued in 2024–25, representing a decrease of two from the previous year. No TCNs were issued in 2023–24 or 2024–25.

Table 51: Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given – paragraphs 317ZS(1)(a)–(c) of the Telecommunications Act

Agency	Requests or notices given					
	TAR		TAN		TCN	
	23/24	24/25	23/24	24/25	23/24	24/25
ACIC	5	5	-	-	-	-
AFP	-	4	2	-	-	-
NSW Police	47	43	-	-	-	-
SA Police	-	1	-	-	-	-
VIC Police	3	5	-	-	-	-
WA Police	5	-	-	-	-	-
TOTAL	**60**	**58**	**2**	**-**	**-**	**-**

Offences enforced through industry assistance

Paragraph 317ZS(1)(d) of the Telecommunications Act provides that if any TARs, TANs or TCNs were given during the reporting period related to one or more kinds of serious Australian offences, this report must set out those kinds of serious Australian offences. TARs assisted with the enforcement of a range of serious offences, including 23 for homicide and related offences and 11 for illicit drug offences.

This information is provided in **Table 52**.

Table 52: Kinds of serious Australian offences enforced through Technical Assistance Requests – paragraph 317ZS(1)(d) of the Telecommunications Act

Categories of offences	ACIC	AFP	NSW Police	SA Police	VIC Police	TOTAL
Acts intended to cause injury	-	-	1	-	-	**1**
Abduction	-	-	1	-	-	**1**
Dangerous Acts	-	-	-	-	1	**1**
Fraud, deception and related offences	-	-	2	-	-	**2**
Homicide and related offences	-	-	22	-	1	**23**
Illicit drug offences	-	-	10	-	1	**11**
Justice procedures	-	2	-	-	-	**2**
Robbery, extortion and related offences	-	-	1	-	-	**1**
Sexual assault	-	-	4	1	2	**7**
Weapons	-	-	-	-	-	**-**
Terrorism offences	-	2	-	-	-	**2**

Categories of offences	ACIC	AFP	NSW Police	SA Police	VIC Police	TOTAL
Other serious Australian offences	5	-	2	-	-	**7**
TOTAL	**5**	**4**	**43**	**1**	**5**	**58**

Oversight of industry assistance powers

Use of the industry assistance powers is subject to independent oversight by either the IGIS, the Ombudsman or state and territory oversight bodies.

The IGIS or the Ombudsman (as relevant) must be notified whenever a notice or request for assistance is given, varied, extended or revoked. When an agency gives a notice, they must notify the company of its right to complain to the relevant body. Both the Ombudsman and the IGIS have the authority to inspect the use of these powers by relevant agencies at any time. These bodies may make reports on the outcome of their inspections.

The Ombudsman may also inspect agencies' records to ensure compliance with Part 15 of the Telecommunications Act. As the industry assistance measures complement powers under the TIA Act (as well as other Acts), the Ombudsman considers agency use of these powers collectively.

Where a state or territory law enforcement agency issues a notice to compel technical assistance through a TAN, it must first be reviewed by the AFP Commissioner.

TCNs may only be issued by the Attorney-General, with the approval of the Minister for Communications. This approval process ensures the assistance sought has been thoroughly scrutinised by responsible ministers and is reasonable, proportionate, practicable and technically feasible.

If requested by a company, the Attorney-General must refer any proposed TCN to an independent assessment panel consisting of a retired senior judge and a technical expert. This panel must consider whether proposed requirements are reasonable and proportionate, practicable and technically feasible, and would the proposed TCN would create a systemic vulnerability. Further, any decision to compel assistance may be challenged through judicial review.

Designated communications providers may make a complaint to the relevant oversight body for the agency that issued the request or notice.

Chapter 7: Further information

Further information about the TIA Act and Part 15 of the Telecommunications Act can be obtained by contacting the Department of Home Affairs:

Office of the Communications Access Coordinator

Department of Home Affairs

PO Box 25

Belconnen ACT 2616

CommunicationsAccessCoordinator@homeaffairs.gov.au

More information about telecommunications interception and access to telecommunications data can be found at www.homeaffairs.gov.au.

Previous copies of the Annual Report under the *Telecommunications (Interception and Access) Act 1979* and Part 15 of *Telecommunications Act 1997* can be accessed online at www.homeaffairs.gov.au.

