COMMONWEALTH OMBUDSMAN

Ombudsman Oversight of Covert Electronic Surveillance

Report to the Minister for Home Affairs on agencies' compliance with the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997* from Commonwealth Ombudsman inspections conducted from 1 July 2024 to 30 June 2025.

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 2025

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

Commonwealth Ombudsman
Level 5/7 London Circuit
Canberra ACT 2601
Tel: 1300 362 072
Email: ombudsman@ombudsman.gov.au

Contents

Executive summary

This report contains the results of my Office's inspections of agencies' use of telecommunications data, stored communications, and International Production Order powers under the *Telecommunications (Interception and Access) Act 1979*, as well as our inspections of agencies' use of industry assistance powers under the *Telecommunications Act 1997*.

The powers are highly intrusive and impact the privacy of individuals. As the powers used are covert in nature, those whose privacy has been impacted are unaware of the actions of law enforcement agencies, so they do not have an opportunity to challenge or complain about how the powers were used. My Office provides transparency to the Parliament and the public about how agencies are using the powers.

I am concerned with the level of record-keeping by some agencies for telecommunications data powers that are internally authorised and not subject to scrutiny by independent issuing authorities. When enacting these laws, Parliament balanced the need for external scrutiny against key safeguards built into legislation, such as ensuring that the powers would only be used for offences that met certain thresholds, and that considerations around the privacy impacts of persons subject to the use of the power would be recorded and accountable through our oversight and reporting. My report includes two case studies that emphasise the importance of the role of authorised officers, who can authorise access to telecommunications data for an agency, in upholding these safeguards.

I was pleased with the level of compliance demonstrated across the use of stored communications powers. The report details some concerns my Office has with practices at some agencies with destroying information obtained under warrants, but we are encouraged by steps agencies are taking to improve in this area.

This reporting period marks the first year my Office has inspected agencies' use of International Production Orders (IPO), now that some agencies have become certified and are using the powers. While this report references some findings, including around demonstrating that the information being requested under an IPO is proportionate, we did not identify any serious or systemic non-compliance.

In relation to agencies' use of Industry Assistance powers, my Office did not identify any serious or systemic non-compliance. The report notes areas for improvement with record-keeping practices around the use of these powers.

A list of all the recommendations we made and an overview of all our findings and the agencies we inspected can be found in **Appendix A**.

Iain Anderson

Commonwealth Ombudsman

Our key findings

We found that records at 8 agencies did not demonstrate that access to telecommunications data was consistent with the intent of the TIA Act

We found that New South Wales Police Force were unable to demonstrate the requirements of the TIA Act were met when using telecommunications data powers to investigate public order offences

Most telecommunications data records we inspected at Victoria Police and Queensland Police Service contained insufficient information to demonstrate the requirements of the TIA Act were met

We did not identify any serious or systemic non-compliance in the use of stored communications, international production orders, or industry assistance powers.

Oversight of Covert Electronic Surveillance

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 electronic surveillance powers to covertly gather information or evidence to enforce the criminal law or assist a criminal investigation.

Telecommunications Data

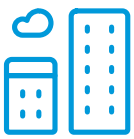
enables agencies to access what is commonly referred to as 'metadata'. It is information about electronic communications such as the date, time and duration of a communication, but not the contents or substance of that communication.

Stored Communications

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

International Production Orders

allows agencies to access telecommunications 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.

Agencies using these powers must comply with legislative requirements and are subject to oversight and reporting each year by our Office. For stored communications and telecommunications data, we must inspect and report on each agency, while for International Production Orders and Industry Assistance powers we may choose whether to inspect an agency but must report on any inspections we do. We may also report on broader observations from our inspections, such as the adequacy of an agency's policies and procedures to demonstrate compliance with the legislation.

This annual report summarises key findings regarding agencies' compliance with the TIA Act and the Telecommunications Act from inspections conducted in the 2024-2025 financial year. The breakdown of the agencies and our findings is in **Appendix A**.

