Australian Government
Attorney-General's Department

2023–24 Annual Report under the *Telecommunications (Interception and Access) Act 1979* and Part 15 of the *Telecommunications Act 1997*

Contents

Abbreviations

Abbreviation	Term
AAT	Administrative Appeals Tribunal
ACLEI	Australian Commission for Law Enforcement Integrity
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACT Integrity Commission	Australian Capital Territory Integrity Commission
AFP	Australian Federal Police
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
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police Force

Abbreviation	Term
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 Statistics

- There were 3,007 interception warrants that were issued to 15 interception agencies. This is a decrease of 203 from the 3,210 issued in 2022–23.
- There were 16 applications for interception warrants that were refused. This decreased by 12 compared to 2022–23.
- The majority of serious offences that were specified in interception warrants issued were serious drug offences and/or trafficking (1,208), followed by loss of life and/or personal injury (559) and murder (354).
- Information obtained under interception warrants was used in 1,592 arrests, 2,048 prosecutions and 1,060 convictions.
- There were 738 stored communications warrants that were issued to 9 criminal law-enforcement agencies. This is a decrease of 57 on the 795 issued in 2022–23.
- There was one application for a stored communications warrant that was refused. This is a decrease of one from 2022–23.
- Information obtained under stored communications warrants was used in 283 arrests, 210 proceedings, and 158 convictions. This is a decrease of 183 from the 466 arrests made in 2022-23, an increase of 54 on the 156 proceedings conducted in 2022-23 and a decrease of 6 on the 164 convictions obtained in 2022-23.
- There were 359,921 authorisations made by 21 enforcement agencies for the disclosure of existing telecommunications data. This is an increase of 28,182 authorisations on the 331,739 authorisations made in 2022–23.[1] Of these, 353,342 were made to enforce the criminal law.
- Authorisations for existing telecommunications data covered a range of crimes, including 63,925 authorisations for illicit drug offences, 39,934 for abduction and 36,907 authorisations for unlawful entry.
- There were 52,863 authorisations made by 19 criminal law-enforcement agencies for disclosure of prospective telecommunications data. This is an increase of 8,384 on the 44,479 authorisations made in 2022–23.
- No journalist information warrants were issued to enforcement agencies in 2023–24. This is consistent with 2022-23.
- There were 60 technical assistance requests given to designated communications providers by 4 interception agencies. This is a decrease of 6 from the 66 given in 2022–23.

[1] This includes adjustments made to the 2022–23 Annual Report (see Appendix D).

- There were 2 technical assistance notices given in this reporting period. This is an increase of 2 from 2022-23. No technical capability notices were given to designated communications providers in 2023-24, consistent with 2022-23.

Chapter 1: Introduction

The 2023–24 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 2023 and 30 June 2024.

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, helping to eliminate potential suspects and to consider whether more intrusive investigative tools including search warrants and interception warrants 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, and only criminal law-enforcement agencies can access prospective telecommunications data to assist in the investigation of offences punishable by at least three years imprisonment.[2] 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.

Criminal law-enforcement agencies may authorise access to telecommunications data. The Attorney-General may also declare additional agencies in limited circumstances for a period of 40 sitting days of Parliament. In the 2023-24 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. The function of section 7 of the TIA Act is to prohibit communications from being intercepted while they are passing over an Australian telecommunications system, except as authorised under the 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. An interception agency is limited to bodies such as the AFP, ACIC, state and territory police forces and 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 **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 7 years' imprisonment. There are exceptions to this threshold.

Interception warrants may be available for offences with a maximum penalty of less than 7 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 communications 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 2023–24 the majority of warrants obtained were to assist with investigations into serious drug offences and/or trafficking (1,208 warrants). Murder was specified in 354 warrants and 559 related to loss of life or personal injury. 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 – paragraphs 100(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
Administration of justice / government offences	22	2	-	**24**
Assisting person to escape or dispose of proceeds	-	32	-	**32**
Bribery, corruption and dishonesty offences	3	11	50	**64**
Child abuse offences	2	66	-	**68**
Conspire/aid/abet serious offence	-	39	-	**39**
Cybercrime offences	1	-	-	**1**
Espionage, foreign interference, secrecy of information and related offences[3]	60	-	-	**60**
Kidnapping	2	109	-	**111**
Loss of life and/or personal injury	35	524	-	**559**
Money laundering	77	44	18	**139**

[3] This category is inclusive of figures reported against offences pursuant to divisions 82, 83, 91, 92, 92A, 119, 122, or s 137.1A of the *Criminal Code Act 1995.*

Categories of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Murder	36	318	-	**354**
Offences involving planning and organisation	21	205	-	**226**
Organised offences and/or offences relating to criminal organisations	37	82	2	**121**
People smuggling and related	7	-	-	**7**
Serious damage to property and/or serious arson	11	88	-	**99**
Serious drug offences and/or trafficking	300	892	16	**1,208**
Serious fraud	12	32	2	**46**
Serious loss of revenue	21	1	5	**27**
Telecommunications offences	-	3	-	**3**
Terrorism offences	74	2	-	**76**
TOTAL	**721**	**2,450**	**93**	**3,264**

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[4]	AFP	NACC	TOTAL
Administration of justice / government offences	-	11	11	**22**
Bribery, corruption and dishonesty offences	-	1	2	**3**
Child abuse offences	-	2	-	**2**
Cybercrime offences	-	1	-	**1**
Espionage, foreign interference, secrecy of information and related offences[5]	-	56	4	**60**
Kidnapping	-	2	-	**2**
Loss of life and/or personal injury	-	35	-	**35**
Money laundering	10	67	-	**77**
Murder	-	36	-	**36**

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

[5] This category is inclusive of figures reported against offences pursuant to divisions 82, 83, 91, 92, 92A, 119, 122, or s 137.1A the *Criminal Code Act 1995.*

Categories of offences	ACIC[4]	AFP	NACC	TOTAL
Offences involving planning and organisation	-	21	-	**21**
Organised offences and/or offences relating to criminal organisations	-	37	-	**37**
People smuggling and related	-	7	-	**7**
Serious damage to property and/or serious arson	-	11	-	**11**
Serious drug offences and/or trafficking	15	285	-	**300**
Serious fraud	1	11	-	**12**
Serious loss of revenue	-	21	-	**21**
Terrorism offences	-	74	-	**74**
TOTAL	**26**	**678**	**17**	**721**

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
Administration of justice / government offences	2	-	-	-	-	-	-	**2**
Assisting person to escape or dispose of proceeds	30	-	-	-	-	2	-	**32**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Bribery, corruption and dishonesty offences	7	-	-	2	-	2	-	**11**
Child abuse offences	56	-	-	-	-	10	-	**66**
Conspire/aid/abet serious offence	39	-	-	-	-	-	-	**39**
Kidnapping	108	-	-	-	-	-	1	**109**
Loss of life and/or serious personal injury	403	1	39	-	-	18	63	**524**
Money laundering	20	-	9	-	-	7	8	**44**
Murder	259	2	9	1	3	29	15	**318**
Offences involving planning and organisation	158	-	-	-	-	-	47	**205**
Organised offences and/or offences relating to criminal organisations	82	-	-	-	-	-	-	**82**
Serious damage to property and/or serious arson	59	-	6	2	-	5	16	**88**
Serious drug offences and/or trafficking	525	24	161	15	4	51	112	**892**
Serious fraud	29	-	1	-	-	1	1	**32**
Serious loss of revenue	-	-	-	-	-	1	-	**1**
Telecommunications offences	3	-	-	-	-	-	-	**3**
Terrorism offences	2	-	-	-	-	-	-	**2**
TOTAL	**1,782**	**27**	**225**	**20**	**7**	**126**	**263**	**2,450**

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	LECC	NSW CC	QLD CCC	TOTAL
Bribery, corruption and dishonesty offences	-	19	19	-	12	**50**
Money laundering	-	-	-	5	13	**18**
Organised offences and/or offences relating to criminal organisations	-	-	-	2	-	**2**
Serious drug offences and/or trafficking	-	-	-	8	8	**16**
Serious fraud	-	-	-	-	2	**2**
Serious loss of revenue	5	-	-	-	-	**5**
TOTAL	**5**	**19**	**19**	**15**	**35**	**93**

Eligibility to issue an interception warrant

An interception warrant under Part 2-5 of the TIA Act may only be issued by an eligible judge, or a nominated Administrative Appeals Tribunal (AAT) member.

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 included 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 AAT[6] 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
- member (of any level).

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 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 AAT members have been used for that purpose.

This information is presented in **Table 2**. As at 30 June 2024, there were 94 issuing authorities for interception warrants.

[6] The Administrative Review Tribunal (ART) commenced operations on 14 October 2024, replacing the AAT, with all matters now transferred to the ART. Members who hold one of the following appointments to the ART may be nominated to issue warrants under Part 2-5 of the TIA Act: Deputy president, senior member and general member.

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

Issuing authority	Number eligible
Federal Court judges	21
Federal Circuit and Family Court judges	40
Nominated AAT members	33
TOTAL	**94**

Issuing of interception warrants

Table 3 states which issuing authorities considered applications for warrants made by each interception agency during 2023–24. In 2023–24, nominated AAT members considered 79 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 AAT members[7]

Agency	Issuing authority			
	Federal Court judges	Federal Circuit and Family Court judges	Nominated AAT members	TOTAL
ACIC	1	1	9	**11**
AFP	1	102	363	**466**
CCC (WA)	-	4	-	**4**
IBAC	-	-	8	**8**
LECC	-	-	19	**19**
NACC	9	4	-	**13**
NSW CC	-	-	10	**10**
NSW Police	-	53	1,733	**1,786**
NT Police	-	27	-	**27**
QLD CCC	15	-	5	**20**

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

Agency	Issuing authority			
	Federal Court judges	Federal Circuit and Family Court judges	Nominated AAT members	TOTAL
QLD Police	-	162	69	**231**
SA Police	-	-	20	**20**
TAS Police	-	-	7	**7**
VIC Police	-	-	127	**127**
WA Police	-	260	14	**274**
TOTAL	**26**	**613**	**2,384**	**3,023**

Applications for interception warrants

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

This information is presented in **Table 4**. In 2023–24, agencies were issued 3,007 interception warrants, being a decrease of 203 from 2022–23, where 3,210 interception warrants were issued. In 2023–24, 530 renewals of interception warrants were issued. This was a decrease of 85 renewals of interception warrants from the 615 issued in the previous reporting period. There was a decrease in the number of telephone applications from 22 to 11 compared to the 2022–23 reporting period.