Appendix A: Lists of tables and figures

Table	Table title	Page no.
Table 1	Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)	12-13
Table 1A	Commonwealth agencies – Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)	14-15
Table 1B	State and Territory Police – Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)	15-17
Table 1C	State and Territory Integrity Agencies – Categories of serious offences specified in interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)	17
Table 2	Federal Court judges, Federal Circuit and Family Court judges, and nominated ART member eligible to issue interception warrants – paragraph 103(ab)	19
Table 3	Interception warrant applications considered by Federal Court judges, Federal Circuit and Family Court judges, and nominated ART members	19–20
Table 4	Applications, telephone applications and renewal applications for interception warrants – paragraphs 100(1)(a)–(c)	20–22
Table 5	Interception warrants issued with specific conditions or restrictions – paragraphs 100(1)(e) and 100(2)(e)	23
Table 6	Arrests on the basis of lawfully intercepted information – paragraphs 102(1)(a) and 102(2)(a)	25
Table 7	Prosecutions per offence category in which lawfully intercepted information was given in evidence – paragraphs 102(1)(b)–(c) and 102(2)(b)–(c)	26–27
Table 8	Convictions per offence category in which lawfully intercepted information was given in evidence – paragraphs 102(1)(b)–(c) and 102(2)(b)–(c)	27–28
Table 9	Applications, telephone applications, and renewal applications for named person warrants – paragraphs 100(1)(ea) and 100(2)(ea)	29-31
Table 10	Named person warrants issued with specific conditions or restrictions – paragraphs 100(1)(ea) and 100(2)(ea)	31
Table 11	Named person warrants by reference to services intercepted under the warrant – paragraphs 100(1)(eb) and 100(2)(eb)	31-32
Table 12	Total number of services intercepted under service-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)	32-33
Table 13	Total number of services and devices intercepted under device-based named person warrants – paragraphs 100(1)(ec) and 100(2)(ec)	33
Table 14	Applications for B-Party warrants, telephone applications and renewal applications for B-Party warrants – paragraphs 100(1)(ed) and 100(2)(ed)	34
Table 15	B-Party warrants issued with conditions or restrictions – paragraphs 100(1)(ed) and 100(2)(ed)	35

Table	Table title	Page no.
Table 16	Duration of original and renewal interception warrants – paragraphs 101(1)(a)–(d) and 101(2)(a)–(d)	35-36
Table 17	Duration of original and renewal B-Party warrants – paragraphs 101(1)(da) and 101(2)(da)	36
Table 18	Final renewals – paragraphs 101(1)(e) and 101(2)(e)	37
Table 19	Percentage of eligible warrants – subsections 102(3) and 102(4)	38
Table 20	Number of occasions on which an officer or staff member of an agency intercepted a communication in reliance on subsection 7(4) or 7(5) – section 102A	39
Table 21	Interceptions carried out on behalf of other agencies – paragraph 103(ac)	40
Table 22	Total expenditure incurred by each agency in connection with the execution of interception warrants and average expenditure per interception warrant – paragraphs 103(a) and 103(aa)	41
Table 23	Recurrent interception costs per agency	41-42
Table 24	Emergency service facility declaration – paragraph 103(ad)	43
Table 25	Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 162(1)(a)–(b), 162(2)(a)–(b) and 162(2)(c)	55-56
Table 26	Stored communications warrants subject to conditions or restrictions – paragraph 162(2)(d)	56
Table 27	Arrests, proceedings and convictions made on the basis of lawfully accessed information – paragraphs 163(a)–(b)	57
Table 28	Domestic preservation notices – subsection 161A(1)	58-59
Table 29	Authorisations made by an enforcement agency for access to existing information or documents for the enforcement of the criminal law – paragraph 186(1)(a)	62-63
Table 30	Authorisations made for access to existing information or documents for the location of missing persons – paragraph 186(1)(aa)	63-64
Table 31	Authorisations made for access to existing information or documents for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(b)	64-65
Table 32	Total number of prospective data authorisations made – paragraph 186(1)(c)	65-66
Table 33	Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)	68-69
Table 33A	Commonwealth agencies – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)	70-71
Table 33B	State and Territory Police – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)	71-73
Table 33C	State and Territory Integrity Agencies – Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)	73-74

