COMMONWEALTH OMBUDSMAN

Ombudsman Oversight of Covert Electronic Surveillance

Report to the Attorney-General on agencies' compliance with the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997* from Commonwealth Ombudsman inspections conducted from 1 July 2023 to 30 June 2024.

Report by the Commonwealth Ombudsman, Iain Anderson, under section 186J and clause 150 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* and section 317ZRB of the *Telecommunications Act 1997*

December 2024

Contact us
Inquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman
Level 5, 14 Childers Street
Canberra ACT 2600
Tel: 1300 362 072
Email: ombudsman@ombudsman.gov.au

Contents

Abbreviations

Abbreviation	Term
ACT IC	Australian Capital Territory Integrity Commission
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
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 Commission Against Corruption
IPO	International Production Order
LECC	Law Enforcement Conduct Commission
NACC	National Anti-Corruption Commission
NSW CC	New South Wales Crime Commission
NSW CS	NSW Corrective Services
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police Force
QPS	Queensland Police Service
SA Police	South Australia Police
SC	Stored Communications
TCN	Technical Capability Notice
TAN	Technical Assistance Notice
TAR	Technical Assistance Request
TAS Police	Tasmania Police
TD	Telecommunications Data
VIC Police	Victoria Police
WA Police	Western Australia Police Force

Executive summary

The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) and the *Telecommunications Act 1997* (the Telecommunications Act) enable law enforcement agencies to apply for and use the following powers to covertly gather evidence through electronic surveillance by using the following specific powers.

Stored Communications – enables agencies to access communications that already exist and are stored in a telecommunication provider's system. This includes SMS, MMS, emails and voicemails.

Telecommunications Data – enables agencies to access what is commonly referred to as 'metadata'. It is information about electronic communications such as the date, time and duration of a communication but not the contents or substance of that communication.

International Production Orders – allows agencies to access telecommunication interceptions, data and stored communications from prescribed communications providers in a foreign country with whom Australia has a designated agreement.

Industry Assistance – enables interception agencies to request or compel a designated communication provider to give certain types of technical assistance.

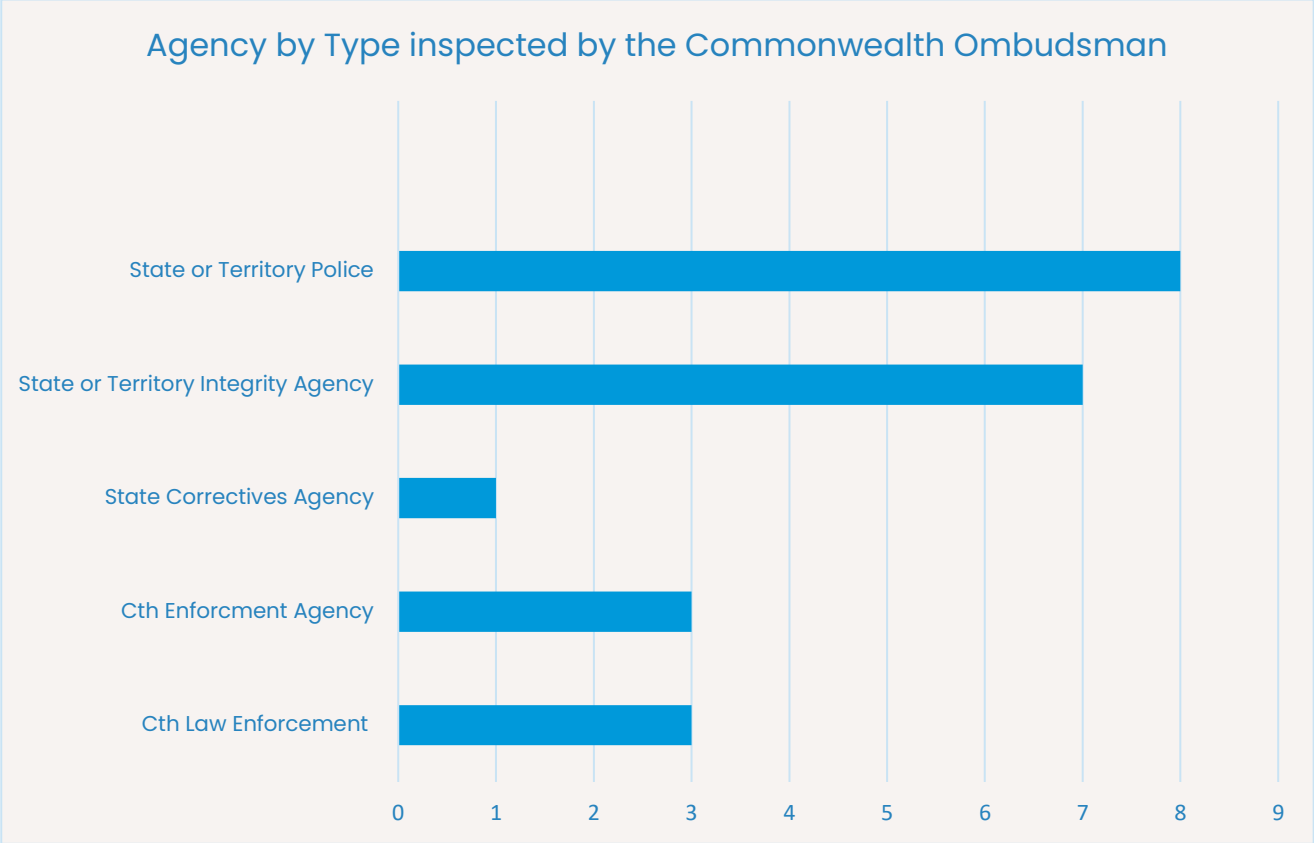
The Office of the Commonwealth Ombudsman's (our Office) oversight of law enforcement agencies' use of these powers is an important community safeguard, particularly because these powers are being used in a covert way. Between 1 July 2023 and 30 June 2024 (the inspection period), we conducted **54** inspections across **22** agencies and made **22** recommendations.

Overview of inspections

During the inspection period, we inspected:

- 22 agencies' access to telecommunications data under Chapter 4 of the TIA Act
- 20 agencies' access to stored communications under Chapter 3 of the TIA Act
- 6 agencies' readiness to use the IPO powers under Schedule 1 of the TIA Act, and
- 6 agencies' use of the industry assistance powers under the Telecommunications Act.

Chart 1: Types of agencies[1] we inspect under the TIA Act and Telecommunications Act



[1] A full list of the agencies inspected by the Commonwealth Ombudsman is within Appendix A.

Table 1: Inspection findings made for the last 3 inspection periods

Regime	Year	Recommendations	Suggestions
Stored Communications	2023-24	2	10
	2022-23	1	26
	2021-22	2	21
Telecommunications Data	2023-24	20	48
	2022-23	6	69
	2021-22	11	124
Industry Assistance	2023-24	0	6
	2022-23	0	7
	2021-22	0	12
International Production Orders	2023-24	0	0
	2022-23	-	-
	2021-22	0	0

State-based law enforcement agencies with high usages of the powers received most of our recommendations for improvement[2]. VIC Police and QPS each received 5 recommendations, NT Police received 4 recommendations[3], TAS Police received 2 recommendations and WA Police received one recommendation. The ACIC was the only Commonwealth agency we made recommendations to, comprising of 5 recommendations to improve internal safeguards when using prospective telecommunications data.

This report provides a summary of the most significant findings from these inspections and identifies matters that will assist agencies to improve their compliance with the legislation, such as the adequacy of their policies. A full list of the inspection recommendation outcomes can be found within Appendix A.

[2] NSW Police is a high usage agency but did not receive any recommendations during this period.
[3] One Recommendation was for both Stored Communications and Telecommunications Data and is therefore counted twice.

Common issues that agencies can improve on

We observed 2 reoccurring issues common to several agencies that used stored communications, telecommunications data and industry assistance powers.

Record keeping and demonstrating considerations when authorising the use of a power

Across several agencies and regimes, we continued to find instances of insufficient records being made to document each use of a power. This included requesting and authorising officers not adequately documenting the facts and circumstances relied upon to exercise the power or their considerations (including any impacts on privacy) when apply for or authorising the use of a power.

Lack of training and guidance materials

We found agencies that had insufficient guidance materials and training were at significant risk of non-compliance, with officers having limited understanding of their legislative obligations and the limitations of the relevant legislative framework.

Oversight of Covert Electronic Surveillance

Introduction

The TIA Act and the Telecommunications Act provide law enforcement agencies with a range of covert electronic surveillance powers. These include access to a person's stored communications and telecommunications data, or directing the activities of communications providers to assist law enforcement to perform a function or exercise a power to obtain information. They also enable law enforcement agencies to intercept communications or access stored communications, or telecommunications data, held by a communication provider in a foreign country with which Australia has an agreement with. 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 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 2023-2024 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.[4]

[4] Our Office also inspects and reports on Commonwealth law enforcement agencies' interception of telecommunications under Chapter 2 (Telecommunications Interception) of the TIA Act. The Ombudsman provides a report annually to the Attorney-General on our findings from our inspections, a summary of which is included in the Attorney-General's annual report on the TIA Act and not included in this report.

Scope and methodology

We conduct our inspections under the following sections within the TIA Act and the Telecommunications Act.