Table 4: Applications, telephone applications and renewal applications for interception warrants[8] – paragraphs 100(1)(a)-(c)

Agency	Status of Application	Applications for warrants		Telephone applications for warrants		Renewal applications	
		22/23	23/24	22/23	23/24	22/23	23/24
ACIC	Made	27	11	-	-	-	3
	Refused	-	1	-	-	-	-
	Issued	27	10	-	-	-	3

[8] 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	
		22/23	23/24	22/23	23/24	22/23	23/24
AFP	Made	518	466	-	-	167	137
	Refused	1	3	-	-	-	-
	Issued	517	463	-	-	167	137
CCC (WA)	Made	12	4	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	12	4	-	-	-	1
IBAC	Made	13	8	-	-	3	-
	Refused	2	-	-	-	-	-
	Issued	11	8	-	-	3	-
LECC	Made	16	19	-	-	12	12
	Refused	-	-	-	-	-	-
	Issued	16	19	-	-	12	12
NACC[9]	Made	8	13	-	2	1	2
	Refused	-	-	-	-	-	-
	Issued	8	13	-	2	1	2
NSW CCC	Made	18	10	-	-	-	3
	Refused	-	-	-	-	-	-
	Issued	18	10	-	-	-	3
NSW Police	Made	1,876	1,786	22	9	363	306
	Refused	17	4	-	-	2	-
	Issued	1,859	1,782	22	9	361	306
NT Police	Made	24	27	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	24	27	-	-	1	-
QLD CCC	Made	12	20	-	-	-	9
	Refused	-	1	-	-	-	-

[9] 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.

Agency	Status of Application	Applications for warrants		Telephone applications for warrants		Renewal applications	
		22/23	23/24	22/23	23/24	22/23	23/24
	Issued	12	19	-	-	-	9
QLD Police	Made	247	231	-	-	43	36
	Refused	1	6	-	-	1	1
	Issued	246	225	-	-	42	35
SA Police	Made	22	20	-	-	2	3
	Refused	-	-	-	-	-	-
	Issued	22	20	-	-	2	3
TAS Police	Made	5	7	-	-	-	-
	Refused	1	-	-	-	-	-
	Issued	4	7	-	-	-	-
VIC Police	Made	145	127	-	-	9	19
	Refused	3	1	-	-	-	-
	Issued	142	126	-	-	9	19
WA Police	Made	295	274	-	-	17	-
	Refused	3	-	-	-	-	-
	Issued	292	274	-	-	17	-
TOTAL	**Made**	**3,238**	**3,023**	**22**	**11**	**618**	**531**
	Refused	**28**	**16**	**-**	**-**	**3**	**1**
	Issued	**3,210**	**3,007**	**22**	**11**	**615**	**530**

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 2023–24, no warrants authorising entry on premises were issued. This is consistent with 2022–23.

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 2023–24, 8 interception warrants were issued with a condition or restriction. This is a decrease of 50 compared to the 58 issued in 2022–23.

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	
	22/23	23/24
AFP	2	-
LECC	1	-
NACC[10]	-	1
NSW Police	55	7
TOTAL	**58**	**8**

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

[10] From 1 July 2023 the Australian Commission for Law Enforcement Integrity (ACLEI) was subsumed into the National Anti-Corruption Commission (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 report.

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 themselves but where 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 2023–24, there were 1,592 arrests made as a result of lawfully intercepted information (comprising 1,330 arrests by the agency to whom the warrant was issued and 253 arrests by another agency). There were also 2,048 prosecutions and 1,060 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	22/23		23/24	
	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	63	50	91	91
NACC[11]	-	2	1	1
NSW CC	-	38	-	78
NSW Police	1,802	16	749	27
NT Police	20	-	43	13
QLD CCC	-	1	3	-
QLD Police	201	-	255	-
SA Police	19	2	19	1
TAS Police	1	1	4	4
VIC Police	164	38	174	38
WA Police	231	154	-	-
TOTAL	**2,501**	**302**	**1,339**	**253**

[11] 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.

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	AFP	ICAC (NSW)	LECC	NACC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Administration of justice / government offence	4	-	-	1	-	7	-	-	-	-	-	**12**
Ancillary offences	1	-	-	1	-	-	-	-	-	-	-	**2**
Assisting to escape or dispose of proceeds	2	-	-	-	-	4	-	-	-	1	-	**7**
Bribery or corruption	-	-	-	1	-	-	10	-	-	2	-	**13**
Cartel offences	-	-	-	-	-	2	-	-	-	-	-	**2**
Child abuse offences	1	-	-	-	-	46	-	-	-	-	-	**47**
Conspire/aid/abet serious offence	12	-	-	-	-	5	-	-	-	1	-	**18**
Espionage, foreign interference, secrecy of information and related offences[12]	1	-	-	-	-	-	-	-	-	-	-	**1**
Kidnapping	-	-	-	-	-	25	-	-	-	-	-	**25**
Loss of life	-	-	-	-	-	-	-	-	-	7	-	**7**
Money laundering	24	-	-	-	1	46	-	-	-	8	-	**79**

[12] This category is inclusive of figures reported against offences pursuant to divisions 82, 83, 91, 92, 92A, 119, 122, or s 137.1A the *Criminal Code Act 1995.*

Category	AFP	ICAC (NSW)	LECC	NACC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Murder	-	-	-	-	1	95	-	-	8	4	-	**108**
Offences involving planning and organisation	2	-	-	-	-	112	-	-	-	18	-	**132**
Organised crime	36	-	-	-	-	87	-	-	-	-	-	**123**
Other offences punishable by 3 years to life	20	-	-	-	-	311	-	-	-	57	-	**388**
Serious arson	2	-	-	-	-	47	-	-	-	3	-	**52**
Serious damage to property	-	-	-	-	-	1	-	-	-	-	-	**1**
Serious drug offences and/or trafficking	92	-	-	-	2	715	5	-	1	48	-	**863**
Serious fraud	3	-	-	-	-	25	5	-	-	3	-	**36**
Serious loss of revenue	-	-	-	-	-	-	-	-	-	-	-	**-**
Serious personal injury	-	-	-	-	-	104	-	-	2	23	-	**129**
Telecommunication offence	3	-	-	-	-	-	-	-	-	-	-	**3**
TOTAL	203	-	-	3	4	1,632	20	-	11	175	-	**2,048**

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	AFP	ICAC (NSW)	LECC	NACC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Administration of justice / government offence	-	-	-	1	-	5	-	-	-	-	-	**6**
Ancillary offences	-	-	-	1	-	-	-	-	-	-	-	**1**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	4	-	-	-	1	-	**5**
Bribery or corruption	-	-	-	1	-	-	10	-	-	1	-	**12**
Child abuse offences	-	-	-	-	-	17	-	-	-	-	-	**17**
Conspire/aid/abet serious offence	1	-	-	-	-	2	-	-	-	1	-	**4**
Espionage, foreign interference, secrecy of information and related offences[13]	1	-	-	-	-	-	-	-	-	-	-	**1**
Kidnapping	-	-	-	-	-	16	-	-	-	-	-	**16**
Loss of life	-	-	-	-	-	-	-	-	-	4	-	**4**
Money laundering	5	-	-	-	1	29	-	-	-	8	-	**43**

[13] This category is inclusive of figures reported against offences pursuant to divisions 82, 83, 91, 92, 92A, 119, 122, or s 137.1A the *Criminal Code Act 1995.*

Category	AFP	ICAC (NSW)	LECC	NACC	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	VIC Police	WA Police	TOTAL
Murder	-	-	-	-	-	58	-	-	7	-	-	**65**
Offences involving planning and organisation	-	-	-	-	-	66	-	-	-	18	-	**84**
Organised crime	7	-	-	-	-	38	-	-	-	-	-	**45**
Other offences punishable by 3 years to life	4	-	-	-	-	157	-	-	-	56	-	**217**
Serious arson	-	-	-	-	-	23	-	-	-	1	-	**24**
Serious damage to property	-	-	-	-	-	1	-	-	-	-	-	**1**
Serious drug offences and/or trafficking	9	-	-	-	2	330	5	-	-	46	-	**392**
Serious fraud	1	-	-	-	-	16	5	-	-	3	-	**25**
Serious personal injury	-	-	-	-	-	74	-	-	1	20	-	**95**
Telecommunications offences	3	-	-	-	-	-	-	-	-	-	-	**3**
TOTAL	**31**	**-**	**-**	**3**	**3**	**836**	**20**	**-**	**8**	**159**	**-**	**1,060**

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 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 2023–24, 533 named person warrants were issued. This is an increase of 45 from 2022–23, in which 488 named person warrants were issued. In 2023-24, 141 renewal applications were issued. This is a decrease of 3 on the 144 issued in 2022–23.

Table 9: Applications, telephone applications, and renewal applications for named person warrants – paragraphs 100(1)(ea) and 100(2)(ea)[14]

Agency	Relevant statistics	Applications		Telephone applications		Renewal applications	
		22/23	23/24	22/23	23/24	22/23	23/24
ACIC	Made	9	5	-	-	-	3
	Refused	-	-	-	-	-	-
	Issued	9	5	-	-	-	3
AFP	Made	237	224	-	-	79	74
	Refused	-	-	-	-	-	-
	Issued	237	224	-	-	79	74
CCC (WA)	Made	4	4	-	-	-	1
	Refused	-	-	-	-	-	-
	Issued	4	4	-	-	-	1
LECC	Made	16	19	-	-	12	12
	Refused	-	-	-	-	-	-
	Issued	16	19	-	-	12	12
NACC[15]	Made	2	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	2	2	-	-	-	-
NSW CC	Made	4	-	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	4	-	-	-	1	-
NSW Police	Made	127	161	-	-	50	44
	Refused	-	-	-	-	-	-
	Issued	127	161	-	-	50	44
	Made	2	5	-	-	-	-

[14] 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.

[15] 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.

Agency	Relevant statistics	Applications		Telephone applications		Renewal applications	
		22/23	23/24	22/23	23/24	22/23	23/24
NT Police	Refused	-	-	-	-	-	-
	Issued	2	5	-	-	-	-
QLD CCC	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
QLD Police	Made	13	16	-	-	2	2
	Refused	1	1	-	-	1	1
	Issued	12	15	-	-	1	1
SA Police	Made	3	1	-	-	1	-
	Refused	-	-	-	-	-	-
	Issued	3	1	-	-	1	-
VIC Police	Made	32	33	-	-	-	6
	Refused	-	-	-	-	-	-
	Issued	32	33	-	-	-	6
WA Police	Made	40	63	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	40	63	-	-	-	-
TOTAL	**Made**	**489**	**534**	**-**	**-**	**145**	**142**
	Refused	**1**	**1**	**-**	**-**	**1**	**1**
	Issued	**488**	**533**	**-**	**-**	**144**	**141**

In 2023–24, no named person warrants were issued with a condition or restriction. This is a decrease of 5 from the 5 issued in 2022-23.

