COMMONWEALTH OMBUDSMAN

Ombudsman Oversight of Covert Electronic Surveillance

2022 to 2023

December 2023

Contents

Abbreviations

Acronym	Agency / Organisation
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACLEI	Australia Commission for Law Enforcement Integrity
ADA	Australian Designated Authority
AFP	Australian Federal Police
ASIC	Australian Securities and Investments Commission
CCC (QLD)	Queensland Crime and Corruption Commission
CCC (WA)	Western Australia Crime and Corruption Commission
CLOUD Act Agreement	Australia-US Clarifying Lawful Overseas Use of Data Act Agreement
DHA	Department of Home Affairs
IA	Industry Assistance
IBAC	Independent Broad-based Anti-Corruption Commission
ICAC (NSW)	New South Wales Independent Commission Against Corruption
ICAC (SA)	South Australia Independent Commissioner Against Corruption
IPO	International Production Order
LECC	Law Enforcement Conduct Commission
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police Force
QLD Police	Queensland Police Service
SA Police	South Australia Police
SC	Stored Communication
TAS Police	Tasmania Police
TD	Telecommunications Data
TMP	Targeting and Minimisation Procedure
VIC Police	Victoria Police
WA Police	Western Australia Police Force
' – '	Indicates nil use of the power

Executive Summary

This report presents the results of inspections conducted by the Office of the Commonwealth Ombudsman (our Office) for the period 1 July 2022 to 30 June 2023 for:

- Stored Communications and Telecommunications Data Powers under section 186B of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act)
- International Production Orders under cl 142 and cl 143 of Schedule 1 to the TIA Act, and
- Industry Assistance Powers under s 317ZRB of the *Telecommunications Act 1997* (the Telecommunications Act).

In order to minimise risk to current law enforcement operations, we conduct retrospective inspections.

Our Office provides independent oversight of agencies' use of these covert and intrusive electronic surveillance powers by inspecting agencies' records, policies and processes to assess whether their use of the powers complies with the legislation. We enhance transparency and public accountability by reporting our findings in this annual report, which the Attorney-General (as the relevant Minister) is required to table in Parliament.

In 2022-2023 we inspected:

- 17 agencies' use of stored communications powers under Chapter 3 of the TIA Act
- 21 agencies' use of telecommunications data powers under Chapter 4 of the TIA Act
- 7 agencies' operational readiness to use international production orders under Schedule 1 of the TIA Act, and
- 4 agencies' use of industry assistance powers under Part 15 of the Telecommunications Act.

There was a decrease in the number of compliance related findings we made in 2022-2023 compared to the 2021-2022 inspection period. This reflected a broad trend across agencies of improved policies, procedures, and controls to mitigate risks of non-compliance based on findings from our previous inspections. The reduction in findings can also be attributed to most agencies continuing to improve their compliance culture and proactively identifying and addressing compliance risks.

While we acknowledge these positive steps, we continued to identify areas for improvement across most agencies. We identified instances at some agencies where we were not satisfied

with the remedial actions taken in response to previous findings, including instances where our recommendations had only been partially implemented. Where we were not satisfied with an agency's progress, we reiterated or made further recommendations or suggestions aimed at improving processes to prevent future recurrence of previously identified issues.

Table 1: Total number of findings 2021-2022 and 2022-2023

Regime	Year	Recommendations	Suggestions	Better Practice Suggestions or Comments
Stored Communications	2022-23	1	26	16
	2021-22	2	21	19
Telecommunications Data	2022-23	6	69	51
	2021-22	11	124	78
Industry Assistance	2022-23	0	6	10
	2021 - 22	0	12	12
International Production Orders	2022-23	-	-	-
	2021-22	0	0	1

We make recommendations, suggestions, comments and better practice suggestions to ask agencies to remedy non-compliances or risks identified through an inspection. Our recommendations address serious or systemic problems with an agency's compliance with the legislation. We make suggestions where we identify less serious problems, administrative issues or practices which we believe create a risk of serious non-compliance. A comment or better practice suggestion is offered where we identify opportunities for improvement or where an agency has already acted to address our concerns. From August 2023, we discontinued the use of better practice suggestions to be consistent in reporting across our Office.

This is the first year our Office inspected agencies' preparation to use international production orders (IPO) under Schedule 1 of the TIA Act. As agencies have not yet used these powers, we conducted health check inspections to assess the operational readiness of an agency to access and administer an IPO. This included inspecting the Australian Designated Authority (ADA), which is part of the Attorney-General's Department, who remain responsible for ensuring IPOs comply with the relevant designated international agreement.

Key Findings

Our findings vary in their impact and level of risk. For this reason, we do not consider changes in the number of recommendations, suggestions and better practice suggestions or comments alone to be an accurate reflection of each agency's level of compliance.

For most agencies, we observed a decrease in concerning behaviours or practices that led to the reduction in the number of recommendations, suggestions and better practice suggestions or comments we made. Despite this, our inspections revealed several common issues across all regimes that we consider pose the greatest risk to an agency's compliance with the TIA Act and Telecommunications Act. These include:

- inadequate, insufficient or inconsistent guidance material provided to staff on the legislative requirements or their obligations
- lack of robust record-keeping practices or inability to demonstrate considerations when making authorisations or decisions
- insufficient training or support for staff in agencies with a high usage of powers, contributing to inadequate compliance with the legislative requirements or inappropriate use of the powers
- compliance staff turnover leading to inconsistency in quality assurance practices and implementation of remedial actions to address our previous findings
- limitations in case management systems to restrict access to data or information obtained using the powers contributing to the risk of inappropriate use or disclosure, and
- despite some agencies having good frameworks, continuing instances of staff not adhering to these frameworks or demonstrating a lax approach to use of the powers and complying with the legislative requirements.

Themes identified by regime

Stored Communications	Telecommunications Data
• stored communications not being destroyed as required by law • victim's stored communications were accessed despite no record demonstrating that consent was unable to be obtained • insufficient record-keeping on the use or communication of stored communications.	• authorisations made for purposes not permitted within the TIA Act • authorised officers not sufficiently demonstrating considerations • insufficient privacy consideration when changing 'ping frequency' • data obtained outside the parameters of an authorisation • data accessed where offence thresholds were not met • inadequate record-keeping on the use or disclosure of data • limited controls to ensure officers consider Journalist Information Warrant (JIW) requirements • discrepancies in Ministerial reporting.
International Production Orders	**Industry Assistance**
• varied levels of readiness to use an order • minimal training had been delivered for staff, including for applicants and authorising officers • solutions for handling information obtained from an order were not tested and finalised.	• inconsistencies between the authorisation or warrant and the enabling industry assessment instrument • insufficient demonstration of the linkage between the assistance sought with the relevant object or an associated authorising process.

Agencies where we identified the most non-compliance issues were generally larger agencies who use the powers more frequently, with higher numbers of requesting and authorised officers (usually geographically dispersed). We observed that these agencies experienced regular staff turnover and that officer awareness of the relevant legislative obligations was harder to maintain. In such situations, agencies need to provide regular targeted training and comprehensive guidance documentation to support officers to comply with the legislation. Failure to do so leads to more non-compliance.

All agencies were receptive to our findings. In some instances, agencies took immediate remedial actions during our inspection to address identified issues. We were encouraged that many agencies proactively identified and disclosed compliance issues prior to, or at the beginning of, our inspections.

Although we were satisfied most agencies undertook remedial action to our previous findings, there were several agencies where issues recurred. While some of the difficulty in implementing a timely response to our findings may be attributed to the retrospective nature of our inspections, there were a small number of instances where we were not satisfied with the remedial action taken by agencies. We made further recommendations or suggestions aimed at improving processes to prevent recurrence of the issues.

Our Office encourages agencies to consider feedback we provide and implement measures to address identified issues in a timely manner, which can prevent repeated findings over sequential inspections. It is also open to agencies to seek early views and compliance feedback from our Office outside our standard inspection schedule as they implement mechanisms to improve compliance.

Oversight of Covert Electronic Surveillance

Introduction

The TIA Act and the Telecommunications Act provide law enforcement with a range of covert electronic surveillance powers. These include access to a person's stored communications and telecommunications data. The powers also allow agencies to direct the activities of communications providers to assist them in performing a function or exercising a power to obtain information relevant to an investigation. These powers are found in Chapter 3 (Stored Communications), Chapter 4 (Telecommunications Data) and Schedule 1 (International Production Orders) of the TIA Act and Part 15 (Industry Assistance) of the Telecommunications Act.

Agencies that use powers under the TIA Act and the Telecommunications Act must comply with reporting requirements and are overseen by the Commonwealth Ombudsman (our Office). Our oversight role helps ensure that agencies exercise these powers in accordance with the law and are accountable for instances of non-compliance. Our Office's reporting obligations provide transparency and a level of assurance to the Attorney-General, the parliament and the public about the use of these powers.

This annual report provides a summary of the most significant findings regarding agencies' compliance with the TIA Act and the Telecommunications Act from inspections conducted in the 2022-2023 financial year. We also report on matters that do not relate to specific instances of non-compliance, such as the adequacy of an agency's policies and procedures to demonstrate compliance with the legislation.

How we oversee agencies

We assess compliance based on a sample of records, discussions with relevant agency teams, reviews of agencies' processes, and observations of agencies' remedial action to issues we identified previously.

We apply a set of inspection methodologies consistently across agencies. These methodologies are based on the requirements of the legislation and better practice standards. We update our methodologies in response to legislative amendments and changes to agency processes.

In warrant-based regimes, such as stored communications and IPO, we do not assess the

merits of a decision by an issuing authority to issue a warrant or order. However, we do review agencies' applications for warrants or orders and accompanying affidavits to assess whether agency processes comply with legislative requirements. This includes whether the agency provided the issuing authority with sufficient and accurate information to make the required considerations when deciding whether to issue a warrant or order.

For internally authorised regimes, such as telecommunications data and industry assistance, our Office does not review the merits of an authorised officer's decision to access data or seek assistance. We assess whether an authorised officer satisfies the requirements of the legislation, which involves assessing whether there is sufficient information for officers to authorise the disclosure or seek the assistance, and whether the requisite considerations were made.

We provide our inspection criteria to agencies before each inspection. This helps agency staff identify the most accurate sources of information to assist our inspection. We encourage agencies to proactively disclose any non-compliance, including remedial action they have already taken. Our Office also seeks to support compliance by assessing agencies' policies, procedures and training, communicating better practices, and facilitating communication across agencies that use the same powers.

For agencies granted new access to powers, we may conduct a 'health check' inspection aimed at assessing the readiness or 'health' of an agency's compliance framework. We focus on determining whether the frameworks, policies and procedures an agency has developed, or is in the process of developing, are suitable for supporting compliance with the legislation.

Risk-Based Oversight

During the 2022-2023 inspection period, we piloted a risk-based approach to our inspections of Chapter 4 (Telecommunications Data) of the TIA, referred to as Risk-Based Oversight (RBO). We did this concurrently with our existing methodology of reviewing records.

RBO directs our efforts towards areas of non-compliance by agencies that pose the greatest risk of harm to the public. It aims to deliver a tailored response to each agency in a way that is proportionate to the level of assessed risk. Our pilot assessed the effectiveness of RBO in providing a more meaningful level of assurance about how agencies use covert and intrusive powers, ahead of a broader roll out of RBO in 2023-2024 to the other covert and intrusive powers our Office oversees.

The pilot focused on improving our understanding of two key risks:

- inappropriately using or disclosing telecommunications data, and
- having insufficient controls to ensure officers considered the requirements for a

Journalist Information Warrant before authorising access to telecommunications data.

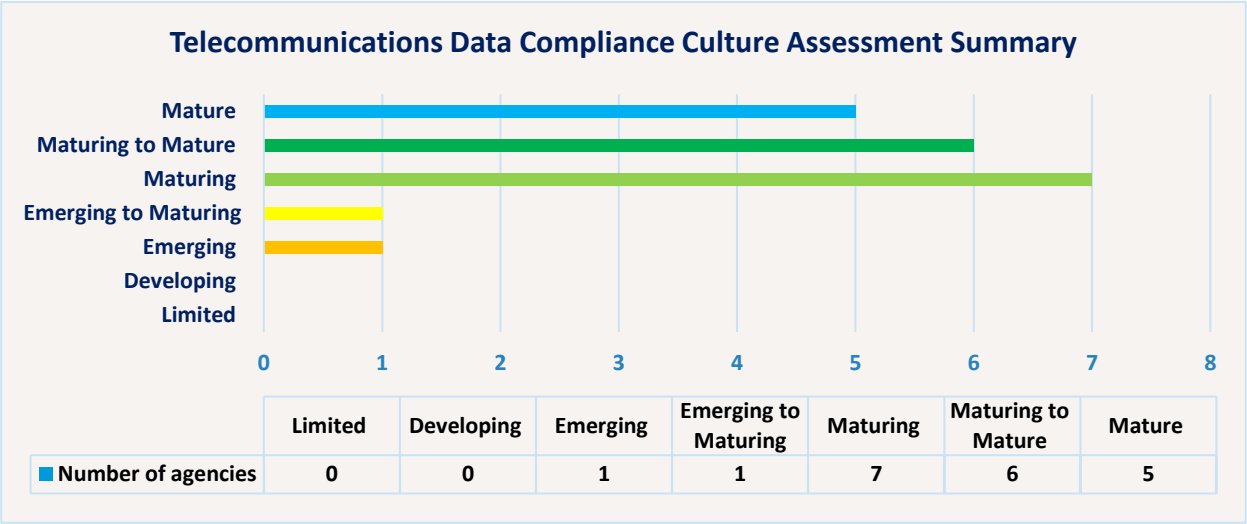
The pilot used an investigative approach in assessing agency records and drivers of risk. This included building our understanding of an agency's governance, practices, training and procedures, along with their compliance culture in using and administering the powers. The findings from the risks we assessed have been included in the Telecommunications Data section of this report.

Through the risk-based pilot we uncovered more meaningful insights that we would have not otherwise identified using our previous record-based approach. Accordingly, we will roll out RBO to the other covert and intrusive powers our Office oversees over the next reporting period.

Culture of Compliance

A mature compliance culture can help mitigate the risk of an agency not complying with the legislation. As part of the RBO pilot, we assessed agencies' culture of compliance with respect to using telecommunications data powers. This included reviewing an agency's maturity in managing their compliance, transparency in disclosing issues, continual learning, and responsiveness to our oversight. Agencies were assigned a rating of limited, developing, emerging, maturing or mature against each of the indicators for a compliance culture.

Figure 1: Summary of compliance culture assessments for agencies using Telecommunications Data powers under Chapter 4 of the TIA Act



	Limited	Developing	Emerging	Emerging to Maturing	Maturing	Maturing to Mature	Mature
Number of agencies	0	0	1	1	7	6	5

Agencies that possess a mature compliance culture had independent quality assurance and data vetting practices to help self-identify and manage compliance issues. These agencies

typically had an established centrally coordinated online request and authorisation system which encouraged compliance by streamlining processes, increasing consistency, and improving record-keeping.

We observed several good practices at agencies which indicated they had a maturing compliance culture. Such practices included disclosing instances of non-compliance to our Office, strong procedures to support the use of telecommunications data powers, continual improvement to compliance practices and appropriate and timely remedial action taken in response to our findings.

Case study

Improving Compliance Culture

South Australia Police (SA Police) received 2 consecutive formal reports from our Office regarding serious or repeat issues of non-compliance in the use of telecommunications data powers. In response to our concerns, we made 5 recommendations, 26 suggestions and 3 better practice suggestions in 2020-2021, followed by 3 recommendations, 14 suggestions and 3 better practice suggestions during the subsequent 2021-2022 inspection.