Table	Table title	Page no.
Table 34	Matters for which authorisations were made under section 179 for access to existing data for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(e)	75-76
Table 35	Offences against which authorisations were made under section 180 for access to specified information or documents that come into existence during the period for which an authorisation is in force – paragraph 186(1)(e)	76-77
Table 35A	Commonwealth agencies – Offences against which authorisations were made under section 180 for access to specified information or documents that come into existence during the period for which an authorisation is in force – paragraph 186(1)(e)	78-79
Table 35B	State and Territory Police – Offences against which authorisations were made under section 180 for access to specified information or documents that come into existence during the period for which an authorisation is in force – paragraph 186(1)(e)	79-81
Table 35C	State and Territory Integrity Agencies – Offences against which authorisations were made under section 180 for access to specified information or documents that come into existence during the period for which an authorisation is in force – paragraph 186(1)(e)	81-82
Table 36	Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)	84-85
Table 37	Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)	86-87
Table 38	Journalist information warrants issued – paragraph 186(1)(j)	87
Table 39	Number of authorisations made under journalist information warrants – paragraph 186(1)(i)	87
Table 40	Public interest advocates	88
Table 41	Industry capital cost of data retention – section 187P	88
Table 42	Applications for international production orders relating to interception, stored communications and telecommunications data for the enforcement of the criminal law – paragraphs 128(a)–(c) of Schedule 1	90
Table 43	Number of international production orders given by the Australian Designated Authority to prescribed communications providers – subparagraphs 130(1)(a)(i) and 130(1)(a)(ii) of Schedule 1	92
Table 44	Number of IPOs cancelled by the Australian Designated Authority under clause 111 – paragraph 130(1)(d) of Schedule 1	93
Table 45	Number of international production orders issued that relate to objections received by the Australian Designated Authority under clause 121 – subparagraph 130(1)(g)(i) of Schedule 1	94
Table 46	Arrests, prosecutions and convictions made on the basis of obtained protected information obtained – paragraphs 128(h) of Schedule 1	95
Table 47	Offences for which international production orders were made under clause 39 of Schedule 1 relating to stored communications – paragraphs 128(j) of Schedule 1	95-96
Table 48	Offences for which international production orders were made under clause 48 of Schedule 1 relating to telecommunications data – paragraphs 128(k) of Schedule 1	96

Table	Table title	Page no.
Table 49	Applications revoked by the chief officer under section 114 – paragraph 128(l) of Schedule 1	97
Table 50	Eligible agencies under Part 15 of the Telecommunications Act	98
Table 51	Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices given – paragraphs 317ZS(1)(a)–(c) of the Telecommunications Act	100
Table 52	Kinds of serious Australian offences enforced through Technical Assistance Requests – paragraph 317ZS(1)(d) of the Telecommunications Act	100-101

Appendix B: Interception agencies under the TIA Act

Commonwealth agency or state eligible authority
Australian Criminal Intelligence Commission (ACIC)
Australian Federal Police (AFP)
Crime and Corruption Commission (Western Australia)
Crime and Corruption Commission (Queensland)
Independent Broad-based Anti-corruption Commission (Victoria)
Independent Commission Against Corruption (New South Wales)
Independent Commission Against Corruption (South Australia)
Law Enforcement Conduct Commission (New South Wales)
National Anti-Corruption Commission (NACC)
New South Wales Crime Commission
New South Wales Police Force
Northern Territory Police Force
Queensland Police Service
South Australia Police
Tasmania Police
Victoria Police
Western Australia Police Force

Appendix C: Categories of serious offences under the TIA Act

Serious offence category	Offences covered
Abuse of Public Office	TIA Act, subsection 5D(8)
Aiding a prisoner to escape/attempt to escape from criminal detention	TIA Act, subsection 5D(8)
Appropriating property of a Commonwealth entity	TIA Act, subsection 5D(8)
Assisting person to escape or dispose of proceeds	TIA Act, subsection 5D(7)
Bribery, corruption and dishonesty offences	TIA Act, subparagraph 5D(2)(b)(vii)
Cartel offences	TIA Act, subsections 5D(5B), 5D(5C)
Child abuse offences	TIA Act, subsection 5D(3B)