Telecommunications data and stored communications

Section 186B of the TIA Act requires the Ombudsman to inspect records of an agency to determine the extent of their compliance with Chapter 3 and Chapter 4 of the TIA Act.

Section 186J of the TIA Act requires the Ombudsman to provide an annual report to the Minister (the Attorney-General) with the results of each inspection conducted under section 186B during the reporting period.

International Production Orders

Under clause 142 of Schedule 1 (the International Production Orders Schedule) to the TIA Act, the Ombudsman may inspect records of a relevant agency to determine the extent of their compliance with the Schedule.

Clause 150 of Schedule 1 to the TIA Act requires the Ombudsman to provide an annual report to the Minister (the Attorney-General) with the results of inspections conducted under clause 142.

Industry Assistance

Under section 317ZRB of the Telecommunications Act, the Ombudsman may inspect the records of an interception agency to determine the extent of their compliance with Part 15 (Industry Assistance) of the Telecommunications Act and may make a report to the Minister (the Attorney-General) on the results of the inspection/s conducted under this section.

How we oversee agencies

We take a risk-based approach to our inspections. We focus on areas where agencies are, or may be, at risk of not complying with the legislative requirements or best practice standards, and where non-compliance would cause public harm.

Our inspections may include reviewing a selection of the agency's records, having discussions with relevant agency staff, reviewing policies and processes, and assessing any remedial action the agency has taken in response to issues we have previously identified with them.

We do not comment in this report on administrative issues or instances of non-compliance where the consequences are low risk and of minimal impact to the community.

Our inspections may identify a range of issues from minor administrative errors through to serious non-compliance that affects an individual's rights (notably privacy), the validity of evidence collected, or systemic issues. If an issue is sufficiently serious or systemic, or was previously identified and not resolved, we may make formal recommendations for remedial action. Where an issue of non-compliance is less serious and was not previously identified, we generally make suggestions to the agency to address the non-compliance and to encourage them to identify and implement practical solutions. We may also make suggestions or comments where we consider an agency's existing practice may expose it to compliance risks in the future.

To ensure procedural fairness, we give agencies the opportunity to respond to our inspection findings before consolidating the significant findings into this annual report to the Attorney-General.

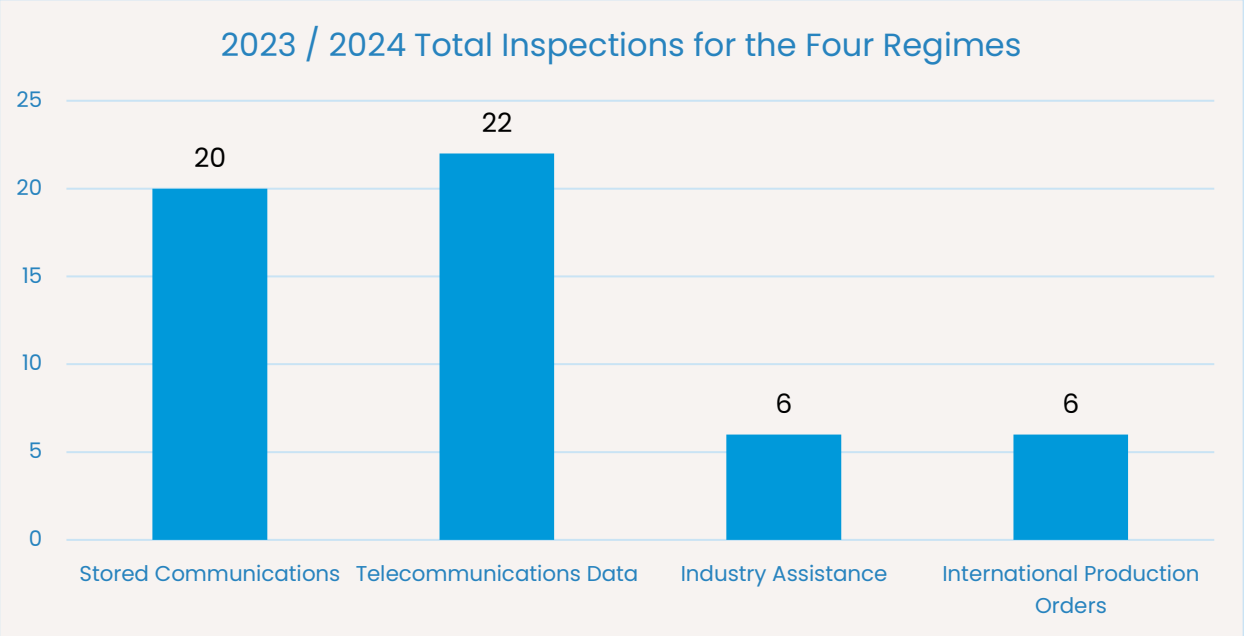
We follow up on any action agencies have taken to address our recommendations and suggestions at our next inspection.

Our Inspections

The requirement for our Office to inspect and report on an agency's use of the powers is different between the four legislated regimes. For example, we must inspect and report on an agency's use of Stored Communications and Telecommunications Data powers each year. The Ombudsman has the discretion to inspect an agency's use of Industry Assistance and International Production Order powers. In the case of IPO, if our Office conducts an inspection, then the Ombudsman must report on the inspection findings. The Ombudsman may elect to report on any findings made from inspections of an agency's use of Industry Assistance.

As such, not every agency was inspected across all four legislative regimes. While none of the agencies were granted the required certification to use IPO, we did complete 6 health check inspections of the agencies' operational readiness to use these powers.

Chart 2 - Total Inspections undertaken by the Commonwealth Ombudsman during 2023-24



Our key findings across the regimes

The 22 agencies using the powers engaged positively with our inspections and were receptive to our findings. We are pleased to find agency staff were open to our feedback and worked with our inspections staff in a full and frank manner. Disclosures of non-compliance by agencies were made quickly and transparently, often with a detailed explanation as to the remedies that were then put in place to mitigate and/or remedy the risks.

What can agencies improve on?

We observed 2 reoccurring issues common to several agencies that used stored communications, telecommunication data and industry assistance powers. As agencies had not yet commenced using IPO powers, we only noted areas of risk that agencies need to consider when preparing to use the powers under Schedule 1 of the TIA Act.

Record keeping and demonstrating considerations when authorising the use of a power

Records are key to our understanding of how decisions were made. Across several agencies[5] and regimes[6] we continued to find instances of insufficient records being made about each use of a power.

While we observed improvements across some agencies, we continued to discover records did not include key information to demonstrate why a power was used or what was considered at the time of authorising the use of that power. In particular, there were poor records of how authorising officers considered the necessity to apply the power and the impacts on privacy.

[5] This comment relates to ASIC, IBAC, NSW Police, QPS, VIC Police and TAS Police.
[6] Stored Communications, Telecommunications Data and Industry Assistance.

We understand that authorising officers may commonly be aware of background information relating to a particular investigation through information on systems, or through oral briefings. That said, we rely on the information provided on the records to demonstrate that the authorising officer has been presented with sufficient information to consider the legislative requirements and that they adequately turned their mind to these considerations prior to authorising the use of the power. This includes ensuring the power is being used for a purpose under the Act and that the necessary legislated threshold has been met.

Requests, applications and authorisations to use a power should include the considerations required in relation to the facts and circumstances of the applicable investigation. This includes:

- sufficient details to demonstrate the reason why the use of the power was necessary
- that it was reasonable and proportionate in the circumstances
- the applicable privacy considerations, which are unique to the circumstances in which the power is being used
- the reasons why the use of the power will assist in the investigation of an offence, enforcement of the criminal law or, if relevant, locating a missing person, and
- that the recorded details are accurate and factually correct.

Whilst check lists are helpful, requesting and authorising officers must still turn their minds to these considerations and record how they apply to the particular circumstances of a matter when requesting or authorising the use of a power.

Lack of training and guidance materials

Lack of guidance materials and training directly impacts on officers' understanding of their legislative obligations and the limitations of the relevant legislative framework.

We found that, particularly with respect to stored communications and telecommunications data powers, some agencies[7] had limited procedural guidance and training materials to adequately support officers in applying these powers appropriately or understanding their compliance obligations under the TIA Act, or had gaps in their guidance and training materials. In some agencies, staff rely on the knowledge of a limited number of experienced officers for guidance, with no continuity of support and consistency in the information being provided. We observed staff turnover in some agencies lead to a loss of corporate knowledge, which when combined with the absence of any formalised training, contributed to instances of serious non-compliance when using the powers.

We encourage agencies to provide adequate training and ensure clear guidance documentation is accessible to all officers using the powers. This improves decision-making and increases requesting and authorising officers' awareness of their legislated obligations.

Good practices

Collaboration and sharing knowledge on compliance practices

Several agencies[8] advised they had developed collaborative relationships with other agencies to discuss and share information on compliance practices and administration of the use of the powers. We observed staff within agencies were engaging with their peers across agencies to improve their collective knowledge of legislated requirements when using industry assistance and IPO powers. As these are both relatively new powers, it was encouraging to see the agencies working together to identify risks or obstacles with the use of the powers and developing potential solutions to ensure they were compliant with the legislation. This included ongoing collaboration between agencies to share policies, procedures, training and templates, which promoted compliance and consistency in the use of the powers, and developed robust governance frameworks.