On this year's inspection we were encouraged by the progress made by SA Police to address our previous findings. We found SA Police had made concerted efforts to improve compliance in their use of the powers. In addition to resolving all previous recommendations and suggestions, SA Police implemented a digital platform to manage telecommunications data requests and authorisations, introduced robust data-vetting processes, drafted a related training package, and updated their templates.

Following this year's inspection, SA Police continued to approach our Office for advice in relation to our findings, and other matters self-identified by the agency. SA Police's commitment to continuous improvement is an indicator of a mature compliance culture.

Stored Communications

A stored communication is a communication that is held on equipment that is operated by and is in the possession of the carrier and cannot be accessed by a person who is not a party to the communication. Examples of stored communications include:

- SMS
- MMS
- Voicemails
- Emails.

To access stored communications, an agency must apply to an external issuing authority (such as a Judge or eligible AAT member) for a stored communications warrant. A stored communications warrant authorises an agency to access stored communications held by a carrier that were made or intended to be received by the person in respect of whom the warrant was issued, subject to any conditions or restrictions specified on the warrant.

Before a warrant is issued, an agency may authorise the preservation of a stored communication. This ensures the relevant carrier retains the communication until it can be accessed under a warrant. There are 3 types of preservation notices:

- historic domestic preservation notices
- ongoing domestic preservation notices, and
- foreign preservation notices (only available to the AFP).

An agency must meet certain conditions under the TIA Act before it can give a preservation notice to a carrier.

Under s 186B(1)(b) of the TIA Act, the Ombudsman must inspect records of a criminal law enforcement agency to determine the extent of compliance by that agency with Chapter 3 when using the stored communications powers. Section s 186J(1) requires the Ombudsman to report to the Attorney-General as soon as practicable after 30 June each year on inspections conducted of agencies' use of both Chapter 3 (Stored Communications) and Chapter 4 (Telecommunications Data) of the TIA Act.

Our Inspections

Our Office inspected 17 agencies' access to stored communications under Chapter 3 of the TIA Act for records covering the period 1 July 2021 to 30 June 2022. We made:

- 1 recommendation

- 26 suggestions, and
- 16 better practice suggestions and comments.

The table below sets out the number of recommendations, suggestions, better practice suggestions or comments made by our Office to each agency during this period compared to the previous year.

Table 2: Number of findings made per agency during the 2022-23 inspection period (Figures from the 2021-22 inspection period are included in brackets)

Agency	Recommendations	Suggestions	Better Practice Suggestions or Comments	Total
ACCC	0 (0)	0 (1)	0 (1)	0 (2)
ACIC[1]	- (0)	- (1)	- (1)	- (2)
ACLEI	0 (0)	0 (1)	0 (0)	0 (1)
AFP	0 (2)	1 (4)	0 (3)	1 (9)
CCC (QLD)	0 (0)	0 (1)	2 (0)	2 (1)
CCC (WA)	0 (-)	0 (-)	1 (-)	1 (-)
DHA[2]	-(0)	- (4)	- (4)	- (8)
IBAC	0(0)	2 (0)	2 (0)	4 (0)
ICAC (NSW)	0 (0)	0 (0)	4 (2)	4 (2)
ICAC (SA)	0 (0)	0 (0)	0 (1)	0 (1)
LECC	0 (0)	6 (1)	1 (0)	7 (1)
NSW CC	0 (0)	0 (2)	0 (2)	0 (4)
NSW Police	0 (0)	2 (0)	0 (0)	2 (0)
NT Police	1 (0)	8 (4)	1 (0)	10 (4)
QLD Police	0 (0)	0 (1)	0 (1)	0 (2)
SA Police	0 (0)	1 (0)	2 (0)	3 (0)
TAS Police	0 (0)	4 (0)	1 (0)	5 (0)
VIC Police	0 (0)	0 (1)	1 (1)	1 (2)
WA Police	0 (0)	2 (0)	1 (3)	3 (3)
TOTAL:	**1 (2)**	**26 (21)**	**16 (19)**	**43 (42)**

1 No inspection conducted in 2022–23 as the ACIC did not use the powers under Chapter 3 of the Act during the relevant records period.
2 No inspection conducted in 2022–23 as the DHA did not use the powers under Chapter 3 of the Act during the relevant records period.

Table 3: Use of stored communications powers and records inspected in the 2022-2023 financial year

Agency	Total Historic PN[3]	Historic PN inspected	Total Ongoing PN	Ongoing PN inspected	Stored Comms Warrants[4]	Warrants inspected	Destructions	Destructions inspected
ACCC	1	1	-	-	1	1	3	3
ACIC[5]	-	-	-	-	-	-	-	-
ACLEI	1	1	1	1	-	-	-	-
AFP	158[6]	22	73	15	35	24	44	44
ASIC[7]	-	-	-	-	-	-	-	-
CCC (QLD)	-	-	15	15	-	-	15	15
CCC (WA)	-	-	5	5	-	-	-	-
DHA[8]	-	-	-	-	-	-	-	-
IBAC	1	1	9	7	8	8	2	2
ICAC (NSW)	-	-	-	-	-	-	4	4
ICAC (SA)	1	1	1	1	-	-	-	-
LECC	-	-	1	1	-	-	51	51
NSW CC	1	1	-	-	1	1	-	-
NSW Police	374	20	225	10	406	25	372	5
NT Police	27	-	39	27	4	4	0	2[9]
QLD Police	-	-	-	-	98	42	130	25
SA Police	69	34	1	1	17	16	16	16
TAS Police	41	7	17	12	29	19	51	28
VIC Police	94	16	71	14	128	30	70	33
WA Police	97	11	57	6	82	20	18	18
TOTAL	**865**	**115**	**515**	**115**	**809**	**190**	**776**	**246**

[3] This is the total of Preservation Notices (PN) reported to our Office. In some instances, this did not reflect the actual number of preservation notices given by the agency during the financial year 2022-23. This is because a preservation notice may still be in force during our inspection and will be subject to compliance assessment on expiration in our next records period, or because an agency has incorrectly reported on the number of preservation notices to our Office.

[4] This is the total of warrants reported to our Office. In some instances, this did not reflect the actual number of warrants issued to the agency during the financial year 2021–22. This occurs where a warrant may still be in force during our inspection and will be subject to a compliance assessment on expiration in our next records period, or because an agency has incorrectly reported on the number of warrants to our Office.

[5] ACIC reported nil use of the powers for the 2022-2023 inspection period/financial year.

[6] AFP's total historic PN and historic PNs include 1 Foreign Preservation Notice in each category.

[7] ASIC reported nil use of the powers for the 2022-2023 inspection period/financial year.

[8] DHA reported nil use of the powers for the 2022-2023 inspection period/financial year.

[9] Both destructions reviewed related to records within the period, but were destroyed after 30 June 2022.

Compliance Issues and Risks

Our inspections revealed several key areas that we consider pose the greatest risk to an agency's compliance with the Act. These include:

- destruction of stored communications
- applying for stored communications warrants in relation to a victim of a serious contravention, and
- record-keeping requirements regarding the use of stored communications.

Destruction of Stored Communications

Section 150(1) of the TIA Act requires that where the chief officer is satisfied that information or a record obtained by accessing a stored communication is not likely to be required for a permitted purpose, the information or record must be destroyed 'forthwith'. This includes destruction of originals and copies of stored communications, as well as ensuring appropriate written approval is obtained from the chief officer prior to the destruction. Failure to destroy stored communications once they are no longer required for a permitted purpose results is an unreasonable infringement on privacy and may create a risk the information will be used when it should have been destroyed.

The TIA Act does not expressly require periodic reviews of stored communications to consider whether any information or records should be destroyed under s 150(1). However, due to the privacy intrusion associated with continued retention of stored communications information, an agency should periodically review whether such information or records are required for a permitted purpose.

We consider the destruction of stored communications to be complete when all steps in a destruction process are finalised. This includes confirmation of destruction by the agency of all information or records that were obtained by accessing stored communications (including any copies and computer records as per the definition of a record in s 5(1) of the TIA Act).

Achieving compliance with destruction requirements requires agencies to:

1. have a strong framework in place to track all relevant stored communications
2. seek appropriate approval for destruction from the chief officer or their delegate, and
3. ensure destruction of relevant records and information (including copies) occurs 'forthwith'.

Agencies can help ensure they meet the 'forthwith' requirement by having established processes to identify and locate relevant stored communications information and records prior to seeking chief officer approval. Robust record-keeping and document tracking processes reduce delays in accounting for records after the chief officer certifies records for destruction. It is also important that agencies have clear guidance available to staff regarding the destruction requirements to achieve compliance with s 150(1) of the Act.

We made 8 suggestions and 7 better practice suggestions across 5 agencies[10] regarding destruction of stored communications. This included:

- ensuring destruction reports are provided to the Minister, in accordance with the requirements under s 150(2) of the TIA Act
- ensuring sufficient records are kept demonstrating whether stored communications were destroyed in accordance with s 150 of the TIA Act, and
- finalising and updating destruction policies and procedures to ensure the agency can comply with legislative requirements.

[10] AFP, IBAC, NSW ICAC, LECC, NT Police and SA Police

Case study

Destructions not occurring 'forthwith'

During our inspection of the Law Enforcement Conduct Commission's (LECC) records, we found several instances where stored communications were authorised for destruction, but destruction had not occurred *forthwith*, with some destructions occurring up to a year later. In addition to being an unreasonable intrusion into privacy, failure to destroy the material in line with the Act creates a risk the information may subsequently be unlawfully used or communicated. We made a better practice suggestion that the LECC implement an internal 'forthwith' timeframe of no more than 28 days following authorisation to meet the 'forthwith' requirement.

In assessing compliance, we are guided by an agency's internal timeframes but will also consider whether this timeframe is a reasonable period in the circumstances, noting the ordinary definition of 'forthwith' as 'immediate and without delay'. Where an agency does not have a timeframe, our Office makes an assessment based on our understanding of an agency's policies and procedures and what we consider to be reasonable in the circumstances.

We would consider a timeframe of two weeks to be reasonable, however, we have accepted a timeframe of up to 28 days at some agencies.

The LECC accepted this finding and gave an undertaking to address it prior to the next inspection.

Applying for stored communications warrants in relation to a victim of a serious contravention

An issuing authority must be satisfied of certain requirements before issuing a stored communications warrant. These considerations are listed in section 116(1) of the TIA Act.

Subject to meeting all other requirements, an issuing authority may grant a stored communications warrant in relation to a victim of a serious contravention if they are satisfied that the person is 'unable' to consent, or it is 'impracticable' for the person to consent to those stored communications being accessed.

Where agencies seek a stored communications warrant in relation to a victim of a serious contravention, they should ensure the accompanying affidavit demonstrates either the victim is

'unable' to provide consent, or that obtaining consent is 'impracticable'. This includes documenting any steps taken to obtain a victim's consent and why such actions were unsuccessful. This will enable the issuing authority to make an informed decision about whether to issue a stored communications warrant in the circumstance.

We made 5 suggestions across 4 agencies[11] relating to stored communications warrants of a victim of a serious contravention. This included:

- demonstrating how the threshold of 'unable' or 'impracticable' to provide consent was met when applying for a stored communications warrant in relation to a victim
- improving guidance materials and raising staff awareness on circumstances where the thresholds of a victim being unable to consent, or where it is impracticable for the victim to consent, could be met, and
- clarifying the implications of obtaining stored communications warrants where the victim has consented to their stored communications being accessed.

In previous inspection cycles we have made findings in relation to improving guidance materials at both AFP and NT Police. While we are satisfied that the AFP has fully addressed previous findings in relation to this issue, we were not satisfied with NT Police's progress against our previous findings. We reiterated our previous suggestion for NT Police to update its policy and templates to fix this issue.

[11] AFP, NT Police, Tasmania Police, WA Police

Case study

Seeking stored communications warrants where the victim refused to consent to stored communications being accessed

Western Australia Police (WA Police) obtained a warrant to access records belonging to a victim of crime, on the basis that the victim refused to provide consent to obtain these records. The application for the warrant did not provide sufficient details of why the victim was 'unable' to consent or what led investigators to the view that obtaining consent was 'impracticable'.

We would consider that a person would be 'unable to consent' where, for example, they are missing and cannot be located, or are incapacitated or deceased. Obtaining consent would be 'impracticable' where a person's situation makes contacting them extremely difficult or put at serious risk the impartiality of an investigation.

If a victim has an opportunity to consent and they do not wish their stored communications to be accessed, we are of the view that an agency should not use a stored communications warrant. The victims' reasons for not providing consent are immaterial.

We suggested that WA Police obtain legal advice before using stored communications obtained under the warrant. We also suggested that WA Police update their guidance material to fully reflect the s 116(1)(da) considerations and outline the thresholds of 'unable' or 'impracticable' to obtain consent, including in circumstances where the victim does not consent to police accessing their stored communications.

These suggestions were accepted by the WA Police.

Obligation to keep records

Agencies are required under s 151(1) of the TIA Act to keep certain records for the period specified in s 151(3). These records include, but are not limited to: preservation notices, revocation of preservation notices, stored communications warrants, revocation of stored communications warrants, use and communication compliance records, destruction records and reports to the Minister (currently the Attorney-General).

An agency should maintain consistent record-keeping processes to ensure it meets its obligations under s 151 of the TIA Act. Record-keeping ensures there is transparency on the use of these covert and intrusive powers and facilitates our oversight.

We made one recommendation, 5 suggestions and one better practice suggestion across 3 agencies[12] relating to record-keeping. This included:

- creating mechanisms that track and record use and communication of stored communications
- strengthening guidance to staff on recording use and communication
- reviewing methodologies for calculating the number of preservation notices in annual reports to the Minister, and
- ensuring staff follow processes to capture information on the giving of preservation notices.

[12] NSW Police, NT Police, WA Police

Case study

Failure to record use or communication of stored communications

Section 133 of the TIA Act provides exemptions to the general prohibition on using, communicating or recording stored communications information. The creation of records under s 151(3) allows an agency to demonstrate any use or communication was compliant with the s 133 exemptions.

We were unable to locate any use or communication logs on file for stored communication warrants obtained by the Northern Territory Police (NT Police). Additionally, NT Police policies and training did not provide guidance on the requirement to record use or communication of stored communications information.

The absence of clear guidance about recording when lawfully accessed information was communicated, used or recorded creates a risk that the agency may not be able to demonstrate compliance with s 133 of the TIA Act.

It also makes it difficult to later track and destroy any originals or copies of stored communications information.

We recommended that NT Police create and maintain use and communication logs for each stored communication warrant and record all use and communication of information received under that warrant. We also suggested that NT Police ensure its policies reflect the legislative requirements under s 151(3) of the Act, and that investigators are reminded of the requirement to maintain a use and communication log.

The NT Police provided no response to this recommendation.