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	
	22/23	23/24
AFP	1	-
LECC	1	-
NSW Police	3	-
TOTAL	**5**	**-**

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	
	22/23	23/24	22/23	23/24	22/23	23/24	22/23	23/24
ACIC	6	3	3	5	-	-	-	-
AFP	70	56	153	129	9	9	3	-
CCC (WA)	2	-	2	-	-	-	-	-
LECC	3	9	13	10	-	-	-	-
NACC[16]	-	2	2	-	-	-	-	-
NSW CC	1	-	3	-	-	-	-	-
NSW Police	49	68	53	75	2	4	-	-
NT Police	-	1	2	4	-	-	-	-
QLD CCC	-	-	-	1	-	-	-	-
QLD Police	1	5	10	9	1	-	-	-

[16] 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.

Agency	Named person warrants by number of services intercepted							
	1 service only		2-5 services		6-10 services		10+ services	
	22/23	23/24	22/23	23/24	22/23	23/24	22/23	23/24
SA Police	-	-	3	1	-	-	-	-
TAS Police	-	-	-	1	-	-	-	-
VIC Police	7	9	10	20	-	1	-	2
WA Police	20	7	20	56	-	-	-	-
TOTAL	**159**	**160**	**274**	**311**	**12**	**14**	**3**	**2**

Under the TIA Act, agencies can apply for a named person warrant in relation to telecommunications 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 at 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 at 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	
	22/23	23/24
ACIC	17	18
AFP	524	465
CCC (WA)	8	-
LECC	39	37
NACC[17]	4	2
NSW CC	12	-
NSW Police	237	256
NT Police	8	-
QLD CCC	-	1
QLD Police	37	33
SA Police	12	2
TAS Police	-	2
VIC Police	36	93
WA Police	69	-
TOTAL	**1,003**	**909**

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	
	22/23	23/24	22/23	23/24
AFP	59	77	-	73
NSW Police	17	47	22	81
VIC Police	15	1	-	-
TOTAL	**91**	**125**	**22**	**154**

[17] 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.

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 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 2023–24, 98 B-Party warrants were issued to interception agencies. This represents a decrease of 20 from the 118 B-Party warrants issued in 2022–23. There was an increase of 6 renewal applications, with 21 issued in 2023-24 and 15 in 2022-23. In 2023–24, 2 B-Party warrants were issued with conditions or restrictions. This is an increase of one from the B-Party warrants issued in 2022–23.

Table 14: Applications for B-Party warrants, telephone applications and renewal applications for B-Party warrants – paragraphs 100(1)(ed) and 100(2)(ed)[18]

Agency	Relevant statistics	Applications for B-Party warrants		Telephone applications for B-Party warrants		Renewal applications for B-Party warrants	
		22/23	23/24	22/23	23/24	22/23	23/24
AFP	Made	26	20	-	-	10	11
	Refused	-	-	-	-	-	-
	Issued	26	20	-	-	10	11
NACC	Made	-	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
NSW Police	Made	92	77	7	4	5	10
	Refused	-	-	-	-	-	-
	Issued	92	77	7	4	5	10
TOTAL	**Made**	**118**	**98**	**7**	**4**	**15**	**21**
	Refused	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**118**	**98**	**7**	**4**	**15**	**21**

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	
	22/23	23/24
NSW Police	1	1
NACC[19]	-	1
TOTAL	**1**	**2**

[18] 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.

[19] 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.

In 2023–24, 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.

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)[20]	Average period specified in warrants (days)	Average period warrants in force (days)[21]
ACIC	90	66	75	66
AFP	85	62	84	68
CCC (WA)	90	90	90	36
IBAC	90	82	-	-
LECC	90	89	81	67
NACC	75	45	76	76
NSW CC	89	200	75	66
NSW Police	77	57	79	65
NT Police	89	52	-	-

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

Agency	Duration of original telecommunications warrants		Duration of renewal telecommunications interception warrants	
	Average period specified in warrants (days)	Average period warrants in force (days)[20]	Average period specified in warrants (days)	Average period warrants in force (days)[21]
QLD CCC	89	55	89	72
QLD Police	79	56	78	63
SA Police	78	54	69	28
TAS Police	90	68	-	-
VIC Police	86	65	78	46
WA Police	88	110	-	-
AVERAGE	**86**	**77**	**58**	**44**

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**.

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)[22]	Average period specified in warrants (days)	Average period warrants in force (days)[23]
AFP	45	34	45	45
NSW Police	35	25	43	41
AVERAGE	**40**	**30**	**44**	**43**

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

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	
	22/23	23/24	22/23	23/24	22/23	23/24
ACIC	-	-	1	-	-	1
AFP	24	14	39	35	47	35
IBAC	3	-	-	-	-	-
LECC	-	-	-	3	3	3
NACC[24]	1	-	-	2	-	-
NSW CC	-	1	-	-	3	-
NSW Police	85	88	57	79	52	51
NT Police	-	-	1	-	-	-
QLD CCC	-	-	-	3	-	3
QLD Police	19	13	15	16	3	6
SA Police	2	1	-	-	-	-
VIC Police	2	7	4	5	2	3
WA Police	7	-	10	-	-	-
TOTAL	**143**	**124**	**127**	**143**	**110**	**102**

[24] 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.

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 2023–24, 76% of total warrants were eligible warrants.

Table 19: Percentage of eligible warrants – subsections 102(3) and 102(4)[25]

Agency	Number of eligible warrants	Total number of warrants in force	%
ACIC	8	14	57
AFP	469	690	68
IBAC	8	8	100
LECC	13	20	65
NACC	1	15	7
NSW CC	8	15	53
NSW Police	1,511	1,930	78
NT Police	16	29	55
QLD CCC	12	19	63

[25] 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	%
QLD Police	227	275	83
SA Police	15	23	65
TAS Police	1	7	14
VIC Police	52	137	38
WA Police	274	274	100
TOTAL	**2,615**	**3,456**	**76**

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	22/23	23/24
AFP	1	2
TOTAL	**1**	**2**

In 2023–24, 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 one instance this occurred with the consent of the person to whom the communication was directed.[26]

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.[27] 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*
- 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 2023–24, there was one occasion 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 a decrease of one from 2022–23.

In 2023-24, 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 s 25A of the *International War Crimes Tribunal Act 1995*. This is consistent with 2022-23.

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

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

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, 24 interceptions were carried out on behalf of other agencies in the reporting period. This is an increase of 8 from the 16 interceptions carried out in 2022–23.

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	Queensland CCC	17
VIC Police	Tasmania Police	7
TOTAL		24

Telecommunications interception expenditure

Table 22 provides information about the total expenditure (including expenditure of a capital nature) incurred by interception agencies in connection with interception warrants and the average expenditure per warrant. The average cost per warrant is affected by capital expenditure, which can vary significantly, for instance, due to a capital upgrade program, and the number of warrants issued, meaning that smaller interception agencies typically have higher average costs as they apply for fewer warrants.

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.

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	$4,796,090	$479,609
AFP	$22,648,805	$48,918
CCC (WA)	$806,832	$201,708

Agency	Total expenditure	Average expenditure
IBAC	$832,553	$104,069
ICAC (NSW)	$352,933	$70,587
ICAC (SA)	$98,767	-
LECC	$1,657,249	$87,224
NACC	$184,866	$14,220
NSW CC	$2,340,510	$234,051
NSW Police	$9,907,744	$5,560
NT Police	$2,216,960	$82,110
QLD CCC	$1,653,915	$87,048
QLD Police	$8,673,227	$38,548
SA Police	$4,401,795	$220,090
TAS Police	$1,207,589	$172,513
VIC Police	$414,231	$3,288
WA Police	$1,651,657	$6,028
TOTAL / AVERAGE	**$63,845,723**	**$109,151**

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.

Table 23: Recurrent interception costs per agency

Agency	Salaries	Administrative support	Capital expenditure	Interception costs	Total ($)
ACIC	$3,021,257	$252,089	$142,109	$1,380,635	**$4,796,090**
AFP	$11,384,657	$531,614	$5,193,230	$5,539,304	**$22,648,805**
CCC (WA)	$294,616	$555	$472,600	$39,061	**$806,832**
IBAC	$630,633	$26,922	$56,460	$218,078	**$932,093**
ICAC (NSW)	$167,000	-	-	$185,933	**$352,933**
ICAC (SA)	-	$98,767	-	-	**$98,767**
LECC	$594,229	$2,837	$1,011,936	$48,247	**$1,657,249**

Agency	Salaries	Administrative support	Capital expenditure	Interception costs	Total ($)
NACC	$55,938	-	$120,792	$8,136	**$184,866**
NSW CC	$1,836,906	$44,591	$2,943	$456,070	**$2,340,510**
NSW Police	$6,979,561	$199,421	-	$2,728,762	**$9,907,744**
NT Police	$489,000	-	$1,602,433	$125,527	**$2,216,960**
QLD CCC	$1,067,386	$391,770	-	$194,759	**$1,653,915**
QLD Police	$6,168,047	$588,273	-	$1,916,907	**$8,673,227**
SA Police	$2,263,146	$364,080	$645,254	$1,129,315	**$4,401,795**
TAS Police	$997,306	$52,570	-	$157,713	**$1,207,589**
VIC Police	$283,304	$23,387	$26,837	$80,703	**$414,231**
WA Police	-	-	-	$1,651,657	**$1,651,657**
TOTAL	**$36,232,986**	**$2,576,876**	**$9,274,594**	**$15,860,807**	**$63,945,263**

Emergency service facilities

Under the TIA Act, listening to or recording calls to and from a facility declared by the Attorney-General to be an emergency service facility does not constitute interception. This exemption ensures that emergency service provides 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 2023–24 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 2023-24.

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

State	Police	Fire brigade	Ambulance	Dispatching
Australian Capital Territory	1	-	-	-

State	Police	Fire brigade	Ambulance	Dispatching
New South Wales	-	-	1	-
Northern Territory	3	3	1	-
South Australia	1	2	3	1
Western Australia	1	-	-	-
TOTAL	**6**	**5**	**5**	**1**

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 the Attorney-General's Department (AGD) with a copy of each interception warrant
- interception agencies to report to the Attorney-General, within 3 months of a warrant ceasing to be in force, detailing the use of information obtained by interception under the warrant
- the Secretary of AGD to maintain a General Register detailing the particulars of all interception warrants. The Secretary of AGD must provide the General Register to the Attorney-General for inspection every 3 months, and
- the Secretary of AGD to maintain a Special Register recording the details of interception warrants that do not lead to a prosecution within 3 months of the warrant expiring. The Special Register is also given to the Attorney-General 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 2023.