[7] This comment relates to ASIC, IBAC, NT Police, NSWPF, QPS, SA ICAC, TAS Police and WA Police.
[8] This comment relates to LECC, NSW CC, NSW Police, NT Police, SA ICAC, SA Police, and VIC Police.

Engagement with our Office

A reliable marker of good compliance practices is the proactive engagement with our Office throughout the inspection period, rather than just during the on-site phase of our inspection.

Across all four regimes, we observed several agencies[9] who regularly approach our Office for advice on various compliance matters. This includes seeking guidance or our views on possible risks to compliance, options for mitigating these risks, disclosing instances of non-compliance, and examples of what we consider better practice looks like.

While an agency is responsible for ensuring it complies with law, it is encouraging to see agencies take a considered approach to maturing their compliance practices. Early engagement with our Office has assisted agencies self-initiate or improve their internal auditing and quality assurance mechanisms to demonstrate compliance with the law and proactively remediate instances of non-compliance.

[9] This comment relates to AFP, ADA, NACC, DHA, CCC (QLD), ASIC, NSW Police, VIC Police, IBAC, SA Police, WA Police and TAS Police.

Stored Communications

A stored communication is a communication that is held on equipment that is operated by and 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 short messaging service – text only
- MMS – multimedia messaging services – text, sound and images
- voicemails, and
- emails.

Due to the intrusive nature of accessing such information, 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).

Our Inspections

We inspected 20 agencies' access to stored communications under Chapter 3 of the TIA Act.

We made **2 recommendations** and **10 suggestions** across **6 agencies**.[10] The breakdown of the agencies and our findings is in Attachment A (Table 3A).

What we found

While we continued to see improvements across most agencies, we identified systemic non-compliance risks in 2 State-based police services.[11] We were pleased to see that most agencies were adequately managing risks to their compliance with Chapter 3 of the TIA Act.

Room to improve

We found 3 key areas of non-compliance in some agency practices requiring attention.

Failing to destroy stored communications forthwith[12]

If the chief officer of an agency is satisfied that stored communications information and records are not likely to be required for a purpose under the TIA Act, they must cause that material to be destroyed 'forthwith'. While the timeframe for forthwith is not defined by the TIA Act, we consider a timeframe of 14 days to be reasonable. However, we accept a timeframe of up to 28 days may be reasonable at some agencies.

We found instances across the AFP, SA Police and WA Police where the chief officers had authorised the destruction of stored communications information and records, but this material was not destroyed forthwith. In the case of the AFP and WA Police, the material was held for up to 42 and 43 days (respectively) before being destroyed. WA

[10] AFP, NT Police, SA Police, TAS Police, VIC Police and WA Police.
[11] This comment relates to NT Police and WA Police.
[12] This comment relates to the AFP, SA Police and WA Police.

Police's destruction policy stated that any record authorised for destruction must be disposed of within 14 days. The AFP had an internal timeframe of 1 month to dispose of any records authorised for destruction.

We also found instances where investigators had advised that they no longer required the stored communications for a purpose under the TIA Act, however there were significant lags between actioning this advice, authorising its destruction and ultimately disposing of the material. In the case of SA Police and WA Police, we identified instances where it took between 5 months and 1 year (respectively) for the investigators' request to be progressed to the chief officer's delegate to authorise its destruction.

Insufficient or inadequate training and guidance available to staff[13]

Having adequate training and guidance material available to staff mitigates risks of systemic and serious non-compliance with the TIA Act. For many agencies, stored communications powers are used infrequently, with officers relying on training and guidance material to navigate the use of the powers and understand their responsibilities under the TIA Act. This risk to non-compliance becomes significant in agencies where officers might rely on a small number of compliance staff to provide advice, or where attrition of experienced staff results in a loss of corporate knowledge.

We found several agencies did not have fit for purpose or formalised training and guidance material. In some cases, such as the AFP and TAS Police, specific parts of their training and procedures need to be updated to provide clarity to investigators when using the powers. By contrast, NT Police still did not have any formal training or procedures in place, despite our Office repeatedly raising our concerns over 5 years about the risks this lack of formal framework posed to their compliance with the TIA Act.

Preservation notices not being revoked[14]

Where an agency has issued a preservation notice to a carrier to preserve stored communications and no longer intends to obtain a warrant to access those stored communications, the agency must revoke the preservation notice and notify the

[13] This comment relates to AFP, NT Police and TAS Police.
[14] This comment relates to TAS Police and SA Police.

carrier. We observed instances in SA Police and TAS Police where investigators had not revoked a preservation notice after deciding not to progress a warrant to obtain any stored communications captured under that notice. In these instances, the preservation notice remained in place until it expired.

Investigators should continually assess the need to use or continue with a preservation notice for stored communications against the circumstances of their investigation. Failure to revoke a preservation notice when it is no longer required risks non-compliance with the mandatory revocation requirements under s 107L(2) of the TIA Act.

CASE STUDY

Incorrect provision on templates for preservation notices

During our inspection of the AFP, we found several notices used to preserve ongoing communications (an ongoing preservation notice) incorrectly referenced provisions that related only to preserving historic stored communications (being a historic preservation notice). A historic preservation notice preserves any stored communications that may exist on a carrier's system in relation to the service subject of the notice. An ongoing preservation notice preserves both these historical stored communications and any ongoing communications made by the service subject of the notice. An agency requires a warrant to access any stored communications that have been preserved by a carrier under a preservation notice.

The AFP amended its templates during our inspection to correct this error. However, we were concerned that the notices that incorrectly referenced the provisions to only preserve historic stored communications may affect any ongoing stored communications that were subsequently accessed under a warrant. We were also unaware of how long these templates had been in use and the extent of any impacted stored communications obtained by the AFP under an incorrect notice.

We suggested the AFP review and advise our Office of any risks and impacts from preservation notices issued with the incorrect provisions. We also suggested the AFP take immediate steps to quarantine and review the lawfulness of stored communications accessed in relation to these affected preservation notices.

The AFP accepted both of these suggestions and will report to us on how they have implemented them.

Good practices

Strong governance supports responsible use of stored communication powers

While some agencies can improve their training and guidance material, we noted overall improvements in agencies'[15] governance frameworks to support the use of stored communication powers. We observed a reduction in incidents of non-compliance in agencies that invested in continually enhancing their policies, guidance material and quality assurance processes.

Additionally, we found that compliance staff in most agencies proactively sought to identify and manage compliance risks and immediately remedy any instances of non-compliance. The staff were responsive to our feedback and agile in introducing any procedural improvements to address potential gaps in compliance.

CASE STUDY

Being responsive to fixing system errors leading to non-compliance

During the inspection of NSW Police's use of stored communications powers, we found several warrants that erroneously struck out templated wording that specified that they were for the victim of a serious contravention, even though the warrant was clearly in relation to obtaining the stored communications for a victim.

Section 118(1)(a) of the TIA act requires stored communications warrants to be in the 'prescribed form' and only redundant paragraphs of a stored communications warrant should be struck out. In this instance, where a stored communications warrant was in relation to a victim of a serious contravention, the wording should not have been struck out.

We found the error had occurred as a result of a newly implemented case management system which erroneously struck out this paragraph in all warrants by default. We raised this issue with NSW Police during the inspection, who took immediate action to rectify the errors and prevent it from reoccurring. Aside from this issue, we found the information on the records and the knowledge of the NSW Police staff to be of a high standard.

[15] This comment relates to ACT IC, CCC (QLD), DHA, and TAS Police.

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.

While we have jurisdiction over agencies using these powers, 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.). Under 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).

Telecommunications data requests are frequently a starting point of an investigation, allowing agencies to enforce the criminal law, investigate offences that attract a pecuniary penalty or locate missing persons.

During the inspection period we inspected 22 agencies. The highest user of the power was VIC Police compared to the lowest user, being NSW CS who used the power twice. State and Territory law enforcement agencies accounted for majority of all uses across both historic and prospective authorisations.

As an internally authorised power, it is incumbent on agencies to have sufficient controls and records to ensure the use of the powers is reasonably necessary, proportionate and justifiable. As telecommunications data does not relate to the content or substance of communications, it is not perceived to be as intrusive as warrant-based powers. However, the volume of data that may be accessed by enforcement agencies potentially impacts the privacy of far more people than just those who are the subject of the investigation.

Our Inspections

We inspected 22 agencies' access to telecommunications data under Chapter 4 of the Act.

We made **20 recommendations, 48 suggestions** across **14 agencies**.[16] The breakdown of the agencies and our findings in relation to them is in Appendix A (Table 4A).

[16] There were no findings made against ACCC, AFP, NSW ICAC, LECC, NACC, NSWCC, CCC (QLD) and CCC (WA) in this inspection period.

What we found

We found most of the agencies we inspected had a sound understanding of the legislated requirements to use the powers.

It is imperative the agency keeps sufficient records to demonstrate the necessity to access telecommunications data and requesting and authorising officers' considerations prior to authorising access to telecommunication data. Some agencies were lax or appeared to have become complacent with recording these reasons and considerations. In some agencies[17], the lack of detail routinely being recorded and accepted by requesting and authorising officers, along with the failure to remediate our previous findings with respect to record keeping, also indicated more systemic behaviours were contributing to the agency's non-compliance with the TIA Act.