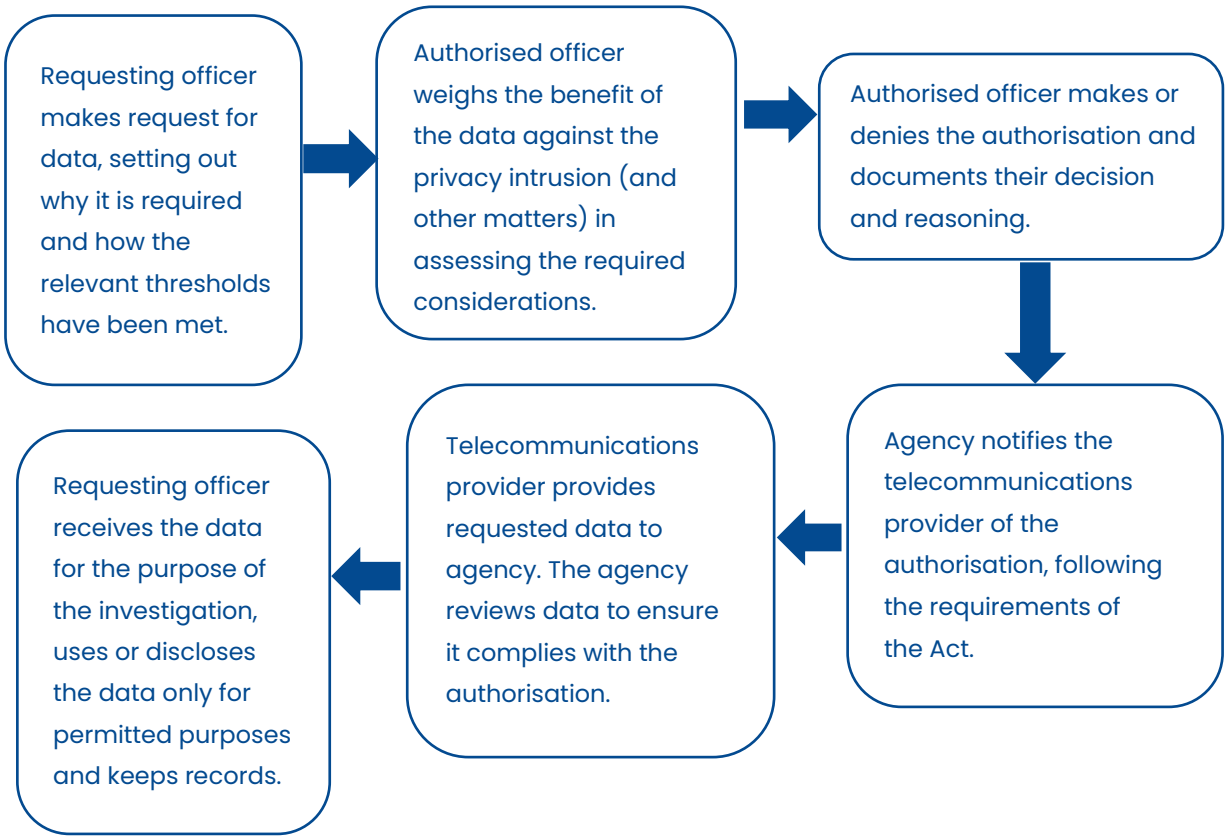
Telecommunications Data

Telecommunications data is information about a communication but does not include the content or substance of that communication. Telecommunications data includes, but is not limited to:

- subscriber information (for example, the name, date of birth and address of the person to whom a service is subscribed)
- date, time, and duration of a communication
- phone number or email address of the sender and recipient of a communication
- Internet Protocol (IP) address used for a session
- start and finish time of each IP session
- amount of data uploaded/downloaded, and
- location of a device from which a communication was made (this may be at a single point in time, or at regular intervals over a period).

Agencies are empowered to internally authorise access to data without applying to a judge or AAT member. To authorise disclosure of data, among other considerations, an authorised officer within an agency must weigh the likely relevance and usefulness of the disclosed telecommunications data to the investigation against the privacy intrusion it causes. Only officers authorised by the chief officer of the agency can authorise disclosure of telecommunications data.

Figure 2: Typical agency authorisation process for disclosure of telecommunications data (excluding journalist information warrants)



Under s 186B(1)(a) of the TIA Act, the Ombudsman must inspect the records of a criminal law enforcement agency to determine the extent of compliance with Chapter 4 by the agency and its officers.

Our office does not have jurisdiction over the activities of telecommunication service carriers, who hold the telecommunications data that agencies seek access to (for example: Telstra, Optus, etc.). Pursuant to s 309 of the Telecommunications Act, the Information Commissioner has the power to monitor compliance with Part 13, Division 5 of the Act, which requires carriers to record certain disclosures of personal information, including disclosures of telecommunications data collected and retained under the data retention scheme, to law enforcement agencies. The Information Commissioner also has the power to monitor the extent of these entities' compliance with their obligations under the *Privacy Act 1988* (Cth).

Our Inspections

Our Office inspected 21 agencies' access to telecommunications data under Chapter 4 for records covering the period from 1 July 2021 to 30 June 2022. We made:

- 6 recommendations across 2 agencies

- 69 suggestions, and
- 51 better practice suggestions and comments

Most of the agencies inspected made significant progress against our previous findings, which reduced the levels of non-compliance and repeat findings in the current period. There were several encouraging findings with some agencies demonstrating high levels of compliance with the TIA Act and a mature culture of compliance in use of the powers. Despite these improvements, we also observed that some agencies had not demonstrated sufficient progress in addressing previous issues identified, resulting in further recommendations and suggestions from our Office.

The table below sets out the number of recommendations, suggestions, better practice suggestions and comments made by our Office to each agency during this period compared to the previous reporting period.

Table 4: Number of findings made per agency during the 2022–23 inspection period (Figures from the 2021–22 inspection period are included in brackets)

Agency	Recommendations	Suggestions	Better Practice Suggestions / Comments	Total
ACCC	0 (0)	3 (3)	2 (3)	5 (6)
ACIC	0 (0)	3 (6)	0 (11)	3 (17)
ACLEI	0 (0)	5 (6)	5 (4)	10 (10)
AFP	0 (2)	3 (11)	6 (6)	9 (19)
ASIC	0 (0)	0 (0)	0 (0)	0 (0)
CCC (QLD)	0 (0)	5 (10)	3 (2)	8 (12)
CSNSW[13]	0	0	1	1
CCC (WA)	0 (0)	1 (0)	0 (3)	1 (3)
DHA	0 (0)	1 (6)	5 (9)	6 (15)
IBAC	0(0)	4 (5)	1 (0)	5 (5)
ICAC (NSW)	0 (0)	0 (1)	2 (1)	2 (2)
ICAC (SA)	0 (0)	1 (7)	2 (4)	3 (11)
LECC	0 (0)	5 (3)	4 (3)	9 (6)
NSW CC	0 (0)	0 (4)	2 (3)	2 (7)
NSW Police	0 (0)	5 (7)	0 (9)	5 (16)

[13] In 2021/22 inspection period a full compliance inspection was not undertaken

NT Police	1 (2)	6 (11)	3 (1)	10 (14)
QLD Police	0 (0)	6 (4)	5 (2)	11 (6)
SA Police	0 (3)	3 (14)	1 (3)	4 (20)
TAS Police	0 (0)	4 (5)	4 (0)	8 (5)
VIC Police	5 (4)	6 (7)	0 (5)	11 (16)
WA Police	0 (0)	8 (14)	5 (9)	13 (23)
TOTAL:	**6 (11)**	**69 (124)**	**51 (78)**	**126(213)**

Table 5: Use of telecommunications data powers and records inspected in the 2022–23 period[14]

Agency	Total Historic	Historic Inspected	Total Prospective	Prospective inspected
ACCC	38	24	3	3
ACIC	4,686	32	1,222	35
ACLEI	265	17	75	16
AFP	14,931	45	5,293	30
ASIC	506	14	74	11
CCC (QLD)	592	23	203	10
CCC (WA)	52	25	49	29
DHA	3,453	57	318	32
IBAC	345	25	158	12
ICAC (NSW)	201	34	4	4
ICAC (SA)	79	30	5	5
LECC	517	23	107	14
NSW CC	3,008	30	926	17
NSW Police	109,255	38	1,984	25
NT Police	2,228	19	439	17
QLD Police	26,302	60	4,131	20
SA Police	4,550	19	324	15
TAS Police	2,893	24	117	13
VIC Police	108,571	35	16,366	38
WA Police	27,407	61	3,810	26

[14] The record numbers listed in 'Total Historic' is the number of historic records reported to our Office by the agency pre-inspection, from which we drew our inspection sample. In some inspections, we made findings where the number of historic authorisations reported to our Office did not reflect the actual number of authorisations made by the agency. While the reasons for these differences varied between agencies, we suggested the impacted agency review and appropriately amend their reporting of the number of historic authorisations.

Agency	Total Historic	Historic Inspected	Total Prospective	Prospective inspected
Total	**309,879**	**635**	**35,608**	**372**

Table 6: Authorisations issued for telecommunications data on behalf of foreign countries

Agency	Foreign Historic	Foreign Historic Inspected	Foreign Prospective	Foreign Prospective Inspected
AFP	46	3	1	0

There were no JIWs issued in the 2021-22 records period.

Compliance Issues and Risks

Our inspections revealed several key areas that we consider pose the greatest risk to an agency's compliance with the TIA Act. These included:

- authorising access to data for purposes not provided for in the TIA Act
- authorising officers providing insufficient information to demonstrate their considerations, including changes to the frequency with which location information is collected
- the handling of data received from carriers that was outside the parameters of an authorisation
- authorising access to data where the relevant offence thresholds were not met
- inconsistent or inadequate record-keeping about use and disclosure of data
- inconsistent or inadequate agency controls to ensure officers consider whether a JIW may need to be sought, and
- discrepancies in agencies' annual reporting on the use of telecommunications data powers to the Minister (the Attorney-General).

Authorising access to data for purposes not provided for in the TIA Act

Sections 178(2), 178A(2), 179(2) and 180(2) of the TIA Act identify the purposes for which an authorised officer may access telecommunications data. This includes for purposes of enforcing the criminal law, finding a missing person or enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue. Our Office examines whether the records kept by agencies demonstrate the authorisation was properly made, including:

- the specified information or documents to be accessed
- the carrier(s)/carriage service provider(s) from whom the information is sought
- the authorised officer's satisfaction that the authorisation was reasonably necessary for a relevant purpose provided for under Chapter 4 of the Act, including meeting the relevant offence threshold
- sufficient information was provided for the authorised officer to appropriately consider the privacy requirements under s 180F of the Act, and
- the authorisation does not give rise to any potential disclosure that would require a JIW to be in force.

In the case of authorising access to prospective data, under s 180(4) of the Act, an authorised officer must not make the authorisation unless satisfied that the disclosure is reasonably necessary for the investigation of a serious offence (as defined by s 5D of the Act) or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

We found instances of agencies making authorisations for:

- purposes not provided for under the Act
- access to information that was not telecommunications data, and
- access to information from organisations that are not telecommunications providers.

We also found one agency made prospective authorisations for offences that did not meet the threshold[15]. As a result, we made one recommendation, 5 suggestions and one better practice suggestion across 3 agencies[16] in relation to these non-compliant authorisations.

Case study

Authorisations made for purposes not provided for in the Act or not meeting legislative thresholds

Authorisations to access data for purposes not provided for in the TIA Act was most prolific in Victoria Police (VIC Police). This included authorisations for prospective data that did not meet the threshold.

We identified a high number of authorisations that did not demonstrate that the access to data was for enforcing the criminal law or locating a missing person. We also identified a significant number of authorisations where the alleged offences referenced incorrect legislation. These are repeat findings for VIC Police that we have made over several inspection periods.

The incorrect use of authorisation provisions risks the legality of the data accessed by VIC Police and the accuracy of their ministerial reporting. Furthermore, data may be disclosed by a carrier in response to the authorisation, resulting in unauthorised data being provided to VIC Police.

We again recommended VIC Police ensure that all authorisations and disclosures under Chapter 4 of the TIA Act are made for the purposes expressly listed in the Act, and for current and correct offence provisions. We also suggested VIC Police implement systems level controls and additional compliance measures to ensure authorisations can only be made for purposes provided for in the Act.

VIC Police acknowledged this finding and advised system controls have been developed and are being progressively implemented, to ensure only authorisations that meet the relevant legislative threshold can be made. With respect to authorisations to prospective data, VIC Police advised that a full review of the erroneous records had commenced, and remedial action would be taken.

Given this is a repeat finding, our Office will review the effectiveness of these measures by VIC Police and conduct a deep dive into any underlying contributors to repeated non-compliance in the next reporting period.

[15] VIC Police

[16] QPS, Victoria Police and NT Police.

Authorised officer demonstrating their considerations when making an authorisation

Records in which authorising officers demonstrate their considerations when making an authorisation are a key safeguard in the legislation. This includes authorising officers demonstrating they have:

- weighed the proportionality of the intrusion into privacy against the gravity of the conduct, the value of the information sought and its likely assistance to the enforcement of the criminal law, locating a missing person, or enforcement of a law imposing a pecuniary penalty or for protection of public revenue
- ensured the request is not seeking disclosure of the contents or substance of a communication
- considered whether a purpose of the data disclosure is to identify a journalist's source and, if so, whether a JIW is in force or should be sought, and
- satisfied the authorisation is for a purpose permitted under Chapter 4 and, where applicable, that the relevant offence thresholds are met.

Section 186A(1)(a)(i) of the TIA Act requires that records are kept for each authorisation that show whether the authorisation was properly made. In addition to providing the grounds for authorising access to the data, we also rely on these records demonstrating the authorised officer's considerations to support our oversight role.

Without sufficient background information in the request, template wording without further consideration in an authorisation is not sufficient to demonstrate the authorised officer has turned their mind to the required considerations. While we understand that authorised officers may be aware of background information relating to a particular investigation, we rely on agency record-keeping practices, including the contemporaneous records made by authorising officers, to be satisfied that the relevant considerations took place.

We made one recommendation, 18 suggestions, 13 better practice suggestions and comments across 14 agencies[17]. These included:

- increasing the awareness among requesting and authorised officers of the key

[17] QCCC, ACLEI, QPS, WA CCC, ACCC, VIC Police, WA Police, LECC, NSW CC, IBAC, SA Police, NSWPF, NT Police and Tasmania Police

considerations and record-keeping requirements of the TIA Act

- demonstrating authorisation of ping frequency changes
- implementing measures to ensure requesting and authorised officers consistently document any information to demonstrate that all relevant matters and safeguards were considered before making an authorisation
- ensuring authorised officers demonstrate they accessed and considered relevant information to conscientiously acquit their role as decision-makers, and
- establishing quality assurance measures to assess requests made for the disclosure of telecommunications data to ensure each request contains sufficient information for an authorised officer to demonstrate they have made the considerations required under Chapter 4 of the Act.

Case study

Improving considerations made by Authorised Officers

The Western Australian Corruption and Crime Commission (CCC (WA)) disclosed instances to our Office where authorised officers did not demonstrate consideration of the requirements under Chapter 4 of the TIA Act prior to renewing an authorisation. This included not providing sufficient justification of the further or continuing privacy intrusion for renewal applications, and not recording how the disclosure from the proceeding authorisation was relevant and useful.

Recording considerations when making an authorisation is a key safeguard to ensure the authorising officer has turned their mind to the appropriate privacy, offence and investigative considerations under s180F of the TIA Act.

We suggested CCC (WA) implement policies, procedures and/or controls to ensure applications to renew an authorisation justify the ongoing privacy intrusion, demonstrate the usefulness of data already obtained, and the relevance of continuing to seek the data.

In response, CCC (WA) advised they implemented measures to ensure continued compliance with the TIA Act with renewing applications. This includes recording in applications for renewals how the data would be relevant and useful to the investigation. The CCC (WA) also amended their training module to require recording these considerations.

Considering privacy impacts when varying ping frequency after an authorisation

We made findings across several agencies relating to authorised officers not recording sufficient considerations when changing a ping frequency after the initial authorisation.

An authorisation for Location Based Services (LBS) (or a 'ping') allows police to request that a carrier plot the approximate location of a mobile device at a given interval. An active mobile phone will automatically contact a tower at certain intervals and the requested information is collected by the carrier.

The frequency with which the phone location is collected can be changed after the s 180 authorisation to provide a higher resolution picture of a phone's movement between telephone towers. These changes often coincide with changes in investigative activity which may require a closer monitoring of a person's movements. Any increase in ping frequency is a more intrusive level of electronic surveillance of a person's movements.