The Ombudsman is required under the TIA Act to report to the Attorney-General 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 Commonwealth Attorney-General. 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 2023–24

Overview

During the 2023–24 financial year (the inspection period), the Ombudsman conducted 6 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.

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

The Ombudsman identified three key areas that require attention:

- internal safeguards should be improved to ensure the ACIC use telecommunication intercepts lawfully

- inadequate review and destruction of records by the ACIC, AFP and the NACC
- lack of records for an emergency telecommunications interception by the AFP.

The Ombudsman did not identify any non-compliance by agencies with their obligation to keep documents connected with the issue of warrants (section 80 of the TIA Act). The AFP complied with requirements to destroy material obtained in relation to an interception Part 5.3 warrant under section 79AA, but there were instances of non-compliance with the record keeping provision of section 81 in relation to records in connection with interceptions. All agencies had instances with non-compliance with the requirement to destroy restricted records that are not likely to be required for a permitted purpose under section 79 of the TIA Act. The Ombudsman also observed other contraventions and risks of non-compliance with the TIA Act across all agencies. The seriousness of the non-compliance varied between the agencies.

Overview of inspections

The Ombudsman conducted biannual inspections of the ACIC, AFP and the NACC. The second inspection of the ACIC was combined with a review of the ACIC's use of other covert powers the Ombudsman oversees. That inspection reviewed the ACIC's use of telecommunication interceptions across 2 Intelligence Operations.

Room to Improve

The Ombudsman observed three key areas in some agency practices that require attention.

Improving internal safeguards to ensure the ACIC use telecommunication intercepts within intelligence operations lawfully

The Ombudsman was concerned the ACIC's planning documents and internal oversight for intelligence operations were not fully effective and that the ACIC failed to use its policy and procedures to support the lawful use of telecommunication intercept powers.

Inadequate review and destruction of records

The ACIC, AFP and NACC all had instances where they did not review and destroy telecommunication interceptions records when they should have. The Ombudsman identified gaps in AFP and NACC procedures which lead to

instances of non-compliance with the destruction requirement under the TIA Act. However, the most serious non-compliance was observed at the ACIC. The ACIC took insufficient steps to review and destroy records predating October 2012.

Lack of records for an emergency interception

The AFP had few records to support an emergency interception under the TIA Act. The Ombudsman was concerned that the lack of records did not adequately demonstrate the emergency circumstances supporting the decision to intercept the telecommunications without a warrant. This included failing to record the considerations when deciding to use a minor as an interpreter when obtaining 'informed consent' for a subsequent related warrant.

Good practices

The AFP complied with obligations under section 79AA of the TIA Act to destroy restricted records and all three agencies complied with the obligations to keep records connected with issue of warrants under section 80 of the TIA Act. The ACIC and NACC also demonstrated compliance with the obligation to keep records in connection with interceptions under section 81.

There was positive engagement with staff at the ACIC, AFP and the NACC. Each agency was receptive to the Ombudsman's questions and showed a willingness to consider and implement the feedback provided by the Ombudsman during the inspections.

The AFP continue to be proactive in identifying and rectifying compliance issues and were transparent with disclosing instances of non-compliance during the Ombudsman's inspections. The Ombudsman considered that the AFP are focused on elevating their compliance maturity, including promoting a healthy approach to proactively identifying and mitigating risks to non-compliance with the TIA Act.

During the inspection period, ACLEI transitioned to become the NACC. The Ombudsman was pleased to see the NACC build upon ACLEI's governance materials during this transition period to strengthen their compliance culture. The Ombudsman found the NACC proactively anticipated compliance risks associated with the increase in the use of the powers and growth in their investigations staffing. Minor instances of non-compliance were identified over both inspections and the Ombudsman remained confident the NACC's internal processes would address any residual compliance issues during the early stages of their operations.

While the Ombudsman's first inspection identified concerns with the ACIC's lack of progress with destroying records, the Ombudsman noted significant efforts by

the ACIC to improve their progress over the entire inspection period. This included a prompt response to the Ombudsman's recommendations to review and destroy most of the affected records by the end of the inspection period.

The Ombudsman changed the focus of the Ombudsman's second ACIC inspection to review their records and compliance with the TIA Act across a sample of ACIC intelligence operations. The Ombudsman recognised this approach changed the demands on ACIC compliance and intelligence team. The ACIC demonstrated significant flexibility to meet the Ombudsman's inspection requirements.

What can agencies improve on?

Improving internal safeguards to ensure the ACIC use telecommunication intercepts within intelligence operations lawfully

A law enforcement agency can obtain a warrant to intercept a telecommunication service(s) if they hold a reasonable suspicion that the material gathered through interception would likely assist in connection with investigating a serious offence.[28] 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 interceptions powers. The Ombudsman recognises the unique role of the ACIC which encompasses the strategic direction of an intelligence agency while having a legal framework that is premised on a law enforcement agency.

At past inspections, the Ombudsman was satisfied that the information contained in the applications and affidavits specified that telecommunications intercepts would be used for an investigative purpose. This inspection was the first time the Ombudsman compared the applications and affidavits with the

[28] Section 46 and 46A limits the issuing of a warrant to intercept communications where an eligible judge or nominated AAT 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.

decisions and plans made by investigators and requesting officers for their intended use of telecommunication intercepts.

The Ombudsman found the ACIC had a robust governance and policy framework in place to allow officers to use these powers in connection with investigating a serious offence. This framework reinforced the need for any telecommunications interception to connect to the investigation of a serious offence. However, in practice, the Ombudsman found planning documents and internal oversight were not fully effective.

An internal operations committee considers submissions for the commencement, prioritisation, extension, review, change or cessation of ACIC projects, and approves the intention to use any covert powers (including telecommunication intercept) when it endorses the project proposal prior to commencing an Intelligence Operation. The project proposal must specify the powers that are intended to be used and the purposes (being project objectives and outputs) for which the powers will be applied. The project proposal that is endorsed by the committee does not authorise the particular use of telecommunication intercepts. That is done through a separate authorisation process.

The Ombudsman reviewed endorsed project proposals and project extensions across two intelligence operations that used telecommunications intercepts powers. The Ombudsman thought there needed to be a better linkage between the use of telecommunications interception to assist in connection with investigating a serious offence with the intended deliverables set out in the project proposals.

The Ombudsman found that ACIC staff did not use its operations management policy and procedures to support the lawful use of telecommunications intercept powers. This policy and related procedures provide a framework that supports using the powers for investigative purposes, including by ensuring that those managing an operation demonstrate that any use of the powers and disclosure of material is connected with the investigative purpose. None of the operations that the Ombudsman reviewed consistently applied the process described in the policy and procedures. The Ombudsman observed a general lack of awareness of the framework across compliance and intelligence teams.

During the Ombudsman's inspection, the Ombudsman made some general observations which indicated that the link with the threshold for being able to use telecommunications intercepts was not always clear. The Ombudsman also appreciates that the line which can distinguish between intelligence activities and the investigation of offences is not clear. Accordingly, the Ombudsman has not yet concluded their views on whether the ACIC has been able to adequately demonstrate a connection between the use of telecommunications intercepts and the thresholds under the TIA Act. The Ombudsman will explore this further at their next inspection.

The Ombudsman made **5 recommendations** to improve the ACIC internal safeguards to ensure telecommunication intercepts are used lawfully within intelligence operations.

In response, the ACIC accepted or accepted in part all of the Ombudsman's recommendations and suggestions. The ACIC commenced activities to strength the internal safeguards supporting the use of telecommunication intercepts.

Inadequate review and destruction of records

Telecommunications interception records are highly intrusive of 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.

The ACIC, AFP and NACC all did not comply with the requirement to destroy telecommunications interception records in accordance with section 79 of the TIA Act when they are not likely to be required for a permitted purpose. The seriousness of the non-compliance varied between the agencies, with the ACIC's delay in handling records being the most concerning.

ACIC

The Ombudsman first noted the ACIC was not reviewing and destroying records during the 2019 inspection. There were a significant number of records dating back to before 2012 that had not yet been reviewed or destroyed. In the Ombudsman's 2021-22 annual report, the Ombudsman highlighted the ACIC had commenced a project to review and assess these legacy records for destruction.

During the first inspection, the Ombudsman was disappointed to learn the ACIC had not significantly progressed the review and destruction of legacy records and more contemporary records also needed reviewing. The project initiated by the ACIC had reached its expected implementation date with very few records being reviewed and destroyed. The Ombudsman was also concerned that the ACIC did not have sufficient procedures in place to review records and ensure they were permitted to be retained under the Act. While there is no requirement in the Act for the ACIC to periodically review the records, the deficiencies in the ACIC's procedures were contributing to the agency's accumulation of records that were not being reviewed for retention or destruction

The Ombudsman **recommended** the ACIC immediately review its Destruction Project and renew the project to ensure dedicated resources,

priority, clear timeframes, executive oversight and regular reporting are implemented to expedite the review and destruction of TI records.

The Ombudsman **recommended** the ACIC policy for reviewing restricted records, to determine whether they should be destroyed or retained for a permitted purpose under the Act, should apply to all restricted records the ACIC holds.

In response to the Ombudsman's findings, the ACIC renewed its project to review and destroy the records. The Ombudsman assessed the progress of this project during the second inspection and found the ACIC had significantly progressed, with the intention to review and destroy all legacy records by 30 June 2024. The ACIC also updated their procedures to ensure records are reviewed every three years in line with the statutory period of a special ACIC Investigation or operation. The ACIC has since advised that this deadline was not met, however were committed to having the destructions project completed by August 2024. The Ombudsman will follow up on the ACIC's progress at the Ombudsman's next inspection.

During this second inspection the Ombudsman noted the ACIC continued to retain records on one warrant, despite the purpose for holding the records no longer existed. The Ombudsman suggested the ACIC ensure that the process of seeking chief officer consideration to authorise destructions forthwith under section 79 of the TIA Act is initiated for these records.

In response the ACIC accepted the Ombudsman's suggestion and committed to reviewing its current procedures.

AFP

During the first inspection the Ombudsman reviewed the AFP's business continuity processes to intercept telecommunications during any system outage. The Ombudsman noted that the AFP relied on a partnership with another agency for its business continuity. This arrangement did not clearly identify which agency held responsibility for destroying records under section 79 of the TIA Act. This created a risk of the AFP not being able to comply with the TIA Act by not being able to destroy records authorised for destruction as they were held on the systems of the third party. The Ombudsman suggested the AFP develop an agreed position with the agency on which agency is responsible for the destruction of these records under section 79 of the TIA Act. In response, the AFP advised they would seek guidance and work with the partner agency to develop an agreed position on who was responsible for destroying any records authorised for destruction.