Adherence to the legislative requirements, combined with responsible compliance practice, are key to an agency demonstrating a mature compliance culture, which in turn fosters public trust, minimises systemic non-compliance and mitigates reputational harm over time.

Room to improve

We found 5 key areas of non-compliance in some agency practices requiring immediate attention.

Insufficient action taken to address previous findings of systemic non-compliance

Where our recommendations or suggestions are implemented, we find the risk of systemic non-compliance is significantly reduced.

We found instances across several agencies where insufficient remedial action had been taken to mitigate previously identified risks of systemic non-compliance with the TIA Act.[18] While we acknowledge that it may take an agency several inspection periods

[17] This comment relates to IBAC, VIC Police and QPS.
[18] This comment relates to NT Police, SA ICAC, TAS Police and VIC Police.

to influence systems and behaviours contributing to non-compliance, 4 State-based police agencies[19] have not addressed our findings over several inspection periods.

For example, since our 2020-21 inspection we have recommended and suggested that TAS Police make changes to their systems to accurately record and report on authorisations to access historical telecommunications data. At our 2023-2024 inspection, we found that these changes had not been fully implemented, frustrating the ability for the compliance team in TAS Police to track and report on authorisations to access telecommunications data, quality assurance processes, support our inspection and produce accurate reports for the Minister. We recommended Tasmania Police develop enhancements to accurately identify, track and report on historic telecommunications data authorisations, including a solution that ensures each historic telecommunications data authorisation carries a unique and auditable reference number. TAS Police accepted this recommendation, and we will follow up on their progress at the next inspection.

Insufficient details recorded in requests to access telecommunications data and insufficient records of considerations made by authorising officers

We rely on records of requesting and authorising officers to assess whether an agency has used the powers to access telecommunications data for a purpose under the Act, and to assess whether the authorising officer has appropriately considered any interference to a person's privacy under s 180F of the TIA Act. This includes assessing whether the authorising officer has considered the relevance, usefulness, gravity, seriousness and the reason why the disclosure is to be authorised.

Irrespective of an authorising officer's prior knowledge of a matter, the requesting officer needs to ensure there is sufficient information in the request for the authorising officer to be satisfied of these conditions. Where the requesting officer has not included sufficient background information, authorising officers should refuse the application.

We found requesting officers at several agencies[20] included minimal information in their requests to adequately demonstrate a connection between the access to

[19] This comment relates to VIC Police, QPS, NT Police and TAS Police.
[20] This comment relates to ASIC, IBAC, NSW Police, QPS and VIC Police.

telecommunications data and the thresholds under the TIA Act. Additionally, the brevity of the information contained in the records inhibits the authorising officers from demonstrating they considered necessary requirements to assess the impacts on privacy under s 180F of the TIA Act.

The TIA Act requires that:

- for access to historic telecommunications data, access must be reasonably necessary to either enforce the criminal law, locate a missing person, or enforce a law imposing a pecuniary penalty or for the protection of public revenue[21]
- for access to prospective telecommunications data, access must be reasonably necessary for the investigation of a serious offence, being an offence with minimum penalty of 3 years imprisonment[22]
- the authorising officer must be satisfied on reasonable grounds that any interference with the privacy of any person is justifiable and proportionate, having regard to prescribed factors,[23] and
- an agency must keep records that demonstrate an authorisation was properly made including whether the authorised officer considered the matters referred to in s 180F of the Act.[24]

If agencies fail to demonstrate that these legislative requirements have been met in their records, we cannot assess compliance with the Act. For example, at VIC Police we found limited instances of authorising officers adequately recording their considerations in the records we inspected, with many authorisations stating 'approved' with no further commentary. This has been a repeat finding for VIC Police over several inspection periods. However, VIC Police demonstrated that they are making a concerted effort to rectify their systems, processes and guidance to authorising officers, and we hope to see improvements in the detail being captured in authorisation records during our next inspection.

---

[21] ss 178, 178A and 179 of the TIA Act.
[22] s 180 of the TIA Act.
[23] s 180F of the TIA Act.
[24] s 186A(1)(a)(i).

Access to telecommunications data for purposes not permitted by 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, 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 TIA 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. When accessing historical telecommunications data under s 178 of the TIA Act, the authorised officer must be satisfied that the access to the telecommunications data is reasonably necessary for the agency to enforce the criminal law.

We found instances of agencies making authorisations for purposes not provided for under the Act.[25] For example, at the Victorian Independent Broad-based Anti-corruption Commission (IBAC) we found multiple authorisations to access prospective data did not demonstrate that the disclosure of this telecommunications data was reasonably

[25] This comment relates to IBAC and SA Police.

necessary for the investigation of a serious offence. Similarly, we considered that several authorisations made by the IBAC did not demonstrate that access to historic telecommunications data was reasonably necessary for the enforcement of the criminal law. We recommended the IBAC review the records we identified and determine whether the relevant legislative thresholds were met to authorise the disclosure of prospective and/or historical data. We advised that if access to the data was not appropriate, then IBAC should take immediate steps to quarantine the data and assess the impact of any use or disclosure of the unlawfully obtained data. In response, the IBAC accepted our recommendation and reviewed the affected records. The IBAC advised that any telecommunications data that had been obtained under an authorisation that did not meet the threshold had been immediately quarantined. We will follow up the actions taken by the IBAC at our next inspection.

Improving internal safeguards to ensure the agency uses prospective telecommunications data within intelligence operations lawfully

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

At past inspections, we were satisfied that the information contained in requests to access prospective telecommunications data would be used for an investigative purpose. This inspection was the first time we compared the requests with the decisions and plans made by investigators and requesting officers for their intended use of prospective telecommunications data powers.

We found the ACIC had a robust governance and policy framework in place to allow officers to use these powers in connection with investigating a serious offence. However, in practice, we found planning documents and internal oversight were not fully effective.

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

During our inspection, we made some general observations which indicated the link with the threshold for being able to use prospective telecommunications data was not always clear. At the same time, we appreciate that the line which can distinguish between intelligence activities and the investigation of offences is also not necessarily clear. Accordingly, we have not yet concluded our view on whether the ACIC has been able to adequately demonstrate a connection between the use of prospective telecommunications data and the thresholds under the Act. We will explore this further at our next inspection.

We made 5 recommendations and 7 suggestions to improve the ACIC's internal safeguards to ensure prospective telecommunications data powers are used lawfully within intelligence operations.

In response, the ACIC accepted, or accepted in part, all of our recommendations and suggestions. The ACIC commenced activities to strengthen the internal safeguards supporting the use of relevant powers.

Lack of training and guidance to support requesting and authorising officers

To ensure that authorisations are properly applied for, given and revoked we consider system controls, regular training and guidance documents to be powerful mitigation against non-compliance. This is particularly the case where agencies might rely on a small number of compliance staff to vet authorisations, which means the agency is at risk of losing its corporate knowledge if those staff leave the agency. Instances of serious non-compliance observed at several agencies[26] were attributed to

[26] This finding relates to IBAC and SA ICAC.

inadequately managing the turnover of experienced officers and compliance staff, combined with limited or no formal training or guidance in the use of telecommunications data powers. This was a repeat finding for several agencies, with protracted inaction contributing to repeated serious or systemic non-compliance with the TIA Act.

CASE STUDY

Accessing data for a journalist's source without a warrant

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 Journalist Information Warrant (JIW) before authorising access to telecommunications data. The JIW provisions recognises the public interest in protecting journalistic sources.

During our inspection, NT Police disclosed they had accessed telecommunications data relating to a journalist and their source on 4 occasions. The unit accessing the data had not updated its templates, training or guidance material in response to the findings from our 2022-23 inspection.

We found that neither the requesting member, the authorising officer nor the intelligence analyst contemplated at the time whether a JIW was required. NT Police advised that the usual authorising officer was on leave and the need for a JIW was not considered by the substituting officer.

Since our 2019-2020 inspection, we have made findings each year relating to NT Police's lack of guidance and controls for JIWs, and failure to implement training for staff who exercise telecommunication data powers. We are of the view that the lack of guidance materials and mandatory training for authorising officers directly contributed to this non-compliance.

We recommended NT Police ensure all authorising officers complete mandatory training before exercising Chapter 4 powers. The training should place emphasis on maintaining compliance with s 180H (Journalist Information Warrants) of the Act. The NT Police accepted this recommendation and advised their training will be reviewed, updated and delivered to all authorising officers.

Good practices

We found 2 key areas where agencies demonstrated positive compliance practices.

Proactively reviewing the need to retain telecommunications data

Several agencies[27] have sought to destroy telecommunications data that is no longer required to be retained for a purpose under the TIA Act. While we are encouraged that these agencies are turning their minds to whether such data should continue to be retained, there are no provisions under the TIA Act for the destruction of telecommunications data. We have encouraged these agencies to work with the respective Commonwealth, State or Territory archiving authorities to lawfully dispose of data that is no longer required for a purpose under the TIA Act. We consider the proactive and regular review of telecommunications data, along with engagement with our Office, to be positive compliance practices.