To ensure that authorised officers can demonstrate they clearly weighed the privacy considerations of a potential change to ping frequency, it is necessary that the initial authorisation specifies the operational circumstances or reasons why the frequency can be changed. Where ping frequency is changed after the authorisation, records should be kept that demonstrate that these changes were in accordance with the original authorisation.

Case study

Amendment of ping frequency after authorisation

During our inspection of the Australian Commission for Law Enforcement Integrity (ACLEI), we discussed options for establishing a process to ensure post-authorisation ping variations are demonstrably consistent with the authorisation.

We consider that varying the ping frequency after authorisation is not authorised unless explicitly addressed by the authorised officer when making the original authorisation.

We suggested ACLEI should implement a 'pre-authorisation' process to ensure authorisations for location-based services (LBS/SEEK) data specify the authorised ping frequency and document the authorised officer's considerations of the privacy impacts of any increase in ping frequency. We also suggested ACLEI ensure record-keeping and processing practices are demonstrably consistent with the original authorisation.

ACLEI accepted these suggestions and advised they had updated the templates to incorporate ping frequency considerations by the authorising officer. ACLEI also updated their standard operating procedures instructing officers to ensure sufficient record-keeping practices to reflect when a ping frequency is altered and communicated these changes to the staff. ACLEI was also planning to deliver agency-wide training in relation to altering ping-frequencies post-authorisation.

Data outside the parameters of an authorisation

On occasion, telecommunications providers will provide agencies with data that was not authorised for disclosure. This is usually inadvertent or due to a provider misunderstanding the terms of the authorisation. We refer to this as 'data outside the parameters of an authorisation.' While agencies may receive data outside the parameters of an authorisation through no fault of their own, the agency is responsible for ensuring this unauthorised data is managed appropriately. This includes ensuring any such data is quarantined from further use or disclosure.

To reduce the risk of data being used or disclosed without proper authority, we rely on agencies having appropriate data vetting in place to assess the information and/or documents received from a provider against what was authorised. Agencies with insufficient or no consistent data vetting procedures tend to have a higher rate of non-compliance in managing data outside the parameters of an authorisation.

We made 8 suggestions and 3 better practice suggestions or comments across 8 agencies.[18] These included:

- strengthening existing processes to address gaps in vetting data received from carriers and quarantining data outside the parameters of the authorisation
- clarifying the implications of any use or disclosure of data that was obtained outside of the authorisation, and
- enhancing internal controls to limit access to quarantined data.

Case study

Identifying and managing unauthorised data

We identified instances where Tasmania Police (TAS Police) received small amounts of data outside the parameters of the authorisation. This was the result of a difference in time zones between the time and date of the authorisation and the data returned by the carrier.

While an agency may not have sought the data, failure to properly quarantine the data until it can be properly discarded from a system presents potential risks with that data being inadvertently or unlawfully used and disclosed.

We suggested Tasmania Police review each of the identified records, quarantine any unauthorised data and, if the information had been used or disclosed, seek advice on the implications of any such use or disclosure. We also suggested TAS Police strengthen their guidance material and data vetting processes to limit unauthorised data being returned where carriers routinely return data from different time zones.

These suggestions were accepted by TAS Police.

Use and disclosure of telecommunications data

Sections 181B and 182 of the TIA Act specify the circumstances in which data may be used or disclosed and prohibits the use or disclosure of data outside of these circumstances. The TIA Act also specifies record-keeping obligations under s 186A(1)(g)(iii) requiring agencies to keep records that show whether any use or disclosure took place in the permitted circumstances.

[18] SA ICAC, ACIC, ACLEI, VIC Police, WA Police, Home Affairs, AFP and Tasmania Police.

During our risk-based oversight pilot we assessed the risks of data being inappropriately used or disclosed across all agencies using the telecommunications data powers. This included reviewing agencies' procedures and templates, interviewing individuals involved in using and managing data, examining records of use and disclosure, and assessing each agency's ability to track use and disclosure of data.

We found that agencies who managed use and disclosure of data well had the following common frameworks in place:

- systems that have functionality to limit access to data to those directly involved with the investigation
- systems that stored data were auditable and could track who viewed or accessed the data
- procedures and workflows to manage the use and disclosure of data (including mandatory use of disclosure logs)
- robust guidance and policies in place to support staff in making decisions, and
- caveats on records containing data to remind staff of their obligations around use and disclosure.

We observed the following common contributors to the risks of inappropriate, unaccounted, or unlawful use and disclosure of data:

- systems where data was accessible by anyone with access to those systems, with no restrictions on a need-to-know basis
- systems where data is able to be taken out of the system or consolidated holdings without records being kept or procedures in place to account for where data was used or disclosed
- insufficient controls in place to ensure access to the data by an external agency (through memoranda of understanding or oversight functions) is for the purposes provided for in the TIA Act
- lack of guidance, policies, and procedures for staff to manage use and disclosure of data in a manner consistent with the TIA Act, and
- lack of staff awareness about the circumstances in which data may be used and disclosed, and their record-keeping obligations.

We made 5 suggestions and 11 better practice suggestions or comments regarding use and

disclosure across 9 agencies.[19] These included:

- implementing record-keeping mechanisms for use and disclosure of data, including when data is later identified as unauthorised
- ensuring controls are sufficient to mitigate the risk of external agencies inappropriately using or disclosing data, and
- providing reminders and prompts to staff about the obligation to keep records when using or disclosing data.

[19] ACLEI, QPS, NSW ICAC, WA Police, LECC, Home Affairs, AFP, NSW CC and NT Police.

Case study

Risk of unauthorised disclosure of telecommunications data

During our inspection of the Queensland Police Service (QPS), we noted several external agencies have direct access to QPS's system. This enabled those agencies to access and view telecommunications data previously accessed by the QPS under Chapter 4 of the TIA Act and held on the system. **We consider that when an external agency accesses this data it is a disclosure of the data to that external agency.**

We found risks that other agencies' could access data held within the QPS system for purposes other than enforcement of the criminal law. It was unclear what data had been disclosed to these agencies and whether these disclosures were for a purpose under the TIA Act.

We suggested QPS establish which agencies have access to this data in their system and implement measures to ensure accesses only take place in circumstances provided for in the TIA Act. QPS should also ensure records are kept to demonstrate how any access was for a purpose under the TIA Act.

QPS acknowledged that providing access to this data to support engagements with other agencies may conflict with the restrictions on use and disclosure under the TIA Act. The QPS undertook to address any non-compliance immediately and proposed to work with the Electronic Surveillance Reform Taskforce to explore these risks and potential implications for the proposed Electronic Surveillance Bill.

Journalist Information Warrant (JIW) controls

Agencies seeking to access the data of a person working as a journalist or their employer, for the purpose of identifying a journalist's source, must apply to an external issuing authority for a JIW before authorising access to telecommunications data. The JIW provisions recognises the public interest in protecting journalistic sources.

Before making any authorisation to access data, the authorising officer must consider, based on the circumstances of the request, whether a JIW may be required to access the data. To demonstrate this consideration, we expect agencies should have procedures and controls so an authorised officer can identify the circumstances where a JIW may be required and record their

considerations, including where legal or other advice was sought. Given the complexity of the legislative tests that apply to potential journalist involvement and JIW requirements, we consider it good practice for authorised officers to seek legal guidance where a journalist may be involved.

During our risk-based oversight pilot we assessed agencies' controls to manage access to data in circumstances where a JIW would be appropriate. We reviewed procedures and templates, conducted record checks, and interviewed individuals involved in requesting and authorising access to data.

While we did not identify any relevant data authorisations issued without a JIW, we made 3 suggestions and 4 better practice suggestions across 5 agencies on improving the controls agencies had in place to ensure JIW requirements are met[20].

These findings were directed at addressing gaps with in-built controls in requesting and authorising processes that require officers to turn their minds to whether requests related to a journalist or an employer of journalists, and if the request was to gather information in relation to a source.

[20] ACLEI, QPS, ACCC, WA Police and Tasmania Police.

Case study

Remediating a lack of JIW controls

Our 2022-23 inspection of NT Police identified that some prospective request forms did not contain any JIW controls to demonstrate that the requesting officer and the authorised officer considered whether JIW provisions could apply before making an authorisation under Chapter 4 of the Act. We also identified that electronic requests contained a prompt for the requesting officer to turn their mind to the JIW considerations under s 180H of the Act. However, there was no such prompt featured within the authorised officer section.

Authorising officers demonstrating that they had considered whether a JIW may be required before making an authorisation is an important safeguard to ensure compliance with legislation and protect journalist sources.

During the inspection, NT Police were proactive in updating their prospective request form to include information that reminds the requesting officer of the JIW obligations and allows them to indicate the potential for journalist involvement or a purpose of the authorisation being to identify a journalist's source. Information was also included to allow the authorised officer to demonstrate that they will turn their mind to the JIW considerations under the Act. Following the inspection NT Police provided confirmation that its electronic request form now contains an additional prompt for the authorised officer to turn their mind to the JIW considerations under the Act.

As a result of the prompt, and remedial action taken by NT Police both during and following the inspection, we made no suggestion or comment in relation to this risk area.

Reporting to the Minister

Section 186 of the TIA Act requires each enforcement agency to give a written annual report to the Attorney-General, as soon as practicable (and in any event within 3 months) after each 30 June. This report must set out the number of historic authorisations made by an authorised officer under s 178 and s 179 of the TIA Act and the number of prospective authorisations made under s 180 of the Act.

Our Office views this reporting obligation as a key accountability measure for agencies' use of telecommunications data powers, supporting transparency to Parliament and the public about the extent of access to data by enforcement agencies. We made 11 suggestions across 9 agencies[21] during our 2022–23 inspections in relation to reporting to the Minister.

Case study

Inaccuracies in ministerial reporting

In our previous 2021-22 inspection period, we identified issues in relation to 'withdrawn' authorisations that affected the accuracy of the Australian Criminal Intelligence Commission (ACIC)'s annual reporting to the Minister. In 2022-23, we again identified inaccuracies with ACIC's annual report to the Minister, relating to authorisations made for information from providers that are not a carrier for the purposes of the TIA Act and including records that had been withdrawn before being authorised.

A 'withdrawn' authorisation is an authorisation that has been approved (authorised) by an authorised officer but never notified to a provider. Consistent with advice from the Attorney-General's Department, **we consider 'withdrawn' notifications must still be included in annual reporting statistics to the Minister.**

We suggested the ACIC review its annual reporting for the previous 3 periods and correct any errors related to foreign providers or 'withdrawn' authorisations accordingly.

In response, the ACIC advised it intended to revisit the position with the Attorney-General's Department and amended its current work practices to define, articulate and collect 'withdrawn' authorisations. The ACIC also advised it will continue to work with our Office on this issue and will prepare to present all 'withdrawn' authorisations as part of future pre-inspection data.

[21] QCCC, ACIC, QPS, ACCC, WA Police, AFP, IBAC, SA Police and NT Police.

International Production Orders

The International Production Order (IPO) framework under Schedule 1 of the TIA Act enables Commonwealth, State and Territory law enforcement and national security agencies to intercept telecommunications and access telecommunications data and stored communications from Prescribed Communications Providers (PCPs) in foreign countries with whom Australia has a designated international agreement.

Australian agencies can seek an IPO for the purposes of either investigating an offence of a serious nature, or monitoring a person subject to a control order to protect the public from terrorist acts, prevent support for terrorist or hostile acts overseas and to detect breaches of that control order. There are 3 types of IPOs that can be sought by law enforcement for these purposes:

1. an order relating to interception
2. an order relating to accessing stored communications, and
3. an order relating to accessing telecommunications data.

Limitations on agencies' abilities to obtain certain IPOs mirrors constraints on accessing similar powers under other parts of the TIA Act. For example, an agency defined as a criminal law enforcement agency will be able to obtain an IPO to access telecommunications data or stored communications but will be restricted from applying for or being issued with an IPO for interception.

An IPO must comply with a nominated designated international agreement, before giving the order to the specified PCP. There is currently one designated international agreement in force to support the use of IPOs. On 15 December 2021, Australia and the United States of America signed 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 CLOUD Act Agreement). On 8 December 2022, Australia's Joint Standing Committee on Treaties ratified the CLOUD Act Agreement, which will remain in force for 5 years.

Despite this agreement being in place, the framework for Australian agencies to use an IPO under this agreement was not in effect during our inspection period. No Australian agency had been certified by the Australian Designated Authority (ADA) as operationally ready to use the powers and comply with the requirements under the agreement.

Under cl 142 and cl 143 of Schedule 1 of the TIA Act, the Ombudsman may inspect the records of an agency or the ADA to determine the extent of compliance with Schedule 1 by the agency and its officers. Section 150 requires the Ombudsman to report to the Attorney-General on the results of inspections conducted under cl 142 or cl 143 as soon as practicable after the end of each

financial year.

Our Inspections

As this was our first round of IPO inspections, we conducted health check inspections of agencies' governance frameworks. A health check inspection assesses an agency's readiness to use the IPO powers and helps identify potential compliance risks and areas for improvement. Our Office conducted health check inspections on 7 agencies seeking to access the IPO powers under Schedule 1 of the TIA Act.

Fourteen agencies advised they were not ready to undertake a health check inspection. We postponed our inspections of these agencies to allow them adequate time to prepare their governance framework to allow our health checks to make a meaningful assessment of compliance and readiness to use the powers. We plan to conduct health check inspections of these agencies during the next inspection period.

Table 7: Australian law enforcement agencies participation in IPO health check inspections by our Office

Agency	Health check conducted
ACLEI	×
ACCC	×
ACIC	✓
ADA	✓
AFP	✓
ASIC	×
CCC (WA)	×
CCC (QLD)	✓
NSW CC	×
DHA	✓
IBAC	×
ICAC (NSW)	×
ICAC (SA)	×
LECC	×
NSW Police	✓

Agency	Health check conducted
NT Police	×
QLD Police	×
SA Police	×
TAS Police	×
VIC Police	✓
WA Police	×

Through the health check inspections, we observed both collaboration and a willingness to share templates, training, and guidance material between agencies, particularly by agencies that had more mature frameworks and were closer to ADA certification. Agencies engaged openly and frankly with our Office and were receptive to suggestions to improve their processes, policies, and procedures.

Compliance Issues and Risks

Our health check inspections reviewed risk areas for non-compliance and identified potential improvement to agencies' processes, policies, and procedures. We observed several key areas we consider pose the greatest risk to an agency's compliance with the IPO provisions of the TIA Act. These included:

- varied levels of readiness to use an IPO
- minimal training had been prepared or delivered for staff on IPOs, including for applicants and authorising officers, and
- solutions for handling information from PCPs were not tested and finalised.

Varied levels of operational readiness

We found agencies' readiness to use the IPO powers varied significantly. Of the 7 agencies we inspected, only ADA, AFP and NSW Police had sufficiently advanced their governance frameworks to support using the powers. This included having sufficient policies, procedures, training, and record-keeping arrangements developed to support the requirements of Schedule 1 of the TIA Act.

The governance frameworks for the remaining 4 agencies were in varying stages of readiness[22]. For these agencies, our suggestions focused on implementing improvements to their policies, procedures, training, and record-keeping arrangements prior to accessing IPOs.

The systems supporting the issuing of an IPO to a PCP, and receiving data in response, remain untested. While the ADA provided regular updates on the progress of these systems, they were not sufficient to support the use of IPOs during the inspection period. We expect that these systems will be tested and operational within the 2023-2024 inspection period.