How we oversee agencies

We take a risk-based approach to our inspections, focusing on where risk of non-compliance with legislative requirements would cause public harm.

Ombudsman's powers

For each of the above oversight regimes, the Ombudsman has coercive information gathering powers. These include the power to require an officer of an agency to give relevant information and attend before a specified inspecting officer to answer questions relevant to the inspection.

The Ombudsman must also be given information and access to information despite any other law, and penalty provisions apply to a breach of such a request.

Notwithstanding the powers available to our Office, we typically rely on strong stakeholder relationships in conducting inspections and rarely have cause to engage our coercive powers.

Our inspections typically involve:

Reviewing a selection of an agency's records 	Having discussions with agency staff 
Assessing remedial action taken to address previous issues 	Reviewing policies and processes 

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 issues ranging from:

Minor administrative errors 	through to 	Serious non-compliance that affects an individual's rights (notably privacy) 
The validity of evidence collected 		Systemic issues 

Our inspections may result in:

Recommendations	If an issue is sufficiently serious and systemic, we make formal **recommendations** for remedial action.
Suggestions	If an issue is less serious and was not previously identified, we generally make **suggestions** to the agency to implement practical solutions.
Comments	We also make **suggestions** or **comments** where we consider an agency's existing practice 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 significant findings into this annual report. We follow up on any action agencies have taken to address our recommendations and suggestions at our next inspection.

Telecommunications Data

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

Subscriber information (e.g. name, date of birth, address) 	Date, time and duration of a communication 	Internet Protocol (IP) address, start and finish time of each IP session 
Phone number or email address of the sender and recipient of a communication 	Location of a device (singular point in time, or at regular intervals over a period) 	

The TIA Act provides that agencies can access telecommunications data that is already in existence, known as historical telecommunications data, as well as telecommunications data that comes into existence over a future period not exceeding 45 days, known as prospective telecommunications data.

Telecommunications data may be accessed only when certain thresholds are met. For historic telecommunications data, this includes for the enforcement of the criminal law, to locate a missing person, or to enforce a law imposing a pecuniary penalty or for the protection of public revenue. For prospective telecommunications data, the specified threshold is for the investigation of a serious offence or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

Authorised Officers – An important safeguard

Agencies may access telecommunications data without obtaining a warrant issued by a third party, such as a judge or Administrative Review Tribunal (ART) member. Only an authorised officer, acting under an authorisation by the chief officer of an agency, can authorise the disclosure of telecommunications data from a telecommunications carrier or carriage service provider.

Authorised officers will consider a written request made from an investigative officer of an agency, which we refer to as requesting officers, who will outline why access to individuals' telecommunications data is required. The TIA Act requires that, to authorise the disclosure of telecommunications data, the authorised officers must be satisfied that:

- the access to telecommunications data is **reasonably necessary** for the specified threshold, and
- there are reasonable grounds that any **interference with privacy is justifiable and proportionate**, having regard to the gravity of the conduct, the likely relevance and usefulness of the information to be obtained, and the reason why the disclosure of telecommunications data has been sought.

We rely on records of requesting and authorising officers to assess whether an agency has used the powers to access telecommunications data consistent with these requirements. The level of detail provided in requests and authorisations should be sufficient to demonstrate to a 'reasonable person' that the access to the data and the privacy impacts are necessary to meet the thresholds to use the powers.

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 either refuse the application or record their own comments demonstrating why in their view the requirements of the TIA Act have been met.

What we found

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

We made **10 recommendations** and **46 suggestions** across **11 agencies**.[1] The breakdown of the agencies and our findings in relation to them is in **Appendix A**.

Good Practice

Comprehensive guidance and training materials

We were pleased that some agencies have developed comprehensive guidance materials to support requesting and authorising officers in the use of telecommunications data powers. These materials included training packages and broader governance frameworks that detailed relevant information on the lawful use of the powers, and the process to be followed when seeking to use the powers. Such guidance helps ensure officers understand their obligations when requesting or authorising access to telecommunications data. These resources contribute to more consistent, informed and compliant authorisations.