Implementing internal quality assurance processes

We observed some agencies[28] proactively and routinely undertake internal quality assurance processes to ensure that accesses to telecommunications data are done in accordance with the TIA Act. We have observed these agencies readily make voluntary disclosures to our Office, use instances of non-compliance as learning opportunities for their staff, and can identify solutions to potential gaps or risks in their use of the powers.

While we acknowledge that human error can contribute to non-compliance, instigating these internal quality assurance process enables agencies to be better placed at identifying and remedying possible serious or systemic risks.

[27] This comment relates to AFP, LECC, NACC and IBAC.
[28] This comment relates to CCC (QLD), WAPOL and DHA.

CASE STUDY

Internal audit processes drive continuous compliance

Internal quality controls are an effective strategy to detect, prevent and effectively respond to non-compliance. Data-vetting and regular internal audits, combined with education where non-compliance is detected, drive continuous improvement in compliant use of the powers. It also assists agencies self-identifying solutions to limit re-occurrence of similar instances of non-compliance.

The Queensland Crime and Corruption Commission's introduction of monthly audits of telecommunications data authorisations has significantly reduced the number of instances of non-compliance. At our last inspection, we made no findings and observed that the authorisations were of a consistently high quality. We attribute this improvement to the combination of internal data-vetting practices and internal audits.

We commend the CCC (QLD)'s approach to continuous improvement in use of telecommunications data powers.

International Production Orders

The 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:

- an order relating to interception
- an order relating to accessing stored communications, and
- 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 AUS-US Data Access 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.

On 30 January 2024, Australia and the United States brought into force the AUS-US Data Access Agreement through a formal exchange of diplomatic notes. Agencies will now have the ability to apply for IPOs once they are certified by the ADA to do so.

In the current inspection period, no Australian agency we oversee had been certified to use an IPO under this agreement. As such, we continued to conduct Health Check Inspections on agencies, focussing on those we did not inspect in the 2022-23 inspection period.

Our Inspections

We conducted 6 health check inspections under clause 142 of the IPO Schedule, including the LECC, NSWCC, NT Police, QPS, SA Police and TAS Police. The purpose of these health check inspections was to assess the level of preparedness by each agency in relation to the development of their IPO framework.

We also used these health check inspections to engage with agencies and provide assistance or guidance where necessary.

What we found

We observed varied levels of preparedness amongst the 6 agencies. We noted that LECC and QPS had significantly progressed developing their procedural documentation which comprised of training resources, templates and policies.

Insufficient resourcing appeared to impact NSWCC, NT Police, SA Police and TAS Police capacity to dedicate effort towards progress their IPO framework. Although these agencies had not significantly progressed developing their policies and procedures, several demonstrated that they had plans in place to development their frameworks when they had available capacity.

Room to improve

We found 2 key areas in some agency practices requiring attention.

Finalising internal frameworks and certification to use IPO powers[29]

While several agencies had progressed developing their IPO framework, none of the 6 agencies had yet been certified by the ADA and were in a position to apply for an IPO. The LECC and QPS were both in the process of finalising draft policies and procedures to support complying with the IPO Schedule, and our feedback to them primarily focussed on administrative refinements and minor improvements to mitigate the risk of non-compliance. We expect both agencies will finalise their procedural guidance and training materials once certified and prior to using the IPO powers.

Insufficient resourcing of compliance areas to support developing IPO framework

Agencies with smaller compliance teams cited that they had insufficient resourcing to progress the development of their IPO framework.[30] This resourcing was being impacted by the support required to sustain effective compliance for other covert and intrusive powers being utilised by the agency.

For example, NT Police emphasised their priority was ensuring their compliance capabilities remained focussed on developing and administering effective policies and procedures for stored communications and telecommunications data powers, prior to commencing the development of an IPO framework. Similarly, NSWCC noted that resourcing was diverted from IPO development work to undertake system upgrades, which would also be required to support a sustainable IPO framework.

[29] This comment relates to LECC and QPS.
[30] This comment relates to NSW CC, NT Police, TAS Police and SA Police.

Good practices

We found 2 key areas where agencies demonstrated positive compliance practices.

Leveraging collaborative networks to improve IPO frameworks

We continued to observe collaborative practices between various agencies to progress IPO frameworks[31]. Inter-agency forums have been established, which agencies use as a centralised platform to collaborate and discuss potential and emerging issues. We identified that some agencies, who are more advanced with their IPO development, have assisted or are willing to share documentation. Several agencies noted that this joint approach to developing their IPO framework promotes consistency.

We found cross-agency engagement with the development of IPOs a positive practice, encouraging agencies to leverage off each other, whilst assisting with technical challenges and other aspects of the IPO framework.

Tailoring training and resources to support the use of IPOs[32]

It was evident from our inspections that LECC and QPS had dedicated considerable time and resources to establishing a fit-for-purpose IPO framework, including working towards appropriate and tailored training. These agencies advised they were developing tailored guidance for different areas in their agency utilising the IPO powers. We view this as responsible practice, allowing agencies to differentiate between the complexities and intricacies for each team involved in seeking and processing an IPO.

Both the LECC and QPS have adequately planned to ensure implementation of a suitable framework to support staff when using IPO powers. Recognising the amount of work this development entails, QPS have introduced planning and tracking mechanisms to oversee the progress of team's implementation activities. This provides a valuable resource to ensure QPS effectively coordinates effort.

---

[31] This finding relates to AFP, ADA, NSW Police, DHA, LECC, NSW CC, NT Police, QPS and SA Police.
[32] This finding relates to LECC and QPS.

CASE STUDY

IPO training resources

We reviewed a draft version of the LECC's internal training package. The LECC was the only agency who had commenced developing the necessary training resources to equip staff with the knowledge to exercise IPO powers during this period. The LECC intended for this training to be mandatory and periodic for all staff involved in the process. This training will consist of the ADA's training portal and an internal PowerPoint delivered to LECC staff. In addition to this, the LECC has drafted the IPO Standard Operating Procedures and Policies, which are detailed and contain practical guidance on how to use the LECC's systems for IPOs.

We reviewed the LECC's training materials and suggested amendments to clarify when to use an IPO in the context of the LECC's functions. We noted that it would be beneficial to include examples in the training that are relevant to the LECC's oversight and reflective of an investigation the LECC would undertake. The LECC was receptive to our feedback and amended the training accordingly.

Industry Assistance

The Industry Assistance (IA) 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 Communication 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 available to interception agencies, as defined in s 317B of the Telecommunications Act.[33]

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 warrants and authorisations required under the TIA Act, *Surveillance Devices Act 2004* (Cth) (the SD Act), or other State or Territory laws, but rather give assistance to an existing warrant and/or authorisation. The assistance provided by a DCP must not provide a new basis for interception. For example, if industry assistance was requested relating to a surveillance device,

[33] Agencies capable of using industry assistance include ACIC, AFP, NACC, NSW PF, VIC Police, QPS, WA Police, TAS Police, SA Police, NT Police, NSW ICAC, NSWCC, LECC, IBAC, CCC (QLD), SA ICAC and CCC (WA).

agencies would still require a warrant under the SD 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 that:

- a request or notice given to a DCP is reasonable and proportionate
- compliance with the request or notice is practicable and technically feasible
- the agency is not requiring or requesting the DCP to implement or build in a systemic weakness, and
- 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.