[22] ACIC, CCC (QLD), Home Affairs and VIC Police

Case study

Leading the way towards IPO operational readiness

Our inspection of NSW Police found they had a comprehensive and robust framework to support the use of IPOs. In addition to reviewing their business rules, policies and procedures, templates, and training, we interviewed staff likely to be involved in accessing and processing IPOs. We found the staff to be knowledgeable on the requirements of Schedule 1 of the TIA Act, the CLOUD Act Agreement and the ADA's Targeting and Minimisation Procedures (TMP). Step-by-step guides had been drafted to enable applicants and authorising officers to navigate through applying for and obtaining an IPO, and processing the IPO through the ADA to the relevant PCP.

We were encouraged by the level of collaboration between NSW Police, ADA and other agencies seeking to access IPO powers to share lessons and draft guidance and training material.

Draft training packages were in place to guide staff through the TMP, however needed to be expanded to cover the application and administration of IPOs under Schedule 1 of the TIA Act.

While NSW Police had made substantial progress towards being operationally ready to use IPOs, we provided feedback aimed at enhancing their templates and guidance material. NSW Police accepted the majority of these comments and advised that their templates, training and guidance material were being updated.

Limited training available for applicants and authorising officers

We observed that very few agencies had developed sufficient internal training programs to support applicants and authorising officers in using and administering the IPO powers. In most instances, training material was limited to complying with the TMP and CLOUD Act Agreement, and did not provide sufficient guidance on obtaining an IPO or on obligations in recording, using, managing, or destroying the data or information received from an IPO.

Only 3 of the 7 agencies had commenced developing formalised training programs[23]. In the case of NSW Police, the training was focused primarily on the role of the ADA, the CLOUD Act

[23] ADA, AFP and NSW Police

Agreement and TMP. AFP and ADA had developed some training materials for compliance with the Schedule 1 of the TIA Act, however these required significant development to support applicants and authorising officers with applying and administering the powers. The remaining agencies appeared to be waiting on the ADA to release their training portal to avoid inconsistencies and duplication in their training materials[24].

We suggested to all agencies that they should develop a training program and materials reflecting their responsibilities under Schedule 1 of the TIA Act, acknowledging the focus of ADA's training is directed towards compliance with the CLOUD Agreement and TMP. Additionally, we suggested agencies develop a plan to ensure all relevant staff in their agency are aware of their responsibilities under Schedule 1 of the TIA Act, including tailoring the delivery of training to areas likely to be significant users of IPOs.

[24] ACIC, CCC (QLD), Home Affairs and VIC Police

Case study

Developing training to support using Schedule 1

Although no formal training had been developed, the Crime and Corruption Commission Queensland (CCC (QLD)) had delivered presentations to their Crime and Corruption divisions on the introduction of the IPO regime. The CCC (QLD) advised that they anticipated staff would need to complete a mandatory training program before they could apply for an IPO.

The CCC (QLD) advised that the development of this mandatory training program was pending access to the ADA's training portal. This was in anticipation that ADA training would cover agencies' responsibilities and obligations in complying with Schedule 1 of the TIA Act. We acknowledged the ADA programs were likely to have limited guidance on compliance obligations under Schedule 1 and suggested the CCC (QLD) develop their own internal training to reflect their responsibilities and obligations under the Schedule. This should include guidance to applicants and authorising officers on accessing and using an IPO, along with complying with the requirements under Schedule 1.

We expect appropriate training and guidance material should be in place to support applicants and authorising officers understand their obligations under Schedule 1 before accessing an IPO.

CCC (QLD) accepted our feedback and advised that they had commenced developing appropriate training material. The CCC (QLD) advised they would make a copy of the material available to our Office once completed.

Untested solutions and procedure to receive information from PCPs

All the agencies we inspected raised concerns about procedures and technical solutions being sufficiently ready to support receiving data and information from PCPs. While acknowledging significant work was underway to implement appropriate systems to handle the anticipated information and data from the PCPs, the procedures supporting these systems were still under development, and testing of the systems had not yet commenced. Additionally, we noted apprehension amongst some agency staff around the anticipated volume of information and data from the PCPs, and the sufficiency of resources and vetting procedures to receive, review, store and, if necessary, quarantine this information and data.

Except for AFP and ADA, each agency acknowledged the need to enhance their in-house technical capabilities and support to receive and store the information and data from PCPs.

Agencies expressed concerns about limitations in their existing systems to receive and store the anticipated volume of information and data – limitations which most considered were the greatest risk to their agency's readiness to use the powers.

We anticipate that most agencies will experience 'teething' issues with receiving and ingesting the data and information they receive in response to an IPO. During our inspections, agencies advised that they were not anticipating using the IPO powers until the procedures and systems were sufficiently ready to receive the information and data from the PCPs. That said, we remain concerned that after receipt of the data or information from the PCP, agencies may not be sufficiently prepared to vet, record, store, manage, use, communicate, quarantine, or destroy the anticipated volume of IPO data or information consistently with the requirements under Schedule 1 of the TIA Act.

Case study

Getting ready to receive data and information from PCPs

During our inspection of the Australian Federal Police (AFP), we interviewed the Digital Forensics team who will be responsible for receiving and vetting the data from the PCPs. They demonstrated a high-level knowledge of IPOs and the requirements under Schedule 1 of the TIA Act and the CLOUD Act Agreement. They were aware of the end-to-end process in applying for and obtaining IPOs, and of the potential liaison requirements with relevant areas within the AFP involved in IPOs. The Standard Operating Procedures (SOP) developed by the team were in-depth.

While we are of the view that the processes AFP Digital Forensics have in place are sufficient to receive, vet and store the data, we recognised that these processes were supported by dedicated technical support resources to help develop, test, quality assure, and, where appropriate, redesign systems to support the anticipated volume of information from PCPs. **This level of technical support was not replicated across the other agencies seeking to access information from PCPs.**

We encouraged agencies seeking to use IPOs to access information from PCPs to leverage the lessons and experiences of the AFP in developing their technical capabilities and support. This includes ensuring agencies dedicate sufficient resources and training, and that technical support is allocated to support staff using a system to access information from a PCP.

Industry Assistance

The Industry Assistance framework was created for law enforcement and intelligence agencies to obtain assistance from the telecommunications industry to support their functions. This framework allows an agency to request or compel a Designated Communications Provider (DCP) to give certain types of assistance, in connection with any or all the eligible activities of the DCP, for a specified purpose under the Telecommunications Act.

The industry assistance powers under Part 15 of the Telecommunications Act are only available to interception agencies, defined under the TIA Act. During the inspection period, these powers were limited to the AFP, ACIC, ACLEI and State and Territory police. Recent amendments under the *National Anti-Corruption Commission (Consequential and Transitional Provisions) Act 2022* expanded the access to industry assistance powers to the NACC and 7 other agencies[25].

The industry assistance powers through which interception agencies can obtain assistance include:

- Technical Assistance Requests (TARs), being a request from the chief officer for a DCP to provide assistance on a voluntary basis
- Technical Assistance Notices (TANs), being a notice issued by the chief officer compelling a DCP to provide assistance to an interception agency, and
- Technical Capability Notices (TCNs), being a notice issued by the Attorney-General compelling a DCP to develop the capability to assist an interception agency.

Industry assistance powers do not replace the warrant and authorisation regimes under the TIA Act, the *Surveillance Devices Act 2004* (the SD Act), or other State or Territory laws, and must not provide a new basis for interception. For example, to intercept communications, interception agencies still need to seek a telecommunications interception warrant under the TIA Act. However, industry assistance mechanisms can be used to seek technical assistance to help give effect to a separate warrant or authorisation.

Part 15 of the Telecommunications Act allows interception agencies to seek reasonable and proportionate assistance directly from DCPs in conjunction with existing warrants and authorisations for specified purposes. The Telecommunications Act also includes a range of procedural requirements and safeguards to ensure:

[25] Additional agencies included NSW ICAC, NSW CC, LECC, IBAC, CCC (Qld), SA ICAC and CCC (WA).

- that any request or notice given to a DCP is reasonable and proportionate
- that compliance with the request or notice is practically and technically feasible
- that the agency is not requiring or requesting the DCP to implement or build in a systemic weakness, and
- that requests or notices are used to enforce the criminal law, as far as it relates to serious Australian or foreign offences punishable by a maximum term of imprisonment of 3 years or more.

Under s 317ZRB(1) of the Telecommunications Act, the Ombudsman may inspect the records of an interception agency to determine the extent of compliance with Part 15 by the agency and its officers. Section 317ZRB(3) provides the Ombudsman with the ability to report to the Attorney-General on the results of one or more inspections conducted under s317ZRB(1).

Our Inspections

Our Office inspected 4 interception agencies' use of industry assistance instruments under Part 15 of the Telecommunications Act for records covering the period from 1 July 2022 to 30 June 2023[26]. We made:

- 6 suggestions, and
- 10 better practice suggestions or comments.

In 2021–2022, we made 12 suggestions and 12 better practice suggestions.

A total of 30 TARs were issued by the 4 agencies, with NSW Police being the highest user of the power (issuing 21 TARs). The TARs sought assistance from DCPs to enable the execution of warrants or authorisations issued under the TIA Act, the SD Act and other legislation for investigation of offences related to organised offences and/or criminal organisations, homicide, illicit drug offences, sexual assault, cybercrime offences and acts intended to cause injury. Several agencies use TARs to develop a standing capability with the DCP to support the execution of telecommunications data authorisations under s 178 of the TIA Act, where a serious offence threshold was met.

There were no TANs or TCNs issued to interception agencies during the reporting period.

[26] ACIC, AFP, NSW Police and Victoria Police

Table 8: Number of suggestions and better practice suggestions or comments made per agency during the 2022–23 inspection period (figures from the 2021–22 inspection period are included in brackets)

Agency	Recommendations	Suggestions	Better practice suggestions and comments	Total
ACIC	0 (0)	0 (3)	1 (2)	**1 (5)**
AFP	0 (0)	2 (3)	5 (2)	**7 (5)**
NSW Police	0 (0)	0 (3)	0 (3)	**0 (6)**
VIC Police	0 (0)	4 (3)	4 (5)	**8 (8)**
TOTAL	**0 (0)**	**6 (12)**	**10 (12)**	**16 (24)**

Compliance Issues and Risks

Our inspections revealed 2 areas that we consider pose the greatest risk to an agency's compliance with the industry assistance provisions of the Act. These included:

- a lack of consistency between the authorisation or warrant and the enabling industry assistance instrument, and
- insufficient information in applications to link the assistance sought with the relevant object or other authorising processes.

Our inspections identified a number of minor administrative or low risk compliance issues across the agencies which have not been included in this report. These included insufficient delegations in place to authorise notifications to our Office[27] and instrument templates and guidance material insufficiently addressing disclosure provisions[28]. The affected agencies accepted our comments and sought to remedy these issues.

Lack of consistency between authorisations or warrants and the enabling industry assistance instrument

Industry assistance legislation assists interception agencies with exercising a function or power and is not a framework by itself to access content or data. Section 317ZH of the Telecommunications Act is a safeguard prohibiting a TAR, TAN or TCN from replacing a warrant or authorisation under the TIA Act or another law, if the issuing agency would otherwise need one for the activity. If the authorisation or warrant seeks information that is only accessible with an industry assistance instrument in place, the agency should ensure there is consistency

[27] ACIC and VIC Police
[28] VIC Police

between the assistance sought and the data or information requested.

We found TAR applications at the AFP where the applicant did not clearly demonstrate how the assistance being sought from the DCP related to data to be accessed through an authorisation or warrant. This was particularly the case in circumstances where a TAR was being used to establish a capability that would enable access to data from an anticipated, but not issued, authorisation or warrant. Additionally, we noted instances where the information or data returned was inconsistent with what was being sought through the TAR.

We consider that the application for an industry assistance instrument should contain sufficient detail to enable the authorising officer to be satisfied that the DCP would not do an act or thing that would otherwise be required through an authorisation or warrant under another Commonwealth, State or Territory law. This should include demonstrating through the application that:

- an appropriate authorisation or warrant exists, or will be obtained, to access data or information being sought
- that the TAR will enable the interception agency to use the authorisation or warrant to access the data or information, and
- any data or information returned through the assistance provided under the TAR is consistent with what is sought under the authorisation or warrant.

Insufficient details in the documentation linking the assistance to the relevant objective and other authorisation processes

To demonstrate compliance with s 317G(2) of the Telecommunications Act, our Office's position is that any application, decision record and TAR must particularise the function or exercise of power being undertaken, and/or offence/s being investigated in connection with the TAR. While it may not be necessary to specify exact offences, it should record how any TAR, or capability created through the TAR, may interact with the underlying authorisation or warrant, to meet the relevant objective provisions under
s 317G(5) of the Telecommunications Act (being that such authorisations or warrants would be for a serious Australian or foreign offence).

We observed one agency used TARs to allow a DCP to develop a capability that would be used to access information or data through an anticipated (not yet issued) authorisation or warrant. It was unclear from the TAR applications how the assistance to be provided by the DCP would support either the functions of the agency or enforce the criminal law, so far as it related to a serious offence (an offence against the law of the Commonwealth, a State or Territory that is punishable by 3 years or more imprisonment, or for life). In the case of the AFP, it was also

unclear, from the application, how the anticipated authorisations would ensure that the serious offence threshold would be met prior to authorising access to the data, via the TAR.

We have concerns that a broadly framed TAR may not sufficiently demonstrate how the assistance to be provided by the DCP support the functions of the agency or would be limited in its application to future authorisations or warrants that meet the serious offence thresholds. To demonstrate compliance with the provision of s 317G(5) of the Telecommunications Act, we would expect that the TAR application and TAR instrument should specify how the assistance to be provided by the DCP will:

- assist the agency with the performance of a function or exercise of a power, conferred by or under a law of the Commonwealth, a State or Territory, and
- assist with the enforcing of the criminal law, so far as it relates to a serious Australian or foreign offence(s).

In the event that the TAR seeks assistance in anticipation of an authorisation or warrant being issued, the TAR application should demonstrate how the agency intends to ensure that the authorisation or warrant will relate to a serious offence threshold.

Case study

Inadequate information recorded on a TAR

During our inspection of the AFP, we identified that it was unclear on the face of 2 of their TARs how the capability being developed through the instrument related to the relevant objective, under s 317G of the Act. In particular, the TAR was limited in respect to demonstrating how the capability would assist the AFP in relation to enforcement of the criminal law, in so far as it related to serious Australian or foreign offences. The TARs did not contain any background to the investigations of the relevant offences. The delegate decision noted in their approval that they were satisfied the request "relates to the investigation of serious Australian offences" but without stating the exact offence or what made it serious.

We are concerned that a broadly framed TAR may not clearly stipulate the organisational function or purpose and/or relevant offences that the industry assistance mechanism relates to and therefore may not be sufficient to demonstrate compliance with the Act.

As a result, we suggested that the AFP make sure that TARs (including applications for TARs) contain sufficient information and explanation to demonstrate how it meets the conditions of ss 317G(2) and 317G(5), including details of how the mechanism is intended to interact with other authorisation processes or warrant regimes to satisfy the conditions under s 317G.

The AFP accepted the suggestion and stated that it had enhanced its template guidance in relation to s 317G of the Act. It also committed to enhancing application vetting guidance processes, and exploring the viability of training for relevant AFP members in relation to its industry assistance application process and required considerations.