During the reporting period, we commented positively in our inspection reports on the quality of guidance and training material maintained by the Australian Competition and Consumer Commission (ACCC), the Queensland Crime and Corruption Commission (QCCC), and the Western Australia Corruption and Crime Commission (WACCC).

[1] 6 out of our 10 recommendations were made in the 2023-24 reporting period. We notified the agencies (Appendix A) that the recommendations would remain open until we were satisfied that they had been fully implemented.

Quality assurance, auditing and vetting procedures

We also found that some agencies had implemented robust mechanisms for auditing, vetting and reviewing materials related to telecommunications data authorisations. This included, but was not limited to:

- Western Australia Police Force (WA Police) undertaking proactive reviews of large samples of authorisations to assess whether staff were applying the powers correctly.
- Australian Border Force (ABF) implementing effective vetting of telecommunications data received by carriers, to ensure that information it obtained was consistent with what was authorised.

We also identified instances where compliance staff at the Australian Securities and Investments Commission (ASIC) identified and provided advice to investigators on less intrusive means to obtain information than accessing telecommunications data.

Inadequate records to support authorisation to access telecommunication data

We found records at 8 agencies[2] were insufficient to support the role of the authorised officer to consider that all requirements to access telecommunications data have been satisfied before authorising access to the data. The following case studies illustrate instances where we were concerned that appropriate records were not kept by agencies to demonstrate that access to telecommunications data was consistent with the intent of the TIA Act.

Case Study 1 concerns access to telecommunications data in circumstances where it could not be adequately demonstrated that the offence under investigation met the

[2] Independent Broad-based Anti-corruption Commission, Law Enforcement Conduct Commission, New South Wales Independent Commission Against Corruption, National Anti-Corruption Commission, New South Wales Police Force, Northern Territory Police, Queensland Police Service, Victoria Police.

threshold to use the powers. It also highlights the need for authorised officers to ensure that records are kept that demonstrate that the threshold was in fact met. **Case Study 2** relates to systemic practices of authorised officers within an agency where appropriate records were not kept to demonstrate that any privacy intrusion was justifiable and proportionate.

CASE STUDY 1

New South Wales Police Force were unable to adequately demonstrate the requirements of the TIA Act were met when using the powers to investigate public order offences

Our inspection at the New South Wales Police Force (NSWPF) reviewed a sample of prospective telecommunication data authorisations made to support the investigation of public order offences. We identified 24 prospective telecommunications data authorisations made by NSWPF where the common law offence of conspiracy was applied to a substantive public order offence, which under relevant legislation carried a maximum penalty of 20 units.

We did not consider that the threshold to access prospective telecommunications data, being a serious offence or an offence punishable by at least 3 years imprisonment, was met. Offences penalised through penalty units only carry monetary penalties, not imprisonment.

We informed NSWPF that we consider the intention of Parliament was that access to prospective telecommunications data would be limited to addressing serious, indictable offences, not summary offences that do not carry a term of imprisonment. In addition, it is difficult to see how the interference with the privacy of a person as a result of the disclosure of data would be justifiable or proportionate in circumstances where the substantive offence does not attract an imprisonment term. Accordingly, we consider there is a not insignificant risk that a court would find that NSWPF have not used the powers lawfully.

We also identified 4 unrelated prospective telecommunications data authorisations made for public order offences where requests and authorisations did not demonstrate a clear link between persons of interest and telecommunications services and the common law offence of conspiracy to endanger persons.

The absence of appropriate records made it difficult for us to be satisfied the authorising officer had adequately considered the legislative threshold when authorising access to the prospective telecommunication data, or that they turned their mind to considerations around whether the intrusion of privacy of persons was justifiable and proportionate in the circumstances.