Serious offence category	Offences covered
Conspire/aid/abet serious offence	TIA Act, subsection 5D(6)
Corrupting benefits given to, or received by, a Commonwealth public official	TIA Act, subsection 5D(8)
Cybercrime offences	TIA Act, subsection 5D(5)
Espionage	TIA Act, subparagraphs 5D(1)(e), (ic), (id), (ie), (ig), (vii) and (viii)
False testimony in judicial proceeding	TIA Act, subsection 5D(8)
Foreign incursions and recruitment	TIA Act, subparagraph 5D(1)(e)(vi)
Foreign interference offences	TIA Act, subparagraph 5D(1)(e)(if)
General dishonesty	TIA Act, subsection 5D(8)
Kidnapping	TIA Act, paragraph 5D(1)(b)
Loss of life	TIA Act, subparagraphs 5D(2)(b)(i)
Money laundering	TIA Act, subsection 5D(4)
Murder	TIA Act, paragraph 5D(1)(a)
Offences involving planning and organisation	TIA Act, subsection 5D(3)
Organised crime	TIA Act, subsections 5D(3AA), (8A) and (9)
People smuggling and related offences	TIA Act, subsection 5D(3A)
Serious arson	TIA Act, subparagraph 5D(2)((iiia)
Serious damage to property	TIA Act, subparagraph 5D(2)(b)(iii)
Serious drug offences and/or trafficking	TIA Act, subsection 5D(5A), subparagraph 5D(2)(b)(iv), paragraph 5D(1)(c)
Serious fraud	TIA Act, subparagraph 5D(2)(b)(v)
Serious loss of revenue	TIA Act, subparagraph 5D(2)(b)(vi)
Serious personal injury	TIA Act, subparagraphs 5D(2)(b)(ii)
Special ACC investigation	TIA Act, paragraph 5D(1)(f)
Telecommunications offence	TIA Act, subsection 5D(9)
Terrorism offences	TIA Act, paragraph 5D(1)(d), subparagraphs 5D(1)(e)(i), (ib), (ii), (iii), (iv), (v) and (vi)
Treason	TIA Act, subparagraph 5D(1)(e)(ia)

Appendix D: Updated figures for previous reporting periods

ASIC 2023–2024

ASIC identified corrections regarding access to historical telecommunications data, authorisations for historical and prospectives data, and retained data covered by select authorisations for the 2023–24 reporting period. These errors were detected by ASIC when preparing for the Commonwealth Ombudsman's inspection. The corrections resulted from a recordkeeping error resulting from the failure to follow naming conventions. ASIC advised that it has reminded its staff of the importance of naming conventions to ensure that the number of authorisations are captured and accurately reported in the future.

The below tables detail both the original figures provided for the previous annual report and the amended figures.

Authorisations made by an enforcement agency for access to existing information or documents for the enforcement of the criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	23/24 Original	23/24 Updated[51]
ASIC	300	301
TOTAL	**353,342**	**353,368**[52]

Authorisations made for access to existing information or documents for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue – paragraph 186(1)(b)

Agency	Authorisations	
	23/24 Original	23/24 Updated[53]
ASIC	2	3
TOTAL	**694**	**695**

[51] Corrections refer to Table 29, pages 60–61, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[52] This figure includes updates identified by other agencies in Appendix D of this Annual Report.
[53] Corrections refer to Table 31, page 63, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	23/24 Original	23/24 Updated[54]
Fraud	285	284
TOTAL (ASIC)[55]	**359**	**360**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)

ASIC	Subscriber data[56]	TOTAL (ASIC) [57]
23/24 Original	148	325
23/24 Updated	150	327

IBAC 2023–2024

IBAC identified corrections regarding its telecommunications interception warrants for the 2023–24 reporting period. IBAC advised that these errors were detected following an internal audit and were a result of administrative errors. Internal processes have been amended, including implementing further quality assurance processes to avoid the risk of similar errors in the future.

The below tables detail both the original figures provided for the previous annual report and the amended figures.

Percentage of eligible warrants – subsections 102(3) and 102(4)

IBAC	Number of eligible warrants	Total number of warrants in force	%
23/24 Original	8	8	100%
23/24 Updated[58]	9	11	82%

[54] Corrections refer to Table 33A, page 69–70, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[55] Categories without corrections have not been replicated in the table. The total includes figures of reported offence categories not included in this table.
[56] Corrections refer to Table 37, pages 86–87, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[57] Categories without corrections have not been replicated in the table. The total includes figures of reported offence categories not included in this table.
[58] Corrections refer to Table 19, pages 34–35, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Total expenditure incurred by each agency in connection with the execution of interception warrants and average expenditure per interception warrant – paragraphs 103(a) and 103(aa)

IBAC	Total expenditure	Average expenditure
23/24 Original	$832,553	$104,069
23/24 Updated[59]	$932,093	$116,512

NT Police 2023–2024

NT Police identified corrections regarding authorisations to access existing data for the 2023–24 reporting period. These errors were detected by the Commonwealth Ombudsman during an inspection and were the result of administrative errors.

The below tables detail both the original figures provided for the previous annual report and the amended figures.