Appendices

Appendix 1 – Glossary of terms

Term (and section of the Act)	***Description***
AAT	Administrative Appeals Tribunal
Accessing a stored communication s 6AA	For the purpose of the TIA Act, accessing a stored communication consists of listening to, reading, or recording such a communication by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.
ADA	Australian Designated Authority – Schedule 1 to the TIA Act establishes the ADA within the Attorney General's Department. The ADA serves as a gateway between domestic requesting agencies and foreign PCPs.
Administrative Arrangements Order	Refers to an order where a minister is delegated the responsibility for the performance of functions and duties and the exercise of powers relating to the legislation outlined in the order.
Administrative errors	Errors made within administrative processes such as document preparation, statistical reporting, and record-keeping. Administrative errors are often a result of human error and may not impact on the validity of an authorisation or warrant. However, some administrative errors result in instances of technical non-compliance. Our Office reports on administrative errors where actual non-compliance has occurred or there is a risk of non-compliance where the error is not rectified.
Administrator of the Act	Under the Administrative Arrangements Order commencing 1 July 2022, the Attorney-General is responsible for the administration of the TIA Act, except to the extent it is administered by the Minister for Home Affairs in relation to the Australian Security Intelligence Organisation.
Affidavit	A written statement confirmed by oath or affirmation for use as evidence in court.
AGD	Attorney-General's Department.
Authorisation for access to telecommunications data ss 178-180B and s 183	An authorisation for access to telecommunications data under Chapter 4 of the TIA Act permits the disclosure of information or documents by a carrier or carriage service provider to enforcement agencies. *Historic authorisations* Agencies may authorise the disclosure of specified information or

Term (and section of the Act)	Description
	documents that came into existence before a carrier or carriage service provider receives notification of an authorisation. Historic authorisations can be made where the authorised officer is satisfied that the disclosure is reasonably necessary for: • enforcing the criminal law (s 178), • the purpose of finding a person who the Australian Federal Police or a Police Force of a State has been notified is missing (s 178A). Section 178A authorisations can only be made by the AFP or a Police Force of a State. • enforcing a law imposing a pecuniary penalty or protecting the public revenue (s 179). *Prospective authorisations* Under s 180 of the TIA Act agencies may authorise the disclosure of specified information or documents that come into existence when an authorisation is in force, if satisfied that the disclosure is reasonably necessary for investigating a serious offence (as defined in s 5D of the Act) or an offence against any Australian law that is punishable by imprisonment for at least 3 years. Prospective authorisations come into force at the time the carrier or carriage service provider receives notification of the authorisation and, unless revoked earlier, cease to be in force at the time specified in the authorisation which must be no later than 45 days from the day the authorisation is made. *Note that different requirements apply for the period in which authorisations made under JIWs are in force.* *Foreign authorisations* Under s 180A of the TIA Act the AFP can authorise disclosure of specified information or documents that come into existence before the carrier or carriage service provider receives notification of the authorisation. Matters about which the AFP must be satisfied in making the authorisation are set out in s 180A(3) of the TIA Act. Under s 180B of the TIA Act, the AFP can authorise disclosure of specified information or documents that come into existence when an authorisation is in force. Matters about which the AFP must be satisfied in making the authorisation are set out in s 180B(3) of the TIA Act. Authorisations under s 180B of the TIA Act come into force at the time the carrier receives notification of the authorisation and, unless revoked earlier, cease to be in force at the time specified in the authorisation which must be no later than 21 days from the day the authorisation is made unless this period is extended. *Form of authorisations*

Term (and section of the Act)	*Description*
	An authorisation for disclosing telecommunications data must be in written or electronic form and meet the requirements outlined in the CAC Determination.
Authorised officer s 5	An authorised officer is an officer with the power to make or revoke authorisations for disclosing telecommunications data or give or revoke an ongoing preservation notice or a foreign preservation notice (the AFP only) under the Act. In addition to the specified positions set out in the definition of authorised officer under s 5 of the TIA Act, the head of an enforcement agency may, by writing, authorise a management office or management position in an enforcement agency as an authorised officer (s 5AB(1)). The Commissioner of Police may authorise in writing a senior executive AFP employee who is a member of the AFP to be an authorised officer (s 5AB(1A)). Authorised officers are a critical control for ensuring telecommunications data powers are used appropriately.
Better practice suggestion	Better practice suggestions are suggestions that our Office considers would further improve agencies' practices and procedures if implemented and reduce risk of non-compliance with the Act. It is important to note that better practice suggestions do not reflect the existence of non-compliance or a shortcoming on an agency's part.
Bi-lateral agreement	An agreement between Australia and a foreign country.
CAC Determination s 183(2)	*Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2018* The above determinations were made under subsection 183(2) of the TIA Act which specifies that the Communications Access Co-ordinator may, by legislative instrument, determine requirements of the form of authorisations, notifications and revocations relating to telecommunications data.
Carrier stored communications warrant response coversheet	When providing stored communications to an agency the carrier will typically complete an "*Response to a stored communications warrant issued under the Telecommunications (Interception and Access) Act 1979*" coversheet. This document outlines important dates and times as recorded by the carrier including when it accessed stored communications on its systems.
Chief officer s 5	The head of an agency, however described by each specific agency. For example, the Commissioner of Police is the chief officer of the Australian Federal Police.
CLOUD Act Agreement	Agreement between the Government of Australia and the

Term (and section of the Act)	*Description*
	Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime.
Conditions and restrictions s 118(2)	A stored communications warrant may specify conditions or restrictions relating to accessing stored communications under the warrant.
Conditions for giving preservation notices s 107H(2) and s 107J(1), s 107N(1) and s 107P	Under s 107H(2) of the TIA Act an agency may only give a domestic preservation notice if the conditions in s 107J(1) of the TIA Act are satisfied. Under s 107N(1) of the TIA Act the AFP must give a foreign preservation notice if it receives a request in accordance with the conditions in s 107P of the Act.
Criminal law enforcement agency s 110A	Section 110A of the TIA Act defines the following agencies as criminal law enforcement agencies: • the Australian Federal Police • a Police Force of a State (as per s 5 of the Act, a State includes the Northern Territory) • the Australian Commission for Law Enforcement Integrity • the Australian Criminal Intelligence Commission • subject to subsection (1A), the Immigration and Border Protection Department (now known as the Department of Home Affairs) • the Australian Securities and Investments Commission • the Australian Competition and Consumer Commission • the NSW Crime Commission • the Independent Commission Against Corruption (NSW) • the Law Enforcement Conduct Commission • the IBAC • the Crime and Corruption Commission (Qld) • the Corruption and Crime Commission (WA) • the Independent Commissioner Against Corruption (SA) • subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.
Data vetting	Where an agency screens stored communications or telecommunications data received from a carrier to confirm whether the information was provided within the parameters of a valid stored communications warrant or telecommunications data authorisation.
DCP	Designated communications provider - This refers to the entity that is requested/required to give assistance. Section 317C of the Telecommunications Act defines what constitutes a DCP.
Destruction of stored communications information	Section 150(1) of the TIA Act sets out the circumstances under which information or records that were obtained by accessing stored communications must be destroyed. When the chief officer

Term (and section of the Act)	*Description*
s 150(1)	of an agency is satisfied that information or records are not likely to be required for a permitted purpose, they must cause the information or record to be destroyed 'forthwith'. While the TIA Act does not define 'forthwith' an agency may hold itself to a particular timeframe which will guide our assessments. However, we will also consider whether this timeframe is reasonable in the circumstances noting the ordinary definition of 'forthwith' as immediate and without delay. Where an agency does not have a strict timeframe for destructions, in assessing compliance with this provision, our Office makes an assessment based on our understanding of an agency's policies and procedures and what we consider to be reasonable in the circumstances.
DIA	Designated International Agreement - An agreement between Australia and a foreign country (for example the CLOUD Act Agreement).
Disclosure by agencies to our Office	Prior to or during an inspection, agencies may make a disclosure to our Office outlining one or more instances of non-compliance with the TIA Act or the Telecommunications Act. Our Office's inspection reports outline the details of disclosed non-compliance and any agency actions to correct or manage the non-compliance. Disclosures may not be reported in inspection reports if they are primarily administrative in nature. We encourage agencies to make disclosures to our Office following self-identified instances of non-compliance.
Disclosure of telecommunications data	A carrier makes a disclosure of telecommunications data (information or documents) to an agency following notification of an authorisation. For example, an agency notifies a carrier of an authorisation through a secure system. The carrier responds by making a disclosure of telecommunications data to the agency, also within the secure system. The telecommunications data disclosed should fall within the parameters specified in the authorisation.
Exit interview	Following an inspection, we hold an exit interview with officers of the agency. We present our preliminary inspection and give the agency the opportunity to comment.
Full and free access s 186B(2)(b)	For the purpose of an inspection, the Ombudsman is entitled to have full and free access at all reasonable times to all records of an agency that are relevant to the inspection.
Health check	An assessment of the readiness or 'health', of an agency's compliance framework to identify any potential issues or risks, and areas for improvement.
Historic authorisation	An historic authorisation enables access to information or

Term (and section of the Act)	*Description*
ss 178, 178A, 179	documents that came into existence before a carrier receives notification of an authorisation. An authorised officer must not make an authorisation unless he or she is satisfied that the disclosure is reasonably necessary for: • enforcing the criminal law • locating a missing person, or • enforcing a law imposing a pecuniary penalty or for protecting public revenue.
IA	Industry Assistance.
IGIS	Inspector-General of Intelligence and Security.
Industry assistance mechanisms	The substantive mechanisms that exist under Part 15 of the Telecommunications Act (i.e., TAR, TAN, TCN).
Inspection period	The period during which an inspection occurs for a specific agency. In relation to the annual reports, this is the financial year during which the inspections being reported were held.
Inspection report	An inspection report presents the findings of an inspection together with any suggestions or recommendations made in response to findings. An inspections report may be formal, streamlined or findings letter. We prepare formal reports where our inspection identified significant or systemic issues or where we consider a formal recommendation is warranted to address legislative non-compliance. Formal reports are generally signed by the Ombudsman and sent directly to an agency's chief officer for action and response. These inspection reports and any subsequent comments on the reports from agencies, contribute to this annual report to the Minister. We prepare streamlined reports when our inspection findings are not indicative of significant or systemic issues. The instances of non-compliance reported in streamlined reports are typically straightforward and non-contentious. A streamlined report may make suggestions and better practice suggestions to an agency to assist it in achieving compliance with the legislation. We provide these reports directly to the relevant business area of an agency.
Intelligence agencies	The Australian Secret Intelligence Service, Australian Security Intelligence Organisation, and the Australian Signals Directorate. These are agencies, other than interception agencies, who are empowered to issue TARs and TANs under Part 15 of the Telecommunications Act. 'Intelligence agencies' is a term of convenience used by Ombudsman staff; it is not used in the legislation.

Term (and section of the Act)	*Description*
Interception agency s 5	The following agencies are interception agencies: • the Australian Federal Police • the Australian Commission for Law Enforcement Integrity • the Australian Criminal Intelligence Commission • an eligible authority of a State in relation to which a declaration under s 34 of the TIA Act is in force.
Integrated Public Number Database (IPND or IPNDe)	The IPND is an industry-wide database which contains all listed and unlisted public telephone numbers. Information contained in the IPND may include the name and address of a customer and the type of service registered to that customer.
IPO	International Production Order.
Journalist information warrant ss 180H, 180R-T and 180X	An enforcement agency must obtain a Journalist Information Warrant (JIW) when it seeks to access the telecommunications data of a journalist (or their employer) where a purpose of accessing the information is to identify another person whom the authorised officer knows, or is reasonably believed to be, a source of that journalist. To obtain a JIW an enforcement agency must apply to an eligible Judge, Magistrate or AAT member who has been appointed by the Minister. The issuing authority must not issue a JIW unless they are satisfied, for example, that the warrant is reasonably necessary for purposes outlined under subsection 180T(2) of the TIA Act and that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source in connection with whom authorisations would be made under the authority of the warrant. JIWs are also subject to scrutiny from a Public Interest Advocate who is appointed by the Prime Minister. Under the TIA Act the Public Interest Advocate may make submissions to an eligible issuing authority about matters relevant to the decision to issue, or refuse to issue, a JIW.
Minister	Under the Administrative Arrangements Order commencing 1 July 2022, the Attorney-General is now the relevant minister, except in relation to the Australian Security Intelligence Organisation where the relevant minister is the Minister for Home Affairs.
Multi-lateral agreement	An agreement between Australia and 2 or more foreign countries.
Mutual Legal Assistance	Is the process countries use to obtain government-to-government assistance in criminal investigations and prosecutions. Australia's mutual assistance system is governed by the *Mutual Assistance in Criminal Matters Act 1987* which is administered by the AGD.
Non-compliance	In the context of our Office's oversight role an agency

Term (and section of the Act)	*Description*
	demonstrates non-compliance when it has not met a requirement or requirements of the Act.
Officers approved to exercise the authority of stored communications warrants s 127	Under s 127(1) of the TIA Act the authority conferred by a stored communications warrant may only be exercised by a person in relation to whom an approval under s 127(2) is in force in relation to the warrant. Under s 127(2) of the TIA Act the chief officer of a criminal law-enforcement agency or an officer in relation to whom an appointment under s 127(3) of the TIA Act is in force may approve a specified person to exercise the authority conferred by warrants (or classes of warrants).
Notification to carrier s 184	When a telecommunications data authorisation or revocation (of authorisation) is made, it is notified to the carrier. Notification may be made via: • fax • email • through the Secure Electronic Disclosures Node (SEDNode), a secure electronic system used by enforcement agencies and carriers to facilitate disclosure of telecommunications data.
Part 5.3 IPO agencies	Refers to a Part 5.3 warrant agency to the extent that the agency applies for warrants issued in relation to Part 5.3 supervisory orders in force in relation to persons. These agencies include the AFP, ACIC and the ACLEI.
Part 5.3 supervisory order	Refers to a control order, extended supervision order or interim supervision order.
PCP	Prescribed Communications Provider – refers to a network entity and transmission, message/call application, storage/ back-up, and general electronic content service providers.
PJCIS	Parliamentary Joint Committee on Intelligence and Security.
Pre-inspection data	Data provided by agencies to the Commonwealth Ombudsman prior to an inspection regarding their use of the powers under Chapter 3 or Chapter 4 of the TIA Act in the relevant period.
Prescribed forms s 118(1)(a) s 180U(1)	A stored communications warrant must be in the prescribed form. The prescribed form of a domestic stored communications warrant is set by Form 6 of Schedule 1 of the *Telecommunications (Interception and Access) Regulations 2017*. A journalist information warrant must be in the prescribed form. The prescribed form of a journalist information warrant is set by Form 7 of Schedule 1 of the *Telecommunications (Interception and Access) Regulations 2017*.
Preservation notice s 107H, s 107N	A preservation notice is an internally issued notice given by an agency which requires a carrier to preserve stored

Term (and section of the Act)	*Description*
	communications that relate to the person or telecommunications service specified in the notice and hold those communications on its systems for a certain period during which time the agency may obtain a warrant to access those communications. There are 2 types of preservation notices: • Domestic preservation notices, and • Foreign preservation notices. <u>Domestic preservation notices</u> • Historic domestic preservation notice – may be given by a criminal law-enforcement agency. These notices require carriers to preserve stored communications it holds at any time on or before the day the carrier receives the notice. • Ongoing domestic preservation notice – may only be given by a criminal law-enforcement agency that is also an interception agency. These notices require carriers to preserve stored communications it holds at any time from when the carrier receives the notice to the end of the 29th day after receipt. <u>Foreign preservation notices</u> • If the AFP receives a request from a foreign entity in accordance with the conditions in s 107P of the Act, the AFP must give a foreign preservation notice. These notices require carriers to preserve stored communications it holds at any time on or before the day the carrier receives the notice. • Foreign entities who may make a request to the AFP to preserve stored communications are a foreign country, the International Criminal Court, or a War Crimes Tribunal (s 107P(1) of the Act).
Privacy considerations s 180F	Section 180F of the TIA Act stipulates that matters relating to privacy must be considered by an authorised officer before making a telecommunications data authorisation. The authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate having regard to the following matters: • the gravity of any conduct in relation to which the authorisation is sought, including: ○ the seriousness of any offence in relation to which the authorisation is sought

Term (and section of the Act)	*Description*
	○ the seriousness of any pecuniary penalty in relation to which the authorisation is sought ○ the seriousness of any protection of the public revenue in relation to which the authorisation is sought ○ whether the authorisation is sought for the purposes of finding a missing person • the likely relevance and usefulness of the information or documents, and • the reason why the disclosure or use concerned is proposed to be authorised.
Prospective authorisation s 180 TIA Act	A prospective authorisation enables access to information or documents that come into existence when an authorisation is in force. A prospective authorisation may also authorise the disclosure of 'historic' data – telecommunications data that came into existence before the time the authorisation comes into force. Authorised officers must not make a prospective authorisation unless the disclosure is reasonably necessary for investigating a serious offence or an offence against the law of the Commonwealth, a State or Territory that is punishable by imprisonment for at least 3 years. Prospective authorisations come into force when a person (usually a carrier) receives notification of the authorisation. Unless the authorisation is revoked earlier or is an authorisation made under a JIW, the authorisation ceases to be in force at the time specified in the authorisation. This time must be no longer than 45 days beginning on the day the authorisation is made. For example, a prospective authorisation is made on 1 March 2019 for all telecommunications data relating to a specified telecommunications number. The authorisation is in force until 31 March 2019. The authorisation is notified to Telstra at 12pm on 2 March 2019. Telstra is then required to disclose all telecommunications data relating to the number from 12pm 2 March 2019 to 11:59pm 31 March 2019.