NACC

At the Ombudsman's first inspection at the NACC, they found the NACC did not have a definition or timeframe for destroying records 'forthwith'. As the NACC relied on a partner agency to destroy records authorised for destruction, the lack of a clear timeframe for destroying these records resulted in several records not being destroyed in a timely way. The Ombudsman suggested the NACC update their internal governance material to include a definitive timeframe for destroying records 'forthwith' and review its partnership arrangements to be compliant with the TIA Act. The NACC advised they updated their procedures to ensure material is destroyed within 28 days of being authorised for destruction. The NACC also transitioned to a new telecommunication interceptions platform and now maintain administrative control of their records.

Deficient record keeping for an emergency circumstance

Keeping adequate records ensures agencies can demonstrate compliance with the TIA Act and account for the use of the telecommunications interception powers.

During the second inspection of the AFP, the Ombudsman reviewed the records relating to a decision to intercept, without a warrant, a telecommunication service in emergency circumstances. The Ombudsman found the AFP did not keep adequate records supporting a critical decision to authorise an emergency interception of a service under section 7(5) of the TIA Act. No contemporaneous notes, records or briefings were provided by the AFP to support the application for an emergency interception or record the considerations made at the time of authorisation.

> The Ombudsman **recommended** the AFP must keep adequate records supporting a decision to make and authorise an emergency interception. This should include recording facts and any considerations of those facts that inform the applicant and authorising officer's reasonable belief and the emergency circumstances that make it impractical to apply for a warrant under Part 2-5 of the Act.

The AFP advised they will update their Standard Operating Procedure and National Guideline to ensure adequate records are kept supporting a decision to make and authorise an emergency interception.

The Ombudsman also found the AFP used a minor as an interpreter to obtain informed consent from the user of telecommunication service (being a parent) to support the emergency interception. While the AFP holds a recording of the conversation with the parent and minor, the Ombudsman was concerned the

AFP did not record any reasons for not seeking a qualified interpreter or any considerations given as to reliability of, or appropriate use of, the minor to act as an interpreter.

> The Ombudsman **recommended** the AFP record the considerations and any decisions to not use a qualified interpreter when obtaining 'informed consent' to support an application for an emergency interception or warrant under Part 2-5 of the TIA Act. The Ombudsman also recommended the AFP determine whether, and in what circumstances, it is appropriate to use a child as an interpreter and incorporate these parameters into their policy and guidelines.

The AFP advised they are seeking advice before providing the Ombudsman's office with an informed response. The Ombudsman will follow up with the AFP at their next inspection.

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.

Definition

An **'issuing authority'** is defined at section 6DB of the TIA Act and means a judge, magistrate or an AAT member who is enrolled as a legal practitioner for at least 5 years, and who has been appointed by the Attorney-General.

'Criminal law-enforcement agencies' are set out at section 110A of the TIA Act. These agencies include all interception agencies as well as the Department of Home Affairs (Home Affairs), ASIC, ACCC and ACT Integrity Commission.

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

A **'serious contravention'** includes:

- offences punishable by imprisonment for a period of at least 3 years,
- serious offences (offences for which a telecommunications interception warrant can be obtained), and
- offences punishable by a fine of at least 180 penalty units ($49,500 at the end of the reporting period) for individuals or 900 penalty units ($247,500 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 2023–24, 738 stored communications warrants were issued, representing a decrease of 57 from the 795 stored communications warrants issued in 2022–23.

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	
		22/23	23/24	22/23	23/24	22/23	23/24
AFP	Made	22	27	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	22	27	-	-	-	-
CCC (WA)	Made	1	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
IBAC	Made	1	3	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	1	3	-	-	-	-
NSW Police	Made	430	357	-	-	-	-
	Refused	1	-	-	-	-	-
	Issued	429	357	-	-	-	-
NT Police	Made	3	8	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	3	8	-	-	-	-
QLD Police	Made	96	121	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	96	121	-	-	-	-

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants		Renewal applications for stored communications warrants	
		22/23	23/24	22/23	23/24	22/23	23/24
SA Police	Made	22	2	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	22	2	-	-	-	-
TAS Police	Made	25	31	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	25	31	-	-	-	-
VIC Police	Made	115	113	-	-	-	-
	Refused	-	-	-	-	-	-
	Issued	115	113	-	-	-	-
WA Police	Made	82	77	-	-	-	-
	Refused	1	1	-	-	-	-
	Issued	81	76	-	-	-	-
TOTAL	**Made**	**797**	**739**	**-**	**-**	**-**	**-**
	Refused	**2**	**1**	**-**	**-**	**-**	**-**
	Issued	**795**	**738**	**-**	**-**	**-**	**-**

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 2023–24, 418 stored communications warrants were subject to conditions or restrictions, this is a decrease of 79 warrants compared to 2022–23.

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

Agency	22/23	23/24
AFP	19	24
NSW Police	429	357
SA Police	22	2
TAS Police	25	31
VIC Police	2	4
TOTAL	**497**	**418**

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 2023–24, lawfully accessed information:

- contributed to 283 arrests
- was given in evidence in 210 proceedings, and
- resulted in 158 convictions in proceedings where such information had been given in evidence.

This is a decrease of 183 from the 466 arrests in 2022-23, an increase of 54 on the 156 proceedings in 2022-23 and a decrease of 6 on the 164 convictions in 2022-23.

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

Agency	Arrests		Proceedings		Convictions	
	22/23	23/24	22/23	23/24	22/23	23/24
AFP	16	39	4	12	4	3

Agency	Arrests		Proceedings		Convictions	
	22/23	23/24	22/23	23/24	22/23	23/24
NSW Police	335	111	55	76	49	38
QLD Police	56	70	48	4	48	4
SA Police	-	-	4	1	-	-
TAS Police	7	5	4	-	-	-
VIC Police	52	58	41	117	63	113
TOTAL	**466**	**283**	**156**	**210**	**164**	**158**

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. Please note that 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 3 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 2023–24, 1,557 domestic preservation notices were given. This is a decrease of 17 notices on the 1,574 given in 2022–23.

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

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	22/23	23/24	22/23	23/24
AFP	141	141	90	-
CCC (WA)	4	3	2	-
Home Affairs	-	2	-	-
IBAC	15	10	5	5
NACC[29]	-	1	-	1
NSW CC	-	1	-	1
NSW Police	656	595	131	163
NT Police	48	96	33	63
QLD CCC	12	11	3	1
QLD Police	225	239	63	61
SA Police	48	39	28	33
TAS Police	69	70	43	27
VIC Police	154[30]	147	21	27

[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 Vic Police for the 2022-23 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).

Agency	Domestic preservation notices issued		Domestic preservation revocation notices issued	
	22/23	23/24	22/23	23/24
WA Police	202	202	104	123
TOTAL	**1,574**[31]	**1,557**	**523**	**505**

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 2023–24, no foreign preservation notices or revocation notices were given. This is the same as in 2022–23.

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,

[31] The figure for Vic Police for the 2022-23 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).

or of a State or Territory that is of the same, or substantially similar nature to, the international offence.

In 2023–24, no applications were made for stored communications warrants as a result of an international assistance application. This is the same as in 2022–23.

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 2023–24, 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. There was no change from 2022–23.

Ombudsman inspection report

The Ombudsman inspects the preservation notices and stored communications access records of all criminal law-enforcement agencies. Under section 186J of the TIA Act, the Ombudsman continues to have a statutory obligation to report on the results of these inspections to the Attorney-General.

The Attorney-General 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.

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. 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.

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.

A criminal law-enforcement agency can authorise the disclosure of prospective data when the disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least 3 years. A prospective data authorisation comes into force once the relevant carrier receives the request and is effective for a maximum period of 45 days.

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 2023–24, there were 353,342 authorisations made by agencies under section 178 of the TIA Act. This is an increase of 28,174 from the 325,168[32] authorisations made in 2022–23.

[32] This includes adjustments made to the 2022-23 Annual Report (see Appendix D).

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	
	22/23	23/24
ACCC	44	45
ACIC	4,894	3,811
AFP	14,304	11,711
ASIC	239	300
CS NSW	2	10
CCC (WA)	109	49
Home Affairs	2,465	2,706
IBAC	286	182
ICAC (NSW)	126[33]	198
ICAC (SA)	111	47
LECC	516[34]	395
NACC[35]	298	332
NSW CC	2,171	2,104
NSW Police	113,078	124,079
NT Police	2,158	2,280
QLD CCC	353	443
QLD Police	27,663	31,125
SA Police	7,026	6,562
TAS Police	2,508[36]	3,118

[33] The figure for ICAC (NSW) for the 2022-23 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).
[34] The figure for LECC for the 2022-23 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).
[35] 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.
[36] The figure for TAS Police for the 2022-23 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).

Agency	Authorisations	
	22/23	23/24
VIC Police	112,749	129,561[37]
WA Police	34,068	34,284
TOTAL	**325,168[38]**	**353,342**

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 2023–24, there were 5,885 authorisations made by agencies under section 178A of the TIA Act. This is an increase of 661 from the 5,224 authorisations made in 2022–23.

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

Agency	Authorisations	
	22/23	23/24
AFP	73	48
NSW Police	2,709	3,641

[37] Note the Victoria Police has reported that 520 of these authorisations were inadvertently given for missing persons. Consequently, the total number of prospective data authorisations is reported as larger than the total number of offences associated with this at Table 33B.
[38] This reflects amendments made to the figures for ICAC (NSW), LECC and TAS Police for the 2022-23 reporting period due to errors (refer to Appendix D of this Annual Report).

Agency	Authorisations	
	22/23	23/24
NT Police	36	28
QLD Police	364	635
SA Police	128	150
TAS Police	407[39]	116
VIC Police	1,134	973
WA Police	373	294
TOTAL	**5,224**[40]	**5,885**

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 2023–24, there were 694 authorisations made by agencies under section 179 of the TIA Act. This is a decrease of 653 from the 1,347 authorisations made in 2022–23.

[39] The figure for TAS Police for the 2022-23 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).
[40] The figure for TAS Police for the 2022-23 reporting period has been amended due to an error (refer to Appendix D of this Annual Report).

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	
	22/23	23/24
ACCC	-	21
AFP	10	17
ASIC	7	2
Home Affairs	20	36
NSW Police	1,299	598
NT Police	1	-
TAS Police	3	2
WA Police	7	18
TOTAL	**1,347**	**694**

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 imprisonment for at least 3 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 2023–24, there were 52,863 prospective data authorisations made by agencies under section 180 of the TIA Act. This is an increase of 8,384 on the 44,479 authorisations made in 2022–23.