Authorisations made by an enforcement agency for access to existing information or documents for the enforcement of the criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	23/24 Original	23/24 Updated[60]
NT Police	2,280	2,334
TOTAL	353,342	353,368[61]

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	23/24 Original	23/24 Updated[62]
Abduction	344	220
Acts – injury	44	32
Conspire/aid/abet serious offences	31	16
Cybercrime and telecommunications	39	29
Dangerous acts	73	54
Fraud	35	25

[59] Corrections refer to Table 22, pages 37–38, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[60] Corrections refer to Table 29, page 60–61, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[61] This figure includes updates identified by other agencies in Appendix D of this Annual Report.
[62] Corrections refer to Table 33B, page 77–71, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Categories of offences	23/24 Original	23/24 Updated[62]
Homicide	308	174
Illicit drug offences	1955	1347
Loss of life	11	13
Misc.	189	120
Justice procedures	8	4
Organised offences	5	3
People smuggling	19	6
Property damage	8	7
Robbery	67	44
Sexual assault	382	199
Theft	31	20
Unlawful entry	16	19
TOTAL (NT Police)[63]	**3,567**	**2,334**

Offences against which authorisations were made under section 180 for access to specified information or documents that come into existence during the period for which an authorisation is in force – paragraph186(1)(e)

Categories of offences	23/24 Original	23/24 Updated[64]
Abduction	4	5
Dangerous acts	-	1
Homicide	9	10
Illicit drug offences	449	451
TOTAL (NT Police)[65]	**563**	**568**

[63] Categories without corrections have not been replicated in the table. The total includes figures of reported offence categories not included in this table.
[64] Corrections refer to Table 35B, pages 80–81, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[65] Categories without corrections have not been replicated in the table. The total includes figures of reported offence categories not included in this table.

Periods for which retained data was held by carrier before authorised disclosure – paragraph 186(1)(f)

NT Police	Age of disclosure									TOTAL (NT Police)
	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18–21 months	21–24 months	Over 24 months	
23/24 Original	2106	78	20	30	13	7	5	8	21	**2,288**
23/24 Updated[66]	1874	119	26	43	24	9	8	14	242	**2,359**

Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)

NT Police	Subscriber data	Traffic data	TOTAL(NT Police)
23/24 Original	1,715	573	**2,288**
23/24 Updated[67]	1,730	632	**2,362**

[66] Corrections refer to Table 36, pages 84–85, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[67] Corrections refer to Table 37, pages 86–87, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

TAS Police 2023–2024

TAS Police identified corrections regarding access to telecommunications data for the 2023–24 reporting period. These errors were detected following an inspection by the Commonwealth Ombudsman which found that Tasmania Police had reported authorisations incorrectly. Internal processes are being updated to avoid the risk of similar errors in the future.

The below tables detail both the original figures provided for the previous annual report and the amended figures as identified and corrected.

Authorisations made by an enforcement agency for access to existing information or documents for the enforcement of the criminal law – paragraph 186(1)(a)

Agency	Authorisations	
	23/24 Original	23/24 Updated[68]
TAS Police	3,118	3,089
TOTAL	**353,342**	**353,368**[69]

Offences for which authorisations were made under section 178 to access existing data to enforce the criminal law – paragraph 186(1)(e)

Categories of offences	Authorisations	
	23/24 Original	23/24 Updated[70]
Misc.	38	9
TOTAL (TAS Police)[71]	**3,118**	**3,089**

[68] Corrections refer to Table 29, pages 60–61, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[69] This figure includes updates identified by other agencies in Appendix D of this Annual Report.
[70] Corrections refer to Table 33B, pages 71–72, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[71] Categories without corrections have not been replicated in the table. The total includes figures of reported offence categories not included in this table.

WA Police 2023–2024

WA Police identified corrections regarding expenditure on telecommunications interception for the 2023–24 reporting period. Following the preparation of the 2024–25 Annual Report, WA Police identified errors in relation to the expenditure costs of telecommunications interception warrants for the previous reporting period. WA Police advised that internal processes are being updated to avoid the risk of similar errors in the future.

The below tables detail both the original figures provided for the previous annual report and the amended figures as identified and corrected.

Total expenditure incurred by each agency in connection with the execution of interception warrants and average expenditure per interception warrant – paragraphs 103(a) and 103(aa)

WA Police	Total expenditure	Average expenditure
23/24 Original	$1,651,657	$6,028
23/24 Updated[72]	$3,324,800	$12,134

Recurrent interception costs per agency

WA Police[73]	Salaries	Capital expenditure	Interception costs	Total ($)
23/24 Original	-	-	$1,651,657	**$1,651,657**
23/24 Updated[74]	$2,570,000	$750,000	$54,800	**$3,324,800**

[72] Corrections refer to Table 22, pages 37–38, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.
[73] Categories without corrections have not been replicated in the table.
[74] Corrections refer to Table 23, pages 38–39, 2023–24 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Notes