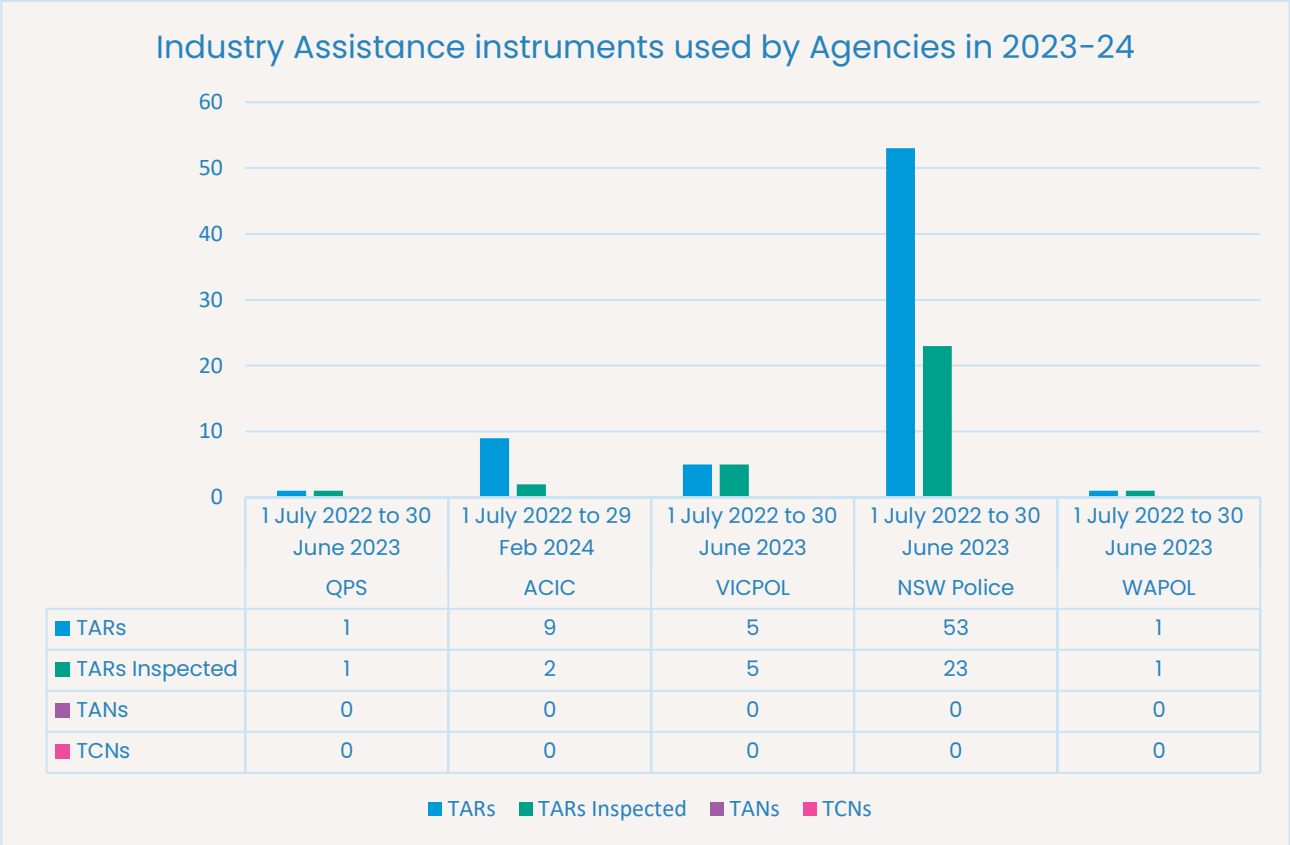
Our inspections

We inspected 6 agencies' use of the industry assistance powers, including the ACIC, AFP, NSW Police, VIC Police, QPS and WA Police. We made no recommendations and made 6 suggestions to address minor non-compliance or administrative errors. The breakdown of the agencies and our findings in relation to them is in Attachment A (Table 6A).

What we found

Industry Assistance is a relatively new power and not all agencies have actively pursued using the powers as part of their operational activities. NSW Police is the most frequent user of the power, accounting for 53 of the 69 TARs issued in 2023-24.

Chart 3 – Breakdown of the use of the Industry Assistance instruments for 2023-24



	1 July 2022 to 30 June 2023 QPS	1 July 2022 to 29 Feb 2024 ACIC	1 July 2022 to 30 June 2023 VICPOL	1 July 2022 to 30 June 2023 NSW Police	1 July 2022 to 30 June 2023 WAPOL
TARs	1	9	5	53	1
TARs Inspected	1	2	5	23	1
TANs	0	0	0	0	0
TCNs	0	0	0	0	0

During our inspections we observed instances where TARs were issued by agencies to DCPs to provide the same type of assistance, each in a different manner (i.e. we found that the listed acts or things requested under 317E of the Telecommunications Act to achieve the same effect varied between agencies). This may be because there are prohibitions on agencies communicating industry assistance information and outcomes under the Act, so they do not necessarily have visibility of the requests that are being made to DCPs. Section 317ZF of the Telecommunications Act states that unauthorised disclosure of information about, or obtained under, an industry assistance instrument is an offence.

We also observed some TARS with long validity periods. Section 317J of the Telecommunications Act states that, once issued, a TAR remains in force for 90 days, unless a specific expiry date is listed, or it is revoked. Section 317JB of the Telecommunications Act states that decision-makers must revoke a TAR if satisfied that any ongoing requirements are no longer reasonable, proportionate, practical or technically feasible. With this in mind, we monitor the use of TARs with long validity

periods (i.e., over 90 days). We found that TARs with long validity periods are often issued to support the execution of warrants or authorisations not yet issued. During our inspections, we were satisfied that the thresholds to use the powers for long periods were being met and the periods for the TARs we inspected were valid. We will continue to monitor TARs with long validity periods at future inspections.

Room to improve

We observed 3 areas in some agency practices requiring attention.

Authorising officers not adequately recording their considerations[34]

Before issuing a TAR, s 317JAA(4) of the Telecommunications Act requires the chief officer (or delegate) to be satisfied that:

- the request is reasonable and proportionate, and
- compliance with the request is practicable and technically feasible.

In determining that a TAR is reasonable and proportionate, the chief officer must also turn their mind to 9 specific considerations at s 317JC(a)-(i) of the Telecommunications Act.

We found that NSW Police did not adequately demonstrate that authorised officers had turned their mind to the reasonableness or proportionality of a request to a DCP before issuing a TAR. Instead of recording their own considerations, authorising officers were adopting the considerations of requesting officers by way of signing and dating applications. We noted that the applications also contained pre-ticked check boxes that purportedly demonstrated that authorised officers had considered the matters required by s 317JC(a)-(i) of the Telecommunications Act.

The authorisation of a TAR is a discretionary decision that requires the authorising officer to demonstrate that they have turned their mind to specific considerations when making the decision to issue the TAR. We do not consider endorsing pre-populated

[34] This comment relates only to NSW Police.

considerations or templated wording adequately demonstrates the authorising officer has considered the requirements under ss 317JAA and 317JC of the Telecommunications Act before making the decision to issue a TAR. Records should reflect that the authorised officer has been presented with sufficient information to consider these requirements and demonstrate that the authorised officer has turned their mind to these considerations before issuing the TAR.

We suggested NSW Police immediately amend its forms to ensure authorising officers adequately demonstrate and record their considerations under s 317JC of the Telecommunications Act.

Although NSW Police recognise that the authorising officer must give genuine consideration to every criterion required by the legislation before issuing a request, the agency had a different view of how the considerations are required to be recorded. Despite the difference in position, NSW Police advised they enhanced their forms to strengthen how authorising officers demonstrate their considerations.

Issuing TARs when no assistance was required[35]

Under s 317ZH(1)(a) of the Telecommunications Act, requesting DCP assistance through a TAR when a warrant or authorisation could be issued to achieve the same objective may render the TAR ineffective. The purpose of the industry assistance framework is to assist agencies in performing and exercising their existing statutory functions and powers. If, for example, the information requested is of a kind that can be disclosed under a telecommunications data authorisation, and the DCP is capable of providing the requested information, it should be provided under the authority of that authorisation because there is no need for the TAR. Section 317JC also says that the chief officer of an interception agency must not give a TAR unless satisfied the request is reasonable and proportionate by considering certain matters, including the availability of other means to achieve the objectives of the request and whether the request is necessary.

At QPS, we identified an instance where although the agency was aware a DCP had developed a capability to lawfully provide access to information through a non-

[35] This comment relates to AFP and QPS.

industry assistance authorisation or warrant instrument, QPS issued a TAR to access the capability. We suggested QPS ensure they have considered and recorded whether there are any other means of obtaining the information before issuing an industry assistance instrument - including whether the industry assistance instrument is necessary. QPS advised that our suggestion would be fully implemented.

Reviewing the feasibility, necessity, proportionality and reasonableness of TARs[36]

As outlined above, under the Telecommunications Act, if a TAR is given by the chief officer of an interception agency and they are satisfied that the request is not reasonable and proportionate or compliance with the request is not practicable and technically feasible, the chief officer must revoke the TAR.

At QPS, a TAR was given with an extended validity period of up to 12 months to enable the execution of a warrant or authorisation, as the need arose. At the time of our inspection, and several months after the TAR was given, only one request had been made under the industry assistance instrument and QPS could not foresee that a future request was likely. Given the limited use of the TAR, we were concerned about the ongoing feasibility, necessity, proportionality and reasonableness of the TAR. We suggested that QPS internal guidance should be updated to ensure internal reviews of TARs with prolong validity periods are reviewed at 6-month intervals. QPS accepted our suggestion.

CASE STUDY

Considering alternate means of achieving an objective

During our inspection of the AFP, we were advised that in response to a request from a DCP, the agency was considering issuing a TAR to enable access to telecommunications data through an existing capability held by the DCP. We understand the capability was developed through the previous use of industry assistance powers.

[36] This comment relates only to QPS.

Before authorising a TAR, the chief officer of an interception agency must have regard to the availability of other means to achieve the objectives of the request.

We raised concerns that the grounds for the TAR to be reasonable and proportionate under s 317JC of the Telecommunications Act were unlikely to exist as the data could be obtained using other means, and the use of a TAR in this circumstance would therefore be unnecessary.

The AFP accepted our comment and did not proceed with the TAR, as the considerations set out in s 317JC of the Telecommunications Act could not be satisfied.

Good practices

We found 2 key areas where agencies demonstrated positive compliance practices.

Regular reviews of current and proposed industry assistance

The Telecommunications Act imposes restrictions, limitations and requirements for interception agencies using industry assistance powers in relation to notifications, communication and disclosure of industry assistance information.

At NSW Police, we were pleased to see weekly meetings where both proposed and current authorisations were discussed and reviewed. NSW Police advised the meetings included legislated considerations of reasonableness, proportionality and feasibility of industry assistance instruments and reviews against revocation criteria.

This process serves as both a legislative control point and a reminder for officers of their compliance requirements when using the powers.

Policies, procedures and guidance

Having approved and accessible guidance material and training available to applicants and authorising officers significantly reduces the risks of non-compliance.