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

Agency	Number of authorisations made	
	22/23	23/24
ACCC	4	7
ACIC	1,526	1,042
AFP	7,863	12,613
ASIC	36	50
CCC (WA)	29	19
Home Affairs	299	372
IBAC	170	77
ICAC (NSW)	36	41
LECC	161	171
NACC[41]	36	44
NSW CC	781	1,300
NSW Police	3,365	3,788
NT Police	403	568
QLD CCC	76	111
QLD Police	4,989	6,391
SA Police	452	497
TAS Police	118	212
VIC Police	18,733[42]	19,181[43]
WA Police	5,402	6,379
TOTAL	**44,479**	**52,863**

[41] 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.

[42] Note the Victoria Police has reported that 63 of these authorisations were inadvertently given for missing persons.

[43] Note the 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 2023–24, the AFP made the following authorisations under section 180A, 180B, 180C, and 180D of the TIA Act:

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

The AFP made 25 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: China (1 disclosure), Croatia (2 disclosures), France (2 disclosures), Germany (1 disclosure), Greece (2 disclosures), Republic of Korea (South Korea) (2 disclosures), Macau (2 disclosures), Montenegro (1 disclosure), Nepal (1 disclosure), New Zealand (2 disclosures), Poland (1 disclosure), San Marino (1 disclosure), Singapore (1 disclosure), Taiwan Province (1 disclosure) and United States of America (5 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 63,925 authorisations for illicit drug offences, 39,934 for abduction and 36,907 authorisations for unlawful entry.

Under section 178A of the TIA Act, 5,879 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	154	39,774	6	**39,934**
Acts – injury	105	18,037	2	**18,144**
Bribery or corruption	496	106	719	**1,321**
Cartel offences	42	10	-	**52**
Conspire/aid/abet serious offence	26	335	-	**361**
Cybercrime and telecommunications	710	4,305	3	**5,018**
Dangerous acts	29	7,604	-	**7,633**
Fraud	4,005	23,008	532	**27,545**
Homicide	406	31,656	182	**32,244**
Illicit drug offences	7,794	54,808	1,323	**63,925**
Loss of life	18	1,470	4	**1,492**
Misc.	1,118	14,958	107	**16,183**
Justice procedures	269	2,324	132	**2,725**
Organised offences	718	4,029	10	**4,757**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	-	1,154	-	**1,154**

Category of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Public revenue	96	236	1	**333**
People smuggling	143	20	-	**163**
Weapons	350	6,214	144	**6,708**
Property damage	146	1,235	-	**1,381**
Public order offences	4	1,071	-	**1,075**
Robbery	148	19,042	15	**19,205**
Serious damage	4	7,746	-	**7,750**
Sexual assault	2,059	23,616	44	**25,719**
Terrorism offences	406	559	188	**1,153**
Theft	232	28,221	4	**28,457**
Traffic	2	3,460	-	**3,462**
Unlawful entry	117	36,778	12	**36,907**
TOTAL	**19,597**	**331,776**	**3,428**	**354,801**

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[44]	AFP	ASIC	Home Affairs	NACC	TOTAL
Abduction	-	-	154	-	-	-	**154**
Acts – injury	-	-	105	-	-	-	**105**
Bribery or corruption	-	-	36	-	-	460	**496**
Cartel offences	42	-	-	-	-	-	**42**
Conspire/aid/abet serious offence	-	-	6	20	-	-	**26**
Cybercrime and telecommunications	-	-	681	29	-	-	**710**
Dangerous acts	-	-	29	-	-	-	**29**
Fraud	-	2,313	799	283	105	505	**4,005**
Homicide	-	-	406	-	-	-	**406**
Illicit drug offences	-	1,342	4,862	-	1,590	-	**7,794**
Loss of life	-	-	18	-	-	-	**18**
Misc.	-	2	365	27	724	-	**1,118**
Justice procedures	3	-	266	-	-	-	**269**

[44] 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[44]	AFP	ASIC	Home Affairs	NACC	TOTAL
Organised offences	-	-	718	-	-	-	**718**
Public revenue	-	96	-	-	-	-	**96**
People smuggling	-	-	143	-	-	-	**143**
Weapons	-	-	109	-	241	-	**350**
Property damage	-	-	146	-	-	-	**146**
Public order offences	-	-	4	-	-	-	**4**
Robbery	-	-	148	-	-	-	**148**
Serious damage	-	-	4	-	-	-	**4**
Sexual assault	-	32	2,027	-	-	-	**2,059**
Terrorism offences	-	-	404	-	2	-	**406**
Theft	-	26	162	-	44	-	**232**
Traffic	-	-	2	-	-	-	**2**
Unlawful entry	-	-	117	-	-	-	**117**
TOTAL	**45**	**3,811**	**11,711**	**359**	**2,706**	**965**	**19,597**

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	14,574	344	4,683	270	461	16,337	3,105	**39,774**
Acts – injury	9,696	44	1,420	94	27	4,503	2,253	**18,037**
Bribery or corruption	-	1	71	13	4	1	16	**106**
Cartel offences	10	-	-	-	-	-	-	**10**
Conspire/aid/abet serious offence	215	31	1	5	-	-	83	**335**
Cybercrime and telecommunications	2,583	39	1,092	7	290	107	187	**4,305**
Dangerous acts	1,549	73	-	256	11	5,179	536	**7,604**
Fraud	8,846	35	660	650	157	11,147	1,513	**23,008**
Homicide	20,438	308	1,316	767	182	7,014	1,631	**31,656**
Illicit drug offences	18,711	1,955	4,054	2,457	877	21,030	5,724	**54,808**
Loss of life	897	11	354	13	36	159	-	**1,470**
Misc.	6,273	189	7,674	80	38	259	445	**14,958**
Justice procedures	764	8	119	48	65	853	467	**2,324**
Organised offences	3,126	5	43	16	1	49	789	**4,029**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	1,141	-	-	3	3	7	-	**1,154**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Public revenue	-	-	-	-	-	236	-	**236**
People smuggling	1	19	-	-	-	-	-	**20**
Weapons	2,373	-	297	170	18	3,279	77	**6,214**
Property damage	1,075	8	-	110	21	19	2	**1,235**
Public order offences	411	-	13	-	7	560	80	**1,071**
Robbery	7,280	67	1,664	281	81	7,381	2,288	**19,042**
Serious damage	913	-	878	4	92	5,110	749	**7,746**
Sexual assault	9,553	382	2,466	712	214	7,094	3,195	**23,616**
Terrorism offences	165	-	1	18	-	372	3	**559**
Theft	9,727	31	1,585	227	356	12,631	3,664	**28,221**
Traffic	609	1	457	27	12	2,024	330	**3,460**
Unlawful entry	3,149	16	2,277	334	165	23,690	7,147	**36,778**
TOTAL	**124,079**	**3,567**	**31,125**	**6,562**	**3,118**	**129,041**	**34,284**	**331,776**

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	ACT IC	CS NSW	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Abduction	-	-	-	-	-	-	-	6	-	**6**
Acts – injury	-	-	2	-	-	-	-	-	-	**2**
Bribery or corruption	-	-	38	174	69	47	260	-	131	**719**
Cybercrime and telecommunications	-	-	-	-	3	-	-	-	-	**3**
Fraud	-	-	-	3	122	-	13	287	107	**532**
Homicide	-	-	-	-	-	-	1	181	-	**182**
Illicit drug offences	-	-	-	-	-	-	6	1,151	166	**1,323**
Loss of life	-	-	-	-	-	-	-	4	-	**4**
Misc.	-	-	9	-	-	-	-	98	-	**107**
Justice procedures	-	10	-	5	2	-	115	-	-	**132**
Organised offences	-	-	-	-	-	-	-	10	-	**10**
Public revenue	-	-	-	-	-	-	-	1	-	**1**
Weapons	-	-	-	-	-	-	-	144	-	**144**
Robbery	-	-	-	-	2	-	-	13	-	**15**
Sexual assault	-	-	-	-	-	-	-	5	39	**44**
Terrorism offences	-	-	-	-	-	-	-	188	-	**188**
Theft	-	-	-	-	-	-	-	4	-	**4**

Categories of offences	ACT IC	CS NSW	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NSW CC	QLD CCC	TOTAL
Unlawful entry	-	-	-	-	-	-	-	12	-	**12**
TOTAL	**-**	**10**	**49**	**182**	**198**	**47**	**395**	**2,104**	**443**	**3,428**

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	ACT IC	ASIC	Home Affairs	NSW Police	NT Police	TAS Police	WA Police	TOTAL
Abduction	-	-	-	-	-	23	-	-	4	**27**
Acts – injury	-	-	-	-	-	22	-	-	-	**22**
Cartel offences	-	-	-	-	-	-	-	-	-	**-**
Conspire/aid/abet serious offence	-	-	-	-	-	1	-	-	-	**1**
Cybercrime and telecommunications	-	-	-	-	-	2	-	-	-	**2**
Dangerous acts	-	-	-	-	-	94	-	-	-	**94**
Fraud	-	-	-	2	-	51	-	-	-	**53**
Homicide	-	-	-	-	-	8	-	-	-	**8**
Illicit drug offences	-	-	-	-	-	80	-	-	-	**80**
Loss of life	-	-	-	-	-	9	-	-	-	**9**

Categories of offences	ACCC	AFP	ACT IC	ASIC	Home Affairs	NSW Police	NT Police	TAS Police	WA Police	TOTAL
Miscellaneous	-	-	-	1	-	39	-	2	2	**44**
Justice procedures	-	-	-	-	-	7	-	-	5	**12**
Organised offences	-	-	-	-	-	42	-	-	2	**44**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	21	11	-	-	36	79	-	-	-	**147**
Public revenue	-	6	-	-	-	-	-	-	-	**6**
Weapons	-	-	-	-	-	6	-	-	-	**6**
Property damage	-	-	-	-	-	14	-	-	-	**14**
Public order	-	-	-	-	-	4	-	-	-	**4**
Robbery	-	-	-	-	-	33	-	-	-	**33**
Serious damage	-	-	-	-	-	-	-	-	-	**-**
Sexual assault	-	-	-	-	-	19	-	-	-	**19**
Terrorism offences	-	-	-	-	-	-	-	-	-	**-**
Theft	-	-	-	-	-	34	-	-	-	**34**
Traffic offences	-	-	-	-	-	27	-	-	5	**32**
Unlawful entry	-	-	-	-	-	4	-	-	-	**4**
TOTAL	**21**	**17**	**-**	**3**	**36**	**598**	**-**	**2**	**18**	**695**

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)