Term (and section of the Act)	*Description*
Quarantine	In the context of managing stored communications and telecommunications data, the term 'quarantine' means to restrict the use of information through removing access to that information by physical, electronic, or other means. The purpose of quarantining information is to prevent any use, communication, or disclosure of that information. For example: if an agency receives information outside the parameters of a stored communications warrant or telecommunications data authorisation the agency may quarantine the information by: • Storing the information on a separate disc and locking the disc away from investigators • Copying the information to a separate password protected file accessible only to nominated officers • Other actions in line with agency policies and procedures.
Receiving stored communications information s 135	Section 135(2) of the TIA Act states the chief officer of a criminal law-enforcement agency may authorise in writing officers or classes of officers, of the agency to receive information obtained by accessing stored communications under stored communications warrants, or classes of such warrants issued to the agency. For example, the chief officer may authorise certain officers by position title or members of an investigative team to receive stored communications accessed by a carrier under a stored communications warrant. Our Office considers stored communications information to be received for the purpose of s 135 of the TIA Act when it is first opened and viewed.
Recommendation	In an inspection report we may make a recommendation to an agency where significant non-compliance and / or deficiencies in agency processes are identified on inspection.
Remedial action	Remedial action is steps taken by an agency to address a compliance issue or finding that our Office has made from of an inspection.
Reporting period	The period for which records are being reviewed – generally, the financial year ending prior to commencement of inspections.
Requesting officer	Within an agency a requesting officer is an officer who makes a request for a telecommunications data authorisation. The requesting officer is typically an agency investigator or other person with intimate knowledge of an investigation. The request is forwarded to an authorised officer for their consideration. The request typically contains:

Term (and section of the Act)	*Description*
	• details of the investigation, for example the serious offence, or missing person or pecuniary penalty involved • relevant person(s) and service(s) • the relevance or usefulness of the telecommunications data sought, and • privacy considerations
Retrospective	Our inspections of agencies' compliance with Chapters 3 and 4 of the TIA Act operate retrospectively. This means that we review the previous financial year's records during an inspection. During our inspections conducted in the 2020–21 financial year we primarily reviewed records for the 2019–20 financial year.
Revocation ss 107J, 107L, 107R, 122 and 180(7)	Preservation notices Under s 107L(2) of the TIA Act an agency must revoke a preservation notice if the conditions for giving a preservation notice under s 107J(1)(b) or (c) of the TIA Act are no longer satisfied or if the agency decides not to apply for a warrant to access the preserved stored communications. A domestic preservation notice is revoked by the issuing agency giving the carrier to whom it was given written notice of the revocation. Mandatory revocation provisions for foreign preservation notices given by the AFP are outlined under s 107R of the TIA Act. An agency may also revoke a preservation notice at any time at its own discretion (s 107L(1) of the TIA Act). Stored communications warrants Under s 122(1) of the TIA Act, a chief officer must revoke a stored communications warrant in writing if the grounds on which the warrant was issued have ceased to exist. If another criminal law-enforcement agency is exercising the authority of the warrant, the chief officer of the issuing agency must inform the chief officer of the other agency of the proposed revocation prior to it occurring. Section 123 of the TIA Act states that, following the revocation, the chief officer of the issuing agency must inform the chief officer of the other agency 'forthwith' of the revocation. Telecommunications data authorisations Under s 180(7) of the TIA Act an authorised officer of a criminal law-enforcement agency must revoke an authorisation if they are satisfied that the disclosure is no longer required or, if the authorisation is made under a JIW, the warrant is revoked under s 180w.
Risk mitigation	Risk mitigation in the context of our inspections is action that can be taken by agencies to reduce the likelihood of future non-

Term (and section of the Act)	*Description*
	compliance.
the **Schedule**	Schedule 1 of the *Telecommunications (Interception and Access) Act 1979*.
Serious contravention s 5E	Section 5E(1) of the TIA Act defines a serious contravention as a contravention of a law of the Commonwealth, a State, or a Territory that: (a) is a serious offence or (b) is an offence punishable: (i) by imprisonment for a period, or a maximum period, of at least 3 years or (ii) if the offence is committed by an individual—by a fine, or a maximum fine, of at least 180 penalty units or (iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 900 penalty units or (c) could, if established, render the person committing the contravention liable: (i) if the contravention were committed by an individual—to pay a pecuniary penalty of 180 penalty units or more, or to pay an amount that is the monetary equivalent of 180 penalty units or more or (ii) if the contravention cannot be committed by an individual—to pay a pecuniary penalty of 900 penalty units or more, or to pay an amount that is the monetary equivalent of 900 penalty units or more.
Serious offence s 5D	Section 5D of the TIA Act lists those offences classed as a 'serious offence' for the purposes of the Act. Serious offences include but are not limited to murder, kidnapping, theft, drug trafficking and other drug offences, cybercrime, dealing in proceeds of crime, bribery or corruption offences and insider trading.
Standard Operating Procedures (SOPs)	Standard operating procedures, or SOPs, are an agency's written documents that provide guidance on how to undertake actions.
Stored communication (SC) s 5 TIA Act	A communication that: (a) is not passing over a telecommunications system and (b) is held on equipment that is operated by, and is in the possession of, a carrier and (c) cannot be accessed on that equipment by a person who is not a party to the communication without the assistance of an employee of the carrier. Types of stored communications include: • Emails • Text messages (SMS) • Multimedia messages (MMS)

Term (and section of the Act)	*Description*
	• Voicemail messages.
Stored communications warrant ss 116-117	A stored communications warrant is issued under Chapter 3 of the TIA Act. The warrant is issued in respect of a person, and authorises approved persons to access stored communications: • that were made by the person in respect of whom the warrant was issued or • that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued and that become, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.
Stored communications warrants issued in relation to a victim of a serious contravention s 116(1)(da) TIA Act	Subject to other conditions being met, an issuing authority may issue a stored communications warrant in relation to a person who is the victim of a serious contravention if satisfied that the person is unable to consent or it is impracticable for the person to consent to those stored communications being accessed.
Subscriber s 5 TIA Act	A person who rents or uses a telecommunications service.
Suggestion	In an inspection report we may make a suggestion to an agency to improve its compliance with the Act. Suggestions may include but are not limited to: • updating standard operating policies and procedures • seeking legal advice • training for officers involved in using stored communications or telecommunications data powers, and • reviewing workplace practices to reduce the risk of non-compliance. A suggestion is often the first line approach to non-compliance where an agency needs to undertake additional things to stop it reoccurring. These often suggest improvements to processes or suggest that an agency cease a particular process.
Targeting and Minimisation Procedures (TMPs)	Refers to a set of procedures which exist to ensure Australian agencies seeking data from the USA via the IPO framework are compliant with the CLOUD Act agreement. Further to this, these procedures are in place to limit the acquisition, retention and dissemination of information concerning US Persons by an Australian requesting agency.
Technical Assistance Notice (TAN)	A notice issued by a designated intelligence agency or interception agency under s 317L of the Telecommunications Act. A TAN compels a DCP to provide assistance to interception or intelligence agencies. A TAN cannot require a DCP to create a new

Term (and section of the Act)	*Description*
	capability.
Technical Assistance Request (TAR)	A request issued by an intelligence agency or an interception agency under s 317G of the Telecommunications Act. This is a request for the DCP to provide voluntary assistance.
Technical Capability Notice (TCN)	A notice given by the Attorney General under s 317T of the Telecommunications Act requiring that a DCP take steps to ensure it is capable of providing assistance, or otherwise provide assistance to an interception or intelligence agency for a specified purpose.
The **Telecommunications Act**	*Telecommunications Act 1997*
Telecommunications data (TD)	Telecommunications data is information about an electronic communication which does not include the contents or substance of that communication. Telecommunications data includes but is not limited to: • subscriber information • the date, time, and duration of a communication • the phone number or email address of the sender and recipient of a communication • Internet Protocol (IP) address used by the person of interest while accessing / using internet-based services • the start and finish time of each IP session • the amount of data up / downloaded, and • the location of a mobile device from which a communication was made.
Telecommunications Interception (TI)	Telecommunications Interceptions allow law enforcement agencies to listen to or record communications as they pass over telecommunications systems in real time, without the knowledge of the person making the communication. For example, telephone conversations, faxes, email, instant messaging, and internet browsing.
Telecommunications providers	Carriers and carriage service providers who supply certain carriage services over a telecommunications network, as defined in the Telecommunications Act 1997. Carriers in Australia include but are not limited to: • Telstra Corporation Ltd • Singtel Optus Pty Ltd, and • Vodafone Hutchison Australia Pty Ltd.
Template	A model used for arranging information in a document. A template often forms the 'skeleton' of a document where users can input information into defined fields. Information can also be pre-filled into a template.

Term (and section of the Act)	***Description***
The **TIA Act**	*Telecommunications (Interception and Access) Act 1979*
Treaty	A treaty is an **international agreement** concluded in written form between two or more States (or international organisations) and is **governed by international law**. A treaty gives rise to international legal rights and obligations.
Typographical errors	A mistake in typed or printed text often caused by striking the wrong key on a keyboard.
Use and disclosure s 186A(1)(g)	Agencies must keep all documents and other materials which indicate the disclosure and use of information obtained under Chapter 4 of the TIA Act.
Use, communication, and recording s 151(1)(h)	Agencies must keep documents or other materials that indicate whether communicating, using, or recording of lawfully accessed information under Chapter 3 of the TIA Act complied with the prescribed requirements of the TIA Act. 'Communication' is the communication of the information outside the agency, 'use' is the use of the information inside the agency, and 'recording' is the recording of the information, for example by creating copies.
Verbal authorisation	We refer to verbal authorisations having been made where a disclosure of telecommunications data is made to an agency without a written or electronic authorisation signed by an authorised officer in place. This practice is **not** permitted under the TIA Act. There are no provisions under the TIA Act to make verbal authorisations even in urgent or out of hours situations. All authorisations for telecommunications data must be in writing or electronic form and signed by an authorised officer.

Appendix 2A – Stored Communications Inspection Criteria 2022-23

Objective: To determine the extent of compliance with Chapter 3 of the Telecommunications (Interception and Access) Act 1979 (the Act) by the agency and its officers
1. Has the agency properly applied the preservation notice provisions?
1.1 Did the agency properly apply for and give preservation notices?
Process checks • Does the agency have procedures in place for giving preservation notices, and are they sufficient? **Records checks in the following areas** *Domestic preservation notices*: – Whether the agency could give the type of domestic preservation notice given (s 107J(1)(a) of the Act)? – Whether the domestic preservation notice only requested preservation for a period permitted by s 107H(1)(b) of the Act? – Whether the domestic preservation notice only related to one person and/or one or more services (s 107H(3) of the Act)? – Whether the relevant conditions for giving a domestic preservation notice were met (s 107J(1) of the Act)? – Whether the domestic preservation notice was given by a person with the authority to do so (s 107M of the Act)? *Foreign preservation notices*: – Whether the foreign preservation notice only requested preservation for a permitted period (s 107N(1)(b) of the Act)? – Whether the foreign preservation notice only related to one person and/or one or more services (s 107N(2) of the Act)? – Whether the relevant conditions for giving a foreign preservation notice were met (s 107P of the Act)? – Whether the foreign preservation notice was given by a person with the authority to do so (s 107S of the Act)?
1.2 Did the agency revoke preservation notices when required?
Process checks – Does the agency have procedures in place for revoking preservation notices, and are they sufficient? **Records checks in the following areas** *Domestic preservation notices*: – Whether the domestic preservation notice was revoked in the relevant circumstances (s 107L of the Act)? – Whether the domestic preservation notice was revoked by a person with the authority to do so (s 107M of the Act)? *Foreign preservation notices*: – Whether the foreign preservation notice was revoked in the relevant circumstances (s 107R of the Act)? – Whether the foreign preservation notice was revoked by a person with the authority to do so (s 107S of the Act)?
2. Is the agency only dealing with lawfully accessed stored communications?
2.1 Were stored communications properly applied for?
Process checks – Does the agency have procedures in place to ensure that warrants are in the prescribed form (s 118(1) of the Act)? **Records checks in the following areas** – Whether the warrant was applied for by a person with the authority to do so (s 110(2) of the Act)? – Whether applications for stored communications warrants were made in accordance with ss 111 to 113 of the Act, or ss 111(2), 114 and 120(2) of the Act for telephone applications?