We were pleased to observe agencies[37] proactively assessing and improving policies and procedures with respect to the use of industry assistance powers. For example, we observed:

- the AFP revised its guidance documents and presented draft versions for review at our inspection
- at WA Police, formal guidance and training for officers on the industry assistance powers was in the process of finalisation, but we were pleased to see the proactiveness of the WA Police in revising and improving training despite having low use of the powers, and
- at QPS, policy documents clearly outlining the process for obtaining a TAR or TAN, the approval processes for a TAR, TAN or TCN, and the decision-making thresholds and circumstances for varying, extending or revoking a TAR or TAN.

Similarly to WA Police, we noted that QPS's use of the industry assistance powers to date has been minimal and infrequent. QPS had developed thorough governance arrangements and processes for applying for industry assistance. However , we queried whether the level of training, guidance, review and quality assurance that went into the approval of one TAR could be maintained if the powers were used more frequently and/or involved additional approving officers.

[37] This comment also relates to AFP, WA Police and QPS.

Appendix A

Our Recommendations

During the inspection period, 24 recommendations were made across 7[38] agencies within 2[39] regimes.

Table 1A – All recommendations made during 2023-24 inspection period

Stored Communications

	Agency	Findings	Agency Response
1	WA Police	**Stored Communications material not being destroyed 'forthwith' in accordance with the Act.** **Recommendation:** That WA Police ensure that authorised destructions are undertaken 'forthwith' in accordance with s 150(1) of the Act. The Agency had an internal benchmark of 14 days that was not being adhered to, noting the agencies also took longer than the timeframe both our office and the Attorney	Recommendation has been accepted

[38] ACIC, IBAC, NT Police, QLD Police, TAS Police, VIC Police, WA Police.
[39] Stored Communications (2 recommendations) & Telecommunications Data (22 recommendations).

		General considers meeting the threshold of 'forthwith' being within 28 days.	
2	NT Police	**Insufficient action undertaken by the Law Enforcement Agency to complete its compliance framework for using Chapter 3.** **Recommendation:** Within 6 months, NT Police prioritise and resource finalising its compliance framework (including delivery of the Standard Operating Procedure and supporting training) for managing the powers under Chapters 3 of the Act. For the last five years we have made repeat findings that the agency did not have Standard Operation Procedures (SOP) or guidance and training material to ensure officers apply Chapter 3 powers appropriately and understand their compliance obligations under the Act. This presents significant risks to complying with the Act. Staff rely on a limited number of experienced staff for guidance and there is no continuity of support for staff and consistency in the advice being provided.	Recommendation has been accepted

Telecommunications Data

	Agency	Findings	Agency Response
1	NT Police	**Insufficient action undertaken by the Law Enforcement Agency to complete its compliance framework for using Chapter 4.** **Recommendation:** Within 6 months, NT Police prioritise and resource finalising its compliance framework (including delivery of the Standard Operating Procedure and supporting training) for managing the powers under Chapters 4 of the Act. For the last five years we have made repeat findings that the agency did not have SOPs or guidance and training material to ensure officers apply Chapter 4 powers appropriately and understand their compliance obligations under the Act. This presents significant risks to complying with the Act. Staff rely on a limited number of experienced staff for guidance and there is no continuity of support for staff and consistency in the advice being provided.	Recommendation has been accepted
2	NT Police	**A Law Enforcement Agency accessed telecommunications data relating to a journalist and their source without the requesting and authorising officer considering the requirement for a Journalist Information Warrant (JIW).** **Recommendation:** That NT Police ensure all authorising officers complete mandatory training before exercising Chapter 4 powers. The training should place emphasis on maintaining compliance with s 180H of the Act.	Recommendation has been accepted

	Agency	Findings	Agency Response
3	NT Police	**There was no settled process to extract and report telecommunications data authorisations to the Minister, resulting in repeat instances of inaccurate numbers being provided in Ministerial reporting (repeat finding).** **Recommendation:** NT Police should implement a consistent process of recording and reporting telecommunications data authorisations to the Minister.	Recommendation has been accepted
4	TAS Police	**Deficiencies in ATLAS means Tasmania Police cannot adequately demonstrate it has complied with Chapter 4 of the TIA Act in relation to historic TD authorisations.** **Recommendation:** That TAS Police develop enhancements to ATLAS or an analytical tool(s) to accurately identify, track and report on historic TD authorisations, including a solution that ensures each historic TD authorisation carries a unique and auditable reference number.	Recommendation has been accepted
5	TAS Police	**Incorrectly reporting the number of TD authorisations made to the Commonwealth Attorney-General.** **Recommendation:** TAS Police advise the Attorney-General's Department of the inaccuracies in its Ministerial reporting over the previous 3 reporting periods as a result of counting authorisations incorrectly. In certain circumstances, an authorising officer may authorise a TD disclosure for several different service numbers under a single authorisation, providing the relevant privacy considerations are made. We found TAS Police have been reporting each service number included under a single authorisation as separate authorisations in their annual report to the Minister. For example, when 20	Recommendation has been accepted

	Agency	Findings	Agency Response
		numbers have been authorised in relation to one Integrated Public Number Database (IPND) request, this has been captured as 20 authorisations, rather than one authorisation. The Attorney-General's Department have confirmed with our Office that agencies should only report on authorisations at the investigation level, and that where an agency makes a single authorisation for the disclosure of multiple sources of information, only that single authorisation should be reported.	
6	IBAC	**Prospective authorisations did not demonstrate the disclosure was reasonably necessary for the investigation of a serious offence.** **Recommendation:** The Independent Broad Based Anti-corruption Commission review the records identified and determine whether the relevant legislative thresholds were met to authorise the disclosure of prospective and/or historical data. If access to the data was not appropriate, IBAC should take immediate steps to quarantine the data and assess the impact of any use or disclosure of the unlawfully obtained data. We found several prospective telecommunication data applications and authorisations that did not demonstrate that the disclosure was reasonably necessary for the investigation of a serious offence or an offence that is punishable by at least 3 years imprisonment.	Recommendation has been accepted
7	QPS	**Authorising officers did not adequately record their considerations when authorising access to historic telecommunications date – repeat finding.** **Recommendation:** QLD Police implement processes to ensure requesting officers and authorising officers	Recommendation has been accepted

	Agency	Findings	Agency Response
		consistently document their considerations when making a historic TD authorisation under Chapter 4 of the Act. This includes: • how the service number is known to be used by or directly linked to the Person of interest and enforcement of the criminal law • the relevance of the volume and type of data proposed to be disclosed, and • why the disclosure is reasonably necessary.	
8	QPS	**Significant delays were discovered between the making of a historic Telecommunications Data authorisation and when it was sent to the telecommunication carrier – repeat finding.** **Recommendation:** Queensland Police should not process historic Telecommunications Data request after 14 days without verifying the considerations under s 180F of the Act remain valid, consistent with Queensland Police's published guidelines. Queensland Police should also ensure the provisions under s 180F are reconsidered and recorded on any requests taking more than 14 days to process.	Recommendation has been accepted
9	QPS	**The agency had not taken sufficient action to assess and mitigate the risks of unauthorised disclosure of TD to external agencies with direct access to QPrime (repeat finding).** **Recommendation:** As a matter of priority, Queensland Police establish which agencies have direct access to QPrime and Chapter 4 authorisation information or TD protected under s181B and 182 of the Act. Queensland Police implement measures to ensure: • any accesses by external agencies that would constitute disclosure under the Act only take place in circumstances provided for in the Act, and	Recommendation has been accepted

	Agency	Findings	Agency Response
		• appropriate records are kept demonstrating this.	
10	QPS	**Discrepancies in the Agency's annual reporting to the Minister of Telecommunication Data authorisations (repeat finding).** **Recommendation:** Queensland Police prioritise enhancements to QPrime to ensure that annual reports to the Minister are reported accurately.	Recommendation will be prioritised and acted upon as soon as practical.
11-15	ACIC	**Internal safeguards should be improved to ensure the agency's use covert powers within Special Operations** **Recommendation:** The ACIC review its framework of governance, policies and procedures to ensure that staff do not use covert powers for intelligence purposes that would not meet legislative thresholds. **Recommendation:** If an intelligence operation uses the powers, the ACIC ensure that it can demonstrate that the deliverables from the operation include an investigative purpose. **Recommendation:** The ACIC Operations Strategy Forum must ensure any extensions to an Intelligence Operation expressly include the approval to continue using the powers. **Recommendation:** ACIC should review and, where necessary, update its training to ensure staff are aware of and understand the boundaries of the lawful purposes for which the powers can be used. **Recommendation:** The ACIC implement measures to ensure that it can demonstrate that the powers (except access to historical TD) are used within a continuum of	Recommendation has been accepted Recommendation has been partly accepted Recommendation accepted Recommendation accepted

	Agency	Findings	Agency Response
		investigating and prosecuting a serious offence. This should include reviewing how the ACIC records its use of the powers, and supports partner agencies enforcement, investigative and criminal or civil proceedings.	Recommendation has been partly accepted
16-18	VIC Police	**Record keeping: Requesting officers did not record sufficient information in applications for prospective and historic telecommunications data for authorising officers to make considered decisions. Authorising officers did not adequately record their considerations when authorising access to historic and prospective telecommunication data, including insufficiently demonstrating that they had turned their mind to the privacy considerations under s180F of the Act** **and** **Requesting and authorising officers are not exercising due diligence in ensuring applications and authorisations for prospective and historic telecommunications data contain factually correct information** **and** **Authorisation to access prospective TD dd not demonstrate consideration of the increased privacy impacts when members varied the frequency of a Location Based (LBS) 'ping' post authorisation.** **Recommendation:** Victoria Police implement processes to ensure authorised officers consistently and accurately document any information relevant to considering and making a telecommunications data authorisation under Chapter 4 of the Act. This includes demonstrating the	Recommendation has been accepted