Categories of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
Abduction	46	3,433	4	**3,483**
Acts – injury	24	2,163	2	**2,189**
Bribery or corruption	86	30	312	**428**
Cartel offences	7	2	-	**9**
Conspire/aid/abet serious offence	16	201	-	**217**
Cybercrime and telecommunications	188	111	-	**299**
Dangerous acts	10	956	-	**966**
Fraud	944	1,197	230	**2,371**
Homicide	210	1,030	26	**1,266**
Illicit drug offences	3,291	11,451	693	**15,435**
Loss of life	1	62	2	**65**
Misc.	297	388	31	**716**
Justice procedures	76	176	11	**263**
Organised offences	8,154	290	27	**8,471**
Other offences relating to the enforcement of a law imposing a pecuniary penalty	-	16	-	**16**
Public revenue	81	5	-	**86**

Categories of offences	Commonwealth agencies	State and Territory Police	State and Territory Integrity Agencies	TOTAL
People smuggling	82	2	-	**84**
Weapons	166	1,289	289	**1,744**
Property damage	19	96	-	**115**
Public order offences	-	57	-	**57**
Robbery	46	1,955	20	**2,021**
Serious damage	1	698	-	**699**
Sexual assault	309	1,876	7	**2,192**
Terrorism offences	148	58	78	**284**
Theft	159	3,903	7	**4,069**
Traffic	10	146	-	**156**
Unlawful entry	37	5,389	10	**5,436**
TOTAL	**14,408**	**36,980**	**1,749**	**53,137**

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)

Categories of offences	ACCC	ACIC[45]	AFP	ASIC	Home Affairs	NACC	TOTAL
Abduction	-	-	46	-	-	-	**46**
Acts – injury	-	-	24	-	-	-	**24**
Bribery or corruption	-	-	38	-	-	48	**86**
Cartel offences	7	-	-	-	-	-	**7**
Conspire/aid/abet serious offence	-	-	10	6	-	-	**16**
Cybercrime and telecommunications	-	2	186	-	-	-	**188**
Dangerous acts	-	-	10	-	-	-	**10**
Fraud	-	536	308	50	8	42	**944**
Homicide	-	-	210	-	-	-	**210**
Illicit drug offences	-	461	2,676	-	154	-	**3,291**
Loss of life	-	-	1	-	-	-	**1**
Misc.	-	-	168	-	129	-	**297**
Justice procedures	-	-	76	-	-	-	**76**

[45] 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[45]	AFP	ASIC	Home Affairs	NACC	TOTAL
Organised offences	-	-	8,154	-	-	-	**8,154**
Public revenue	-	56	25	-	-	-	**81**
People smuggling	-	-	82	-	-	-	**82**
Weapons	-	-	85	-	81	-	**166**
Property damage	-	-	19	-	-	-	**19**
Robbery	-	-	46	-	-	-	**46**
Serious damage	-	-	1	-	-	-	**1**
Sexual assault	-	7	302	-	-	-	**309**
Terrorism offences	-	-	148	-	-	-	**148**
Theft	-	34	125	-	-	-	**159**
Traffic	-	-	10	-	-	-	**10**
Unlawful entry	-	-	37	-	-	-	**37**
TOTAL	**7**	**1,096**	**12,787**	**56**	**372**	**90**	**14,408**

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)

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Abduction	310	4	721	38	10	2,078	272	**3,433**
Acts – injury	490	26	58	4	6	1,144	435	**2,163**
Bribery or corruption	3	2	-	1	-	24	-	**30**
Cartel offences	2	-	-	-	-	-	-	**2**
Conspire/aid/abet serious offence	34	1	4	2	-	106	54	**201**
Cybercrime and telecommunications	51	15	20	-	3	8	14	**111**
Dangerous acts	32	-	65	1	-	810	48	**956**
Fraud	108	1	213	2	-	745	128	**1,197**
Homicide	174	9	162	12	9	574	90	**1,030**
Illicit drug offences	1,220	449	3,257	286	148	3,923	2,168	**11,451**
Loss of life	38	1	7	-	-	16	-	**62**
Misc.	217	1	44	3	-	18	105	**388**
Justice procedures	35	-	-	2	-	96	43	**176**
Organised offences	51	-	17	1	-	1	220	**290**

Categories of offences	NSW Police	NT Police	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Other offences relating to the enforcement of a law imposing a pecuniary penalty	7	-	9	-	-	-	-	**16**
Public revenue	2	-	-	3	-	-	-	**5**
People smuggling	-	2	-	-	-	-	-	**2**
Weapons	198	-	173	13	1	901	3	**1,289**
Property damage	33	-	42	-	-	21	-	**96**
Public order offences	13	-	-	2	-	14	28	**57**
Robbery	167	7	327	22	7	1,079	346	**1,955**
Serious damage	26	2	78	-	3	409	180	**698**
Sexual assault	122	30	185	62	8	1,042	427	**1,876**
Terrorism offences	2	-	-	3	-	53	-	**58**
Theft	223	-	555	7	6	2,410	702	**3,903**
Traffic	10	13	-	-	4	88	31	**146**
Unlawful entry	220	-	454	37	7	3,586	1,085	**5,389**
TOTAL	**3,788**	**563**	**6,391**	**501**	**212**	**19,146**	**6,379**	**36,980**

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)

Categories of offences	ACT IC	CCC (WA)	IBAC	ICAC (NSW)	LECC	NSW CC	QLD CCC	TOTAL
Abduction	-	-	-	-	-	4	-	**4**
Acts – injury	-	2	-	-	-	-	-	**2**
Bribery or corruption	-	38	77	25	154	-	18	**312**
Fraud	-	-	-	12	6	186	26	**230**
Homicide	-	-	-	-	-	26	-	**26**
Illicit drug offences	-	-	-	-	-	630	63	**693**
Loss of life	-	-	-	-	-	2	-	**2**
Misc.	-	9	-	-	-	22	-	**31**
Justice procedures	-	-	-	-	11	-	-	**11**
Organised offences	-	-	-	-	-	27	-	**27**
Weapons	-	-	-	-	-	289	-	**289**
Robbery	-	-	-	4	-	16	-	**20**
Sexual assault	-	-	-	-	-	3	4	**7**
Terrorism offences	-	-	-	-	-	78	-	**78**
Theft	-	-	-	-	-	7	-	**7**
Unlawful entry	-	-	-	-	-	10	-	**10**
TOTAL	-	49	77	41	171	1,300	111	**1,749**

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 3 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 2023–24, there were 314,837 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.[46]

[46] 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	10	3	7	2	3	2	-	3	43	**73**
ACIC	3,058	356	127	58	98	34	24	2	87	**3,844**
AFP	4,920	2,410	1,318	736	826	235	240	137	1,059	**11,881**
ACT IC	-	-	-	-	-	-	-	-	-	-
ASIC	71	23	20	6	7	15	13	3	47	**205**
CS NSW	5	4	1	-	-	-	-	-	-	**10**
CCC (WA)	32	7	3	-	1	4	-	-	2	**49**
Home Affairs	1,976	412	142	55	33	23	26	21	54	**2,742**
IBAC	208	7	0	12	12	2	2	2	14	**259**
ICAC (NSW)	50	8	0	0	4	3	3	22	109	**199**
ICAC (SA)	15	4	2	2	-	8	-	5	11	**47**
LECC	524	24	10	1	-	-	-	-	7	**566**
NACC	211	17	2	12	-	4	8	8	70	**332**

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
NSW CC	1,737	128	34	89	43	4	7	15	47	**2,104**
NSW Police	118,445	2,715	1,815	2,081	692	563	446	396	1,213	**128,366**
NT Police	2,106	78	20	30	13	7	5	8	21	**2,288**
QLD CCC	285	52	20	18	8	18	15	3	24	**443**
QLD Police	27,021	1,629	965	587	384	255	170	143	609	**31,763**
SA Police	5,251	432	291	224	203	124	118	69	507	**7,219**
TAS Police	2531	245	170	74	47	19	15	19	116	**3,236**
VIC Police	112,886	7,430	3,362	1,898	1,196	663	387	341	2371	**130,534**
WA Police	33,495	2,756	1,426	798	604	300	203	165	1,228	**40,975**
TOTAL	314,837	18,740	9,735	6,683	4,174	2,283	1,682	1,362	7,639	**367,135**

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[47]
- 'Traffic data' which includes information such as the time, duration, and source of a communication[48]

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)[49]

Agency	Subscriber data	Traffic data
ACCC	28	38
ACIC	2,473	1,372
AFP	6,855	5,051
ASIC	148	177
CS NSW	5	6
CCC (WA)	29	20
Home Affairs	2,199	1,274
IBAC	126	88
ICAC (NSW)	73	126
ICAC (SA)	15	32
LECC	279	116

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

Agency	Subscriber data	Traffic data
NACC	223	109
NSW CC	1,221	973
NSW Police	85,349	60,042
NT Police	1,715	573
QLD CCC	322	121
QLD Police	22,906	6,584
SA Police	5,319	1,403
TAS Police	2,295	941
VIC Police	79,638	50,896
WA Police	26,478	14,497
TOTAL	**237,696**	**144,439**

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.

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.

In 2023–24, no JIWs were issued and no authorisations were made under a JIW. This is consistent with 2022–23.

In August 2020, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) handed down its report on its Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press. The PJCIS made a number of recommendations, including to require additional record-keeping and reporting requirements in respect of PIAs. The Government is committed to implementing these recommendations. Ahead of legislative amendments, the Government has included information about the number of PIAs, their location and qualification as at 30 June 2024 in **Table 38**.

Table 38: Public interest advocates

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

Industry estimated cost of implementing data retention

Since 13 October 2015, carriers and service providers have been required to 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.

Information collected from industry by the Australian Communications and Media Authority, shows the cost of complying with the data retention obligations.

This information is set out in **Table 39**. **Table 39** further sets out the costs recovered from criminal law-enforcement agencies for the purpose of complying with their data retention obligations.

Table 39: 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)
2022–23	$26,019,314.37	$15,171,490.00
2023–24	$29,729,879.35	$17,111,920.00

Chapter 5: International production orders

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

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 which can obtain stored communications and interception warrants under Chapters 2 and 3 of the TIA Act and can authorise the disclosure of telecommunications data under Chapter 4 of the TIA Act can obtain IPOs for the equivalent information. (However, unlike Chapter 4 authorisations for telecommunications data, IPOs seeking telecommunications data must be issued by an independent issuing authority and cannot be authorised internally within an agency.)

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), entered into force on 31 January 2024. This is the only designated international agreement under the International Production Order framework.

No applications were made for IPOs, and no IPOs were issued, during 2023-24.

Under clause 128 of Schedule 1 to the TIA Act, agencies are required to provide particular information and statistics to the Attorney-General on their applications for IPOs, and if any IPOs were issued, information about those IPOs. Under paragraph 131(1)(a) of Schedule 1 to the TIA Act, that information must then be included in this report.