– Whether the facts and other grounds in the application made by the agency provided accurate and sufficient information for the issuing authority to make a fully informed decision (ss 113(2) and 116 of the Act)? – Whether the application was only in relation to one person (s 110(1) of the Act)? – If a warrant relates to the same person and the same telecommunications service as a previous warrant – whether the warrant was issued in accordance with s 119(5) of the Act? – Whether a connection can be established between the person listed on the warrant and the relevant telecommunications service (s 117 of the Act)?
2.2 Was the authority of the warrant properly exercised?
Process checks – Does the agency have effective procedures and authorisations in place to ensure the authority of the warrant is properly exercised? **Records checks in the following areas** – Whether the authority of the warrant was exercised in accordance with s 127 of the Act?
2.3 Did the agency revoke stored communications warrants when required?
Process checks – Where an agency becomes aware that the grounds on which a stored communications warrant was issued have ceased to exist, does the agency have processes in place to seek revocation of the warrant (s 122 of the Act)?
3. Has the agency properly received and managed accessed stored communications?
3.1 Were stored communications properly received by the agency?
Process checks – Does the agency have procedures and authorisations in place to properly receive accessed stored communications in the first instance? – Does the agency have secure storage (whether physical or electronic) for accessed information? **Records checks in the following areas** • Whether stored communications were received in accordance with s 135 of the Act?
3.2 Did the agency appropriately deal with accessed stored communications?
Process Checks • Does the agency have processes in place to accurately identify and manage any stored communications received outside the parameters of a warrant or accessed by the carrier after the warrant ceased to be in force? • Does the agency have controls, guidance and/or training in place around dealing with stored communications? **Records checks in the following areas** • Did the agency identify any stored communications received that did not appear to have been lawfully accessed? • Did the agency quarantine stored communications that did not appear to have been lawfully accessed? • Whether any use, communication or recording of lawfully accessed information has been accounted for in accordance with ss 139 – 146 of the Act?
3.3 Were stored communications properly dealt with and destroyed?
Process checks – Does the agency have procedures in place for the destruction of stored communications, and are they sufficient? **Records checks in the following areas** – Whether accessed stored communications were destroyed in accordance with s 150(1) of the Act?
4. Has the agency satisfied certain record keeping and reporting obligations?
Process checks • Does the agency have processes in place which enable it to accurately report to the Minister on the number of preservation notices given and warrants issued (s 159 of the Act)? • Did the agency have effective record-keeping practices in place (including keeping records regarding any use, communication or recording of lawfully accessed information)? **Records checks in the following areas**

• Whether the chief officer provided the Minister a written report, within three months after 30 June, that sets out the extent to which information and records were destroyed in accordance with s 150 of the Act (s 150(2) of the Act)? • Whether the agency has kept records in accordance with s 151 of the Act? • Whether the chief officer has provided an annual report to the Minister, within three months after 30 June, regarding applications and warrants (s 159 of the Act)?
5. Does the agency have a culture of compliance?
Process checks • Is there a culture of compliance? • Does the agency undertake regular training for officers exercising powers? • Does the agency provide support and appropriate guidance material for officers exercising powers? • Was the agency proactive in identifying compliance issues? • Did the agency disclose compliance issues to the Commonwealth Ombudsman's office? • Were issues identified at previous inspections addressed? • Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

Appendix 2B – Telecommunications Data Inspection Criteria 2022–23

Objective: To determine the extent of compliance with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (the Act) by the agency and its officers
1. Is the agency only dealing with lawfully obtained telecommunications data?
1.1 Were authorisations for telecommunications data properly applied for, given, and revoked?
Process checks • Does the agency have effective procedures in place to ensure that authorisations are properly applied for, and are they sufficient? • Does the agency have effective controls, guidance, and training in place for requesting and processing officers to ensure they have sufficient understanding of compliance obligations? • Does the agency have effective controls, guidance, and training in place for authorised officers to ensure that authorisations are properly given? • Does the agency have effective procedures in place to identify when prospective authorisations are no longer required and should be revoked, and to notify carriers of any revocations? **Records checks in the following areas** • Whether authorisations were in written or electronic form as required by the Act • Whether authorisations, notifications and revocations complied with the form and content requirements as determined by the Communications Access Coordinator (s 183(1)(f)) of the Act • Whether there is evidence of sufficient information before an authorised officer, prior to them making an authorisation, to enable them to properly consider the matters listed in s 180F of the Act • Whether authorisations were only made for information permitted by the Act, with consideration to s 172 of the Act • Whether authorised officers have demonstrated that they have considered matters listed under s 180F of the Act, and are satisfied, on reasonable grounds, that the privacy interference is justified and proportionate • Whether authorisations were made by officers authorised under s 5AB of the Act • Whether authorisations were made in relation to specified information or documents (ss 178 to 180 of the Act) • Whether prospective authorisations are in force only for a period permitted by s 180(6) of the Act • Whether prospective authorisations were revoked in relevant circumstances (s 180(7) of the Act)
1.2 Did the agency identify any telecommunications data that was not within the parameters of the authorisation?
Process checks • Does the agency have effective and consistent procedures in place to screen and quarantine telecommunications data it obtains? **Records checks in the following areas** • Whether telecommunications data obtained by the agency was within the parameters of the authorisation • Whether the agency identified any telecommunications data (including content) that did not appear to have been lawfully disclosed, and quarantined the data from use (and if appropriate, sought clarification from the carrier)
1.3 Were foreign authorisations properly applied for, given, extended, and revoked? (AFP)

Process checks

- Does the AFP have effective procedures in place to ensure that foreign authorisations are properly applied for, given, extended, and revoked, and are they sufficient?
- Did the AFP ensure that foreign authorisations were only made in relation to permitted information that was not content?

Records checks in the following areas

- Whether authorisations for telecommunications data on behalf of a foreign law enforcement agency were properly given and disclosed (ss 180A to 180E of the Act)
- Whether the Attorney-General made an authorisation before a prospective authorisation was made under s 180B of the Act
- Whether foreign prospective authorisations were properly revoked in accordance with s 180B(4) of the Act
- Whether extensions of foreign prospective authorisations were properly made in accordance with ss 180B(6) and (7) of the Act

2. Has the agency properly managed telecommunications data?

Process checks

- Does the agency have secure storage facilities for telecommunications data and associated information?
- Does the agency have procedures in place to limit access to telecommunications data that it has obtained?
- Does the agency have processes in place to account for the use and disclosure (and secondary use and disclosure) of telecommunications data?

Records checks in the following areas

- Whether the use and disclosure (and secondary use and disclosure) of telecommunications data can be accounted for in accordance with s 186A(1)(g) of the Act

3. Has the agency complied with journalist information warrant provisions?

3.1 Does the agency have effective procedures and controls to ensure that it is able to identify the circumstances where a journalist information warrant is required?

Process checks

- Does the agency have effective procedures and controls in place to identify the circumstances where a journalist information warrant may be required?

Records checks in the following areas

- Whether officers of the agency actively turned their minds to whether a request related to a journalist
- Whether officers of the agency kept sufficient records around a determination as to whether a request related to a journalist

3.2 Did the agency properly apply for journalist information warrants?

Process checks

- Does the agency have effective procedures and controls in place to ensure that a journalist information warrant is sought in every instance where one is required (s 180H) of the Act?
- Does the agency have effective procedures in place to ensure that journalist information warrants are properly applied for and issued in the prescribed form?

Records checks in the following areas

- Whether the application was made to a Part 4-1 issuing authority (s 180Q(1) of the Act)
- Whether the application related to a particular person (s 180Q(1) of the Act)
- Whether the application was made by a person listed under s 180Q(2) of the Act
- Whether the warrant was issued for a permitted purpose by s 180U(3) of the Act
- Whether the warrant was in the prescribed form and signed by the issuing authority (s 180U(1) of the Act)

3.3 Did the agency notify the Ombudsman of any journalist information warrants?

Records checks in the following areas

- Whether the Ombudsman was given a copy of each warrant issued to the agency as soon as practicable (s 185D(5) of the Act)
- Whether the Ombudsman was given a copy of each authorisation given under the authority of a journalist information warrant, as soon as practicable after the expiry of that warrant (s 185D(6) of the Act)

3.4 Did the agency revoke journalist information warrants when required?
Process checks • Does the agency have effective procedures in place to continuously review the need for a journalist information warrant? **Records checks in the following areas** • Whether the warrant was revoked in the relevant circumstances (s 180W of the Act) • Whether the revocation was in writing and signed by the chief officer or their delegate (s 180W of the Act)
4. Has the agency satisfied certain record-keeping and reporting obligations?

Process checks
• Does the agency have processes in place which enable it to accurately report to the Minister on the number of authorisations made and journalist information warrants issued, as well as all other matters listed under s 186 of the Act?
• Does the agency have effective record-keeping practices in place?
• Does the agency have effective record-keeping practices that sufficiently demonstrate compliance, including:
  ○ Records demonstrating an authorised officer's considerations of the matters listed ins 180F of the Act
  ○ Records to demonstrate compliant use and disclosure (and secondary use and disclosure)
Records checks in the following areas
• Whether the agency sent an annual report to the Minister on time, in accordance with s 186 of the Act and whether the report accurately reflected the agency's use of the Chapter 4 powers
• Whether the agency has kept records in accordance with s 186A of the Act
• Whether the agency retains all other relevant records to enable our Office to determine compliance, this may include training and guidance documents that are provided to requesting and authorising officers, records of data received or quarantined and file notes addressing discrepancies.

5. Does the agency have a culture of compliance?

Process checks
• Is there a culture of compliance?
• Does the agency undertake regular training for officers exercising Chapter 4 powers?
• Does the agency provide support and appropriate guidance material for officers exercising Chapter 4 powers?
• Was the agency proactive in identifying compliance issues?
• Did the agency disclose compliance issues to the Commonwealth Ombudsman's office?
• Were issues identified at previous inspections addressed?
• Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?
• Does the agency have processes to ensure compliance, including:
  ○ Quality control processes are supported by policy and practical guidance documents?
  ○ Effective procedures to measure compliance and identify and action issues as they arise?
  ○ Processes and training to identify and track issues that occur?
  ○ Protocols for advising relevant officers of issues that arise?

Appendix 2C – International Production Orders – Australian Designated Authority 'Health check' criteria 2021–22

Objective: To assess the 'health' of the Australian Designated Authority in establishing its compliance framework and to determine any current or future compliance risks with Schedule 1 of the *Telecommunications (Interception and Access) Act 1979*
Under cl 143 of Schedule 1 of the Telecommunications (Interception and Access) Act 1979 (the TIA Act), the Ombudsman may inspect the records of the Australian Designated Authority (ADA) to determine the extent of its compliance with Schedule 1 of the TIA Act (the Schedule). *This 'health check' will assess the readiness of the ADA's compliance framework against the criteria below, which is informed by the Australian Standard on Compliance Management Systems – Guidelines (AS ISO 19600:2015)*
Compliance preparedness
Organisational context
– Has the Attorney-General's Department (AGD) identified any external, or internal issues, especially those related to compliance risks, that affect its ability to establish processes for, and perform, the ADA function?
– Does AGD have a clear framework of policies and procedures that supports compliance with legislative obligations that arise from the ADA function, and has this framework been communicated to staff who exercise or are involved in the ADA functions?
– Are the ADA's functions or powers under the Schedule delegated within AGD in accordance with cl 179 of the Schedule? – If a delegation instrument is in place, are there procedures in place to mitigate compliance risks associated with organisational change?
Actions to address compliance risks
– Does the ADA have a risk register and risk management plan regarding compliance with the Schedule? – Has the AGD sought legal review of its policies and procedures for the use of the IPO powers and management of information received under IPOs to ensure its processes and systems are compliant with the Schedule and mitigate risk of non-compliance?
Compliance goals and planning to achieve them
– Has AGD established plans to ensure compliance with legal requirements in exercising the ADA function? – What are the outstanding actions, if any, to establish compliance plans and anticipated timeframes for implementation?
Support, training, and guidance
Resources
– **Has AGD developed a support, training, and guidance framework to implement its ADA function?** – What documentation has been, or will be, established by AGD to support its compliance with the Schedule? – Has the ADA identified and set up the necessary resources to manage its ADA function? – If resources are currently in development, what are the outstanding actions and anticipated timeframes for completion?
Competence and training

– Does AGD (or does AGD have an established plan to):
  ○ hold mandatory and periodic refresher training for officers delegated to exercise the ADA function?
  ○ engage with ADA delegates to advise on relevant issues/compliance concerns?
– If not established, what are the outstanding actions to establish a training plan and anticipated timeframes for implementation?

Awareness and communication
– How will the AGD ensure that ADA delegates maintain awareness of their roles and compliance responsibilities? – How will the ADA adequately communicate with relevant external stakeholders about its role and functions, and their development?
Operation preparedness
Operational planning
– Has the ADA established policies, procedures, and templates for giving international production orders (IPOs) in accordance with Part 5 of the Schedule? – Has the ADA established policies, procedures, and templates for processing the revocation of IPOs in accordance with Part 6 of the Schedule? – Has the ADA established policies, procedures, and templates for processing the cancellation of IPOs issued in response to telephone applications, where required action has not been taken, in accordance with Part 14 of the Schedule? – Has the ADA established policies, procedures, and templates for processing prescribed communications provider objections and, where applicable, cancelling IPOs in accordance with Part 7 of the Schedule? – Has AGD established policies and procedures for its ADA reporting and record-keeping requirements under Part 9 of the Schedule? – Has the ADA established policies, procedures, and templates for issuing evidentiary certificates in accordance with Part 12 of the Schedule? – Has the ADA established policies and procedures to store and manage protected information and ensure protected information is not used, recorded, disclosed, or admitted in evidence unless an exception applies under Part 11 of the Schedule? – Has AGD established policies and procedures for facilitating Ombudsman inspections under Part 10 of the Schedule? – Are the relevant standard operating procedures available to everyone involved in the exercise of the ADA's functions? – Where the above policies and procedures are not yet established, what are the outstanding actions and anticipated timeframes for implementation?
Establishing controls and procedures
– Does AGD have quality assurance and control measures established for its ADA function under the Schedule? – If applicable, has AGD established data management procedures (including vetting and quarantining when required) for electronic information received directly from prescribed communications providers? – Where quality assurance and control measures are not yet established, what are the outstanding actions and anticipated timeframes for implementation?
Performance evaluation and improvement
Monitoring, measurements, analysis, and evaluation
– Does AGD have systems in place for capturing and responding to internal and external feedback on ADA compliance performance? – How will AGD identify and manage emerging compliance issues?
Audit and management review
– Does AGD conduct, or intend to conduct, any form of internal audit or routine review of the ADA's compliance with the Schedule?
Non-compliance identification and corrective action
– Does AGD have systems and processes in place to identify and respond to compliance issues?
Continual improvement

- Does AGD have systems and processes in place to facilitate continual improvement of its ADA function under the Schedule?

Appendix 2D: Industry Assistance Inspection Criteria

Objective: To determine the extent of compliance with Part 15 of the *Telecommunications Act 1997* (the Act) by the agency and its officers (s 317ZRB[1])
1. Did the agency access industry assistance in accordance with the Act?
1.1 Were TARs given, varied, and revoked in accordance with the Act?
Process checks: Does the agency have effective procedures in place to ensure that TARs are properly given and varied? Does the agency have effective procedures in place to revoke TARs when required? **Records checks in the following areas:** Whether TARs were given by a person with the authority to do so (ss 317G, 317ZM and 317ZR) Whether TARs were given to a 'designated communications provider' (ss 317G and 317C) Whether form and content requirements were met (s 317H) Whether TARs were given for appropriate purposes (ss 317G, 317C and 317E) Whether key decision-making considerations were demonstrated (ss 317JAA and 317JC) Whether TARs were properly varied (s 317JA) Whether TARs were revoked when required (s 317JB)
1.2 Were TANs given, extended, varied, and revoked in accordance with the Act?
Process checks: Does the agency have effective procedures in place to ensure that TANs are properly given, extended, and varied? Does the agency have effective procedures in place to revoke TANs when required? **Records checks in the following areas:** Whether TANs were given by a person with the authority to do so (ss 317L, 317LA, 317ZM and 317ZR) Whether TANs were given to a 'designated communications provider' (ss 317L and 317C) Whether the provider was consulted before the TAN was given (s 317PA) Whether form and content requirements were met (s 317M) Whether TANs were given for appropriate purposes (ss317L, 317C and 317E) Whether State/Territory interception agencies obtained approval from the AFP Commissioner (s 317LA) Whether key decision-making considerations were demonstrated (ss 317P and 317RA) Whether TANs were properly extended (s 317MA) and/or varied (s 317Q) Whether TANs were revoked when required (s 317R)
1.3 Were TCN-related requests in accordance with the Act?
Process checks: Does the agency have processes in place to ensure TCN-related requests are made in accordance with the Act? **Records checks in the following areas:** Whether requests to the Attorney-General complied with any procedures and arrangements to be followed as determined by the Attorney-General (s 317S) Whether requests to the Attorney-General for a TCN outlined all relevant information (ss 317T, 317U, 317V and 317ZAA) Whether requests to the Attorney-General for variation of a TCN outlined all relevant information (ss 317X, 317XA and 317ZAA)
1.4 Were limitations adhered to?

Process checks:

Does the agency have processes in place to manage the key limitations to TARs, TANs and TCNs?

Records checks in the following areas:

Whether restrictions around systemic weaknesses or vulnerabilities were adhered to (s 317ZG)

Whether TCN limitations were considered in applications to the Attorney-General (s 317ZGA)

Whether relevant warrants or authorisations were in place for the assistance sought (s 317ZH)