	Agency	Findings	Agency Response
		authorised officer took into account all relevant matters, in line with s 180F of the Act, and that the record-keeping requirements under ss 186A(1)(a)(i) of the Act are met. A report on how this recommendation has been effectively implemented should be provided to the Ombudsman by 1 April 2025. **Recommendation:** Victoria Police ensure that all historic and prospective telecommunication data authorisations and disclosures under Chapter 4 of the Act are made for the purposes expressly under the Act. A report on how this recommendation has been effectively implemented should be provided to the Ombudsman by 11 April 2025. **Recommendation:** Victoria Police implement mandatory training for Requesting Officers who seek to access Telecommunication Data under Chapter 4 of the Act, including guidance on: • ensuring requests contain sufficient background and justification to enable an Authorising Officer to make the necessary considerations under s 180F of the Act • providing adequate explanation as to how access to telecommunication data is reasonably necessary for either (for historic TD) enforcement of the criminal law or (for prospective TD) the investigation of a serious offence.	Recommendation has been accepted Recommendation has been accepted
19	VIC Police	**Access to TD made by Special Projects Intelligence Data Analysis Section (SPIDAS) were outside of Victoria Police process and did not providing adequate information to support the request and authorisations to access TD .** **Recommendation:** Victoria Police ensure that any requests and authorisations under Chapter 4 of the Act made and processed outside of Victoria Police's RMSWeb system apply a consistent process, templates and authorising framework, and ensure requesting and	Recommendation has been accepted

	Agency	Findings	Agency Response
		authorising officers records are comprehensive, adequate, accurate and retrievable.	
20	VIC Police	**The Chief Commissioner has not updated the Delegation Instrument authorising PSC to use Chapter 4 since 2015.** **Recommendation:** Victoria Police Chief Commissioner immediately consider the updated delegation instrument under section 5AB(1) of the Act.	Recommendation has been accepted

Table 2A - Overall Findings across the Regimes and Agencies

Agency	Regime	Rec	Sug	Outcome[40]
ACT IC	SC	0	0	Health Check Completed
	TD	0	1	Health Check Completed
ACCC	SC	0	0	Inspection Survey Completed
	TD	0	0	Report Completed
ACIC	SC	0	0	Report Completed
	TD	5	7	Report Completed
	IA	0	0	Report Completed
AFP	SC	0	4	Report Completed
	TD	0	0	Report Completed
	IA	0	0	Report Completed
ASIC	SC	0	0	Inspection Survey Completed
	TD	0	3	Report Completed
CCC (QLD)	SC	0	0	Findings Letter Completed
	TD	0	0	Report Completed
CCC (WA)	SC	0	0	Inspection Survey Completed
	TD	0	0	Report Completed

[40] A Health Check is completed for agencies that have yet to use or have very limited use of a power. An Inspection Survey is completed for agencies that are deemed low risk or have not used a power. A Findings Letter is completed where no areas of concern are revealed during an inspection. A Report is completed when findings have been made.

Agency	Regime	Rec	Sug	Outcome[40]
DHA	SC	0	0	Findings letter Completed
	TD	0	4	Report Completed
IBAC	SC	0	0	Inspection Survey Completed
	TD	1	3	Report Completed
ICAC (NSW)	SC	0	0	Findings Letter Completed
	TD	0	0	Report Completed
ICAC (SA)	SC	0	0	Inspection Survey Completed
	TD	0	3	Report Completed
LECC	SC	0	0	Findings Letter Completed
	TD	0	0	Report Completed
	IPO	0	0	Health Check Completed
NACC	SC	0	0	Findings letter Completed
	TD	0	0	Report Completed
NSW CS	TD	0	1	Report Completed
NSW CC	SC	0	0	Inspection Survey Completed
	TD	0	0	Report Completed
	IPO	0	0	Health Check Completed
NSWPF	SC	0	0	Report Completed
	TD	0	3	Report Completed
	IA	0	2	Report Completed
NT Police[41]	SC	1	1	Report Completed
	TD	3	3	Report Completed
	IPO	0	0	Health Check Completed
QPS	SC	0	0	Report Completed
	TD	4	6	Report Completed
	IA	0	4	Report Completed
	IPO	0	0	Health Check Completed
SA Police	SC	0	1	Report Completed
	TD	0	2	Report Completed
	IPO	0	0	Health Check Completed
TAS Police	SC	0	2	Report Completed
	TD	2	5	Report Completed
	IPO	0	0	Health Check Completed
VIC Police	SC	0	1	Report Completed
	TD	5	4	Report Completed

[41] One Recommendation was for both Stored Communications and Telecommunications Data and is therefore counted twice.

Agency	Regime	Rec	Sug	Outcome[40]
	IA	0	0	Report Completed
WA Police	SC	1	1	Report Completed
	TD	0	3	Report Completed
	IA	0	0	Report Completed
Totals		**22**	**64**	

Table 3A – Stored Communications detailed findings

Agency	Recommendations		Suggestions	
	2022-23	**2023-24**	**2022-23**	**2023-24**
ACT IC	N/A[42]	0	N/A	0
ACCC	0	0	0	0
ACIC	*[43]	0	*	0
NACC	0	0	0	0
AFP	0	0	1	4
CCC (QLD)	0	0	0	0
CCC (WA)	0	0	0	0
DHA	*	0	*	0
IBAC	0	0	2	0
ICAC (NSW)	0	0	0	0
ICAC (SA)	0	0	0	0
LECC	0	0	6	0
NSW CC	0	0	0	0
NSW Police	0	0	2	0
NT Police	1	1	8	1
QPS	0	0	0	0
SA Police	0	0	1	1
TAS Police	0	0	4	2
VIC Police	0	0	0	1

[42] ACT IC did not have permission to use the power.

[43] * not inspected.

Agency	Recommendations		Suggestions	
	2022-23	2023-24	2022-23	2023-24
WA Police	0	1	2	1
TOTAL:	**1**	**2**	**26**	**10**

Table 4A – Telecommunications Data detailed findings

Agency	Recommendations		Suggestions	
	2022-23	2023-24	2022-23	2023-24
ACT IC	n/a	0	n/a	1
ACCC	0	0	3	0
ACIC	0	5	3	7
ASIC	0	0	0	3
AFP	0	0	3	0
CCC (QLD)	0	0	5	0
CCC (WA)	0	0	1	0
DHA	0	0	1	4
IBAC	0	1	4	3
ICAC (NSW)	0	0	0	0
ICAC (SA)	0	0	1	3
LECC	0	0	5	0
NACC	0	0	5	0
NSW CC	0	0	0	0
NSW CS	0	0	0	1
NSW Police	0	0	5	3
NT Police	1	3	6	3
QPS	0	4	6	6
SA Police	0	0	3	2
TAS Police	0	2	4	5
VIC Police	5	5	4	4
WA Police	0	0	8	3
TOTAL:	**6**	**20**	**67**	**48**

Table 5A – International Production Orders Health Checks

Agency	Health Check Conducted		Agency	Health Check Conducted	
	2022-23	2023-24		2022-23	2023-24
ACT IC	No	N/A	**ICAC (SA)**	No	No
ACCC	No	No	**LECC**	No	Yes
ACIC	Yes	No	**NACC**	No	No
ADA	Yes	No	**NSW CC**	No	Yes
AFP	Yes	No	**NSW Police**	Yes	No
ASIC	No	No	**NT Police**	No	Yes
CCC (WA)	No	No	**QPS**	No	Yes
CCC (QLD)	Yes	No	**SA Police**	No	Yes
DHA	Yes	No	**TAS Police**	No	Yes
IBAC	No	No	**VIC Police**	Yes	No
ICAC (NSW)	No	No	**WA Police**	No	No

Table 6A – Industry Assistance detailed findings

Agency	Recommendations		Suggestions	
	2022-23	2023-24	2022-23	2023-24
ACIC	0	0	1	0
AFP	0	0	2	0
NSW Police	0	0	0	2
VIC Police	0	0	4	0
QPS	0	0	0	4
WA Police	0	0	0	0
TOTAL	**0**	**0**	**7**	**6**

Table 7A – Industry Assistance Inspection Statistics

Industry Assistance 2023-24 inspection statistics					
Agency	**Record period**	**TARs**	**TARs Inspected**	**TANs**	**TCNs**
QPS	1 July 2022 to 30 June 2023	1	1	0	0
AFP	1 July 2022 to 30 June 2023	0	0	0	0
ACIC	1 July 2022 to 29 Feb 2024	9	2	0	0
VIC Police	1 July 2022 to 30 June 2023	5	5	0	0
NSW Police	1 July 2022 to 30 June 2023	53	23	0	0
WA Police	1 July 2022 to 30 June 2023	1	1	0	0