Under clause 130, the Australian Designated Authority must report to the Attorney-General particular information and statistics relating to the functions of the Australian Designated Authority. Under Paragraph 131(1)(b), that information must then be included in this report.

No applications were made for IPOs, and no IPOs were issued, during 2023-24.

All of the statistics for the categories of information under clauses 128 and 130 are therefore nil or not applicable.

The department has, and is continuing to, work with prescribed communications providers and Australian agencies to put the Agreement into practical operation. This has included certifying agencies as having in place appropriate policies and procedures to comply with the Agreement and establishing methods of sending IPOs to, and receiving data from, prescribed communications providers.

The IPO framework is currently operational with several orders being issued and sent to the Australian Designated Authority for consideration. As the orders do not relate to the 2023-24 year, they will be reported on in the 2024-25 Annual Report.

Chapter 6: Industry assistance

Part 15 of the Telecommunications Act provides a framework through which Australian agencies and the communications industry 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 through the use of three powers:

- **Technical Assistance Request (TAR):** Agencies can request voluntary help from designated communications providers.[50]
- **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, including in circumstances where they may not have the technical capability to do so.

Table 40: Eligible agencies under Part 15 of the Telecommunications Act

Agency	Industry assistance powers available to agencies		
	TAR	TAN	TCN
Interception agencies[51]	✓	✓	✓
ASD	✓	×	×
ASIO	✓	✓	✓
ASIS	✓	×	×

[50] Categories of designated communications providers and their eligible activities are at section 317C of the Telecommunications Act.

[51] In contrast to the TIA Act, this does not include anti-corruption and integrity commissions.

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 to law enforcement must be related to investigating serious Australian offences or assisting the enforcement of serious foreign offences, or safeguarding national security.

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 3 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 3 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 41**. In 2023–24, 60 TARs and 2 TANs were given by interception agencies to designated communications providers. This represented a decrease of 6 TARs and an increase of 2 TANs from the previous year. No TCNs were issued in 2023-23 or 2023-4.

Table 41: 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	
	22/23	23/24	22/23	23/24	22/23	23/24
ACIC	6	5	-	-	-	-
AFP	-	-	-	2	-	-
NSW Police	53	47	-	-	-	-
QLD Police	1	-	-	-	-	-
VIC Police	5	3	-	-	-	-
WA Police	1	5	-	-	-	-
TOTAL	**66**	**60**	**-**	**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 27 for homicide and related offences and 11 for illicit drug offences.

This information is provided in **Table 42**.

Table 42: Kinds of serious Australian offences enforced through Technical Assistance Requests – paragraph 317ZS(1)(d) of the Telecommunications Act

Categories of offences	ACIC	NSW Police	VIC Police	WA Police	TOTAL
Acts intended to cause injury	-	1	-	-	**1**
Abduction	-	4	-	-	**4**
Fraud, deception and related offences	-	1	1	-	**2**
Homicide and related offences	-	24	3	-	**27**
Illicit drug offences	-	9	1	1	**11**
Justice procedures	-	-	-	1	**1**
Organised crime	-	1	-	1	**2**
Property damage and environment pollution	-	3	-	1	**4**
Robbery, extortion and related offences	-	1	-	-	**1**
Serious damage	-	1	-	-	**1**
Weapons	-	1	-	-	**1**
Theft and related offences	-	-	2	-	**2**
Other serious Australian offences	4	1	-	1	**6**
TOTAL	**4**	**47**	**7**	**5**	**63**

Oversight of industry assistance powers

Use of the industry assistance powers is subject to independent oversight by either the Inspector-General of Intelligence and Security (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 will 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

For further information about the TIA Act and Part 15 of the Telecommunications Act, please contact AGD:

Electronic Surveillance Section

Attorney-General's Department

3-5 NATIONAL CIRCUIT

BARTON ACT 2600

ElectronicSurveillance@ag.gov.au

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

Appendix A: Lists of tables and figures

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
Administration of justice/government offences	TIA Act, subsection 5D(8)
Assist escape punishment/dispose of proceeds	TIA Act, subsection 5D(7)
Bribery or corruption 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)
Conspire/aid/abet serious offence	TIA Act, subsection 5D(6)
Cybercrime offences	TIA Act, subsection 5D(5)
Espionage and foreign interference offences	TIA Act, paragraphs 5D(1)(e), (ic), (id), (if), (ig), (vii) and (viii)
Kidnapping	TIA Act, paragraph 5D(1)(b)
Loss of life or personal injury	TIA Act, subparagraphs 5D(2)(b)(i) and (ii)
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 offences and/or offences relating to criminal organisations	TIA Act, subsections 5D(3AA), (8A) and (9)
People smuggling and related offences	TIA Act, subsection 5D(3A)
Serious damage to property and/or serious arson	TIA Act, subparagraphs 5D(2)(b)(iii) and (iiia)
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 or revenue	TIA Act, subparagraph 5D(2)(b)(vi)
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

Home Affairs 2020-2021

Home Affairs identified a correction regarding stored communications warrants for the 2020-21 reporting period. This error was detected following an inspection by the Commonwealth Ombudsman which found that four stored communication warrants were issued for the reporting period in relation to a single investigation.

The below table details both the original figure provided for the previous annual report and the amended figure as identified and corrected.

Applications, telephone applications and renewal applications for stored communications warrants – paragraphs 162(1)(a)-(b), 162(2)(a)-(b) and 162(2)(c)[52]

Agency	Relevant statistics	Applications for stored communications warrants	
		20/21 original	20/21 updated
Home Affairs	Made	1	4
	Refused	-	-
	Issued	1	4
TOTAL	**Made**	**998**	**1,001**
	Refused	**-**	**-**
	Issued	**998**	**1,001**

[52] Corrections refers to Table 24, page 46, 2020-21 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act*.

ICAC NSW 2022–23

ICAC NSW identified a correction regarding authorisations made for access to existing information or documents for the enforcement of the criminal law for the 2022-23 reporting period. This error was detected following an inspection by the Commonwealth Ombudsman which found that one authorisation was omitted due to an administration error. ICAC NSW advised that electronic workflows are being developed in the case management system. Accurate reports of statistics will be generated from the electronic workflows, replacing the need for data to be manually entered into a physical register and reducing the risk of future mistakes.

The below table details both the original figure provided for the previous annual report and the amended figure 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	
	22/23 original	22/23 updated[53]
ICAC (NSW)	125	126
TOTAL	**326,771**	**325,168**[54]

[53] Corrections refers to Table 30, page 58, 2022-23 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act*.

[54] This figure includes updates identified by other agencies in Appendix D of this Annual Report.

LECC 2022–23

The LECC identified a correction regarding access to telecommunications data for the 2022–23 reporting period. This error was detected by the LECC in the preparation of the Commonwealth Ombudsman's inspection which found that one authorisation was omitted due to an error in recordkeeping.

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	
	22/23 original	22/23 updated[55]
LECC	515	516
TOTAL	**326,771**	**325,168**[56]

[55] Corrections refers to Table 30, page 58, 2022-23 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act.*

[56] This figure includes updates identified by other agencies in Appendix D of this Annual Report.

TAS Police 2022–23

TAS Police identified corrections regarding access to telecommunications data for the 2022–23 reporting period. These errors were detected following an inspection by the Commonwealth Ombudsman which found that the data Tasmania Police had reported on the total number of requests related to individual subscriber checks rather than the number of authorisations. Internal processes have been amended to ensure the number of authorisations is captured and accurately reported on 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	
	22/23 original	22/23 updated[57]
TAS Police	4,113	2,508
TOTAL	**326,771**	**325,168**[58]

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

Agency	Authorisations	
	22/23 original	22/23 updated[59]
TAS Police	1,302	407
TOTAL	**6,119**	**5,224**

[57] Corrections refers to Table 30, page 58, 2022-23 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act*.
[58] This figure includes updates identified by other agencies.
[59] Corrections refers to Table 31, page 60, 2022-23 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	22/23 Original	22/23 Updated[60]
Abduction	319	292
Acts – injury	71	63
Cybercrime	53	46
Dangerous acts	18	21
Fraud	169	139
Homicide	612	405
Illicit drug offences	2,082	825
Loss of life	7	3
Misc.	23	22
Justice procedures	39	40
Weapons	41	29
Property damage	14	11
Robbery	81	72
Serious damage	29	28
Sexual assault	117	112
Theft	303	268
Unlawful entry	122	119
TOTAL (TAS Police)[61]	**4,113**	**2,508**

[60] Corrections refers to Table 34, pages 66-67, 2022-23 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act*.

[61] Categories without corrections have not been replicated in the table. The total includes figures of reported offence categories not included in this table.

Offences for which authorisations were made under section 178A to access existing data to locate a missing person – paragraph 186(1)(e)

Categories of offences	22/23 Original	22/23 Updated[62]
No offence attached to s178 authorisation for the location of a missing person	1,302	407
TOTAL[63]	**6,119**	**5,224**

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

TAS Police	Age of disclosure						
	0-3 months	3-6 months	6-9 months	12-15 months	15-18 months	Over 24 months	TOTAL (TAS Police)[64]
22/23 Original	4,616	430	103	67	37	91	**5,418**
22/23 Updated[65]	2,125	428	97	66	36	92	**2,918**

[62] Corrections refers to page 59, 2022-23 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act*.
[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] Columns without corrections have not been replicated in the table (namely, 9-12, 18-21 and 21-24 months). The total includes figures of reported offence categories not included in this table.
[65] Corrections refers to Table 37, page 82, 2022-23 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act.*

Table 39: Types of retained data disclosed in authorisations – paragraphs 186(1)(g) and 186(1)(h)

TAS Police	Item 1: subscriber data	Items 2-6: traffic data	TOTAL (TAS Police)
22/23 Original	4,322	1,096	**5,418**
22/23 Updated[66]	2,190	728	**2,918**

[66] Corrections refers to Table 38, page 84, 2022-23 Annual Report under the TIA Act and Part 15 of the *Telecommunications Act*.

VIC Police 2022–23

VIC Police identified a correction regarding stored communications data for the 2022-23 reporting period. This error was detected following an inspection by the Commonwealth Ombudsman. VIC Police advised this error occurred due to an internal administrative error.

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

Domestic preservation notices – subsection 161A(1)

Agency	Domestic preservation notices issued	
	22/23 original	22/23 updated[67]
VIC Police	157	154
TOTAL	**1,577**	**1,574**

[67] Corrections refers to Table 29, page 54, 2022-23 Annual Report under the TIA Act and Part 15 of the Telecommunications Act.

Notes