We recommended to NSWPF that it should:

- not rely on the common law offence of conspiracy where the substantive offence under investigation does not meet the definition of a serious offence under the TIA Act, when authorising access to prospective telecommunications data; and
- ensure that a request or authorisation to access prospective telecommunications data provides sufficient information to demonstrate how the person of interest and telecommunication service subject of the request is connected to the investigation of a serious offence.

NSWPF did not accept our recommendations, although it stated that it agreed that records should contain sufficient information to demonstrate how a person of interest and service is connected to the investigation of an offence. We remain concerned that NSWPF is unable to demonstrate that the requirements legislated by Parliament in the TIA Act are being met in these instances. We will continue to engage on the issue at future inspections.

Case Study 2

Most records we inspected at Victoria Police and Queensland Police Service contained insufficient information to demonstrate the requirements of the TIA Act were met

We have made recommendations to Victoria Police over 6 consecutive years to address concerns we hold that authorised officers are not consistently demonstrating that the requirements of the TIA Act have been met before they authorise access to telecommunications data. This included demonstrating that the legislated thresholds to use the powers are met before authorising access to the data, and that the necessary considerations of intrusion on privacy are made.

Most of the records we inspected did not include sufficient information to justify the request, and authorising officers did not adequately record their considerations as to how the requirements of the TIA Act had been satisfied. We also observed there was a low rate of requests that were rejected in areas of Victoria Police that were high users of the powers, indicating that requests may not have been appropriately checked or quality assured.

In the previous 2023-24 reporting period, we made 3 recommendations to Victoria Police that we considered would assist Victoria Police's compliance with the TIA Act. These recommendations were focused on:

- implementing processes to ensure authorised officers consistently and accurately document any information relevant to considering and making a telecommunications data authorisation
- ensuring that all historic and prospective telecommunication data authorisations and disclosures are made for the purposes provided for under the TIA Act, and
- implementing mandatory training for requesting officers to ensure that requests contain sufficient information to enable the authorised officer to make the necessary considerations required under the TIA Act.

Victoria Police accepted our previous recommendations, however at the time of our inspection they were not yet fully implemented. As a result, we notified Victoria Police

that our previous recommendations would remain open until we were able to assess the effectiveness of actions taken at our next inspection.

Similarly, we have across 7 consecutive years made non-compliance findings at Queensland Police Service (QPS) related to keeping records on considerations as to whether privacy intrusions are justifiable and proportionate, and demonstrating that authorisations are properly made. We recommended in the previous reporting period that QPS implement processes to ensure that requesting officers and authorising officers consistently document their considerations when making historic telecommunications data authorisations. While we have made less findings since QPS accepted our recommendation in December 2024, the repeated instances of non-compliance identified in this reporting period remain of concern to our Office. We advised QPS that we would keep our recommendation open until we were able to conduct a complete assessment of the implementation of our recommendation.

Impacts on privacy when changing the frequency of access to location data were not sufficiently considered

Prospective telecommunications data may be used to obtain the location of a telecommunications device, known as a 'ping', at varying intervals of time. We consider the regularity of any interval, and the duration it is authorised for, to be directly relevant to considerations around whether interference with privacy is justifiable and proportionate. This includes whether it is anticipated that the regularity of access to location data may change while the authorisation is in force.

We consider the regularity and duration of access to location data to be directly relevant to considerations around whether interference with privacy is justifiable and proportionate. Any increase in the frequency in which location data is accessed changes the privacy impact on a person. We made recommendations and suggestions on improving practices with access to location data to the NSW Independent Commission Against Corruption (NSW ICAC), NSWPF and Victoria Police in the reporting period.

We had raised in previous reporting periods concerns with practices around either recording or varying frequency of access to location data by NSWPF and Victoria Police. Previous suggestions we made on this issue to both agencies were not accepted on the basis that variations to the frequency of access to telecommunications data was not required to be considered under the TIA Act. We remain of the view that having regard to the frequency of access to data is directly relevant to the requirement under the TIA Act to consider the impacts on privacy, and that the frequency should therefore be considered and this consideration documented. We recommended to both agencies that requests and authorisations for access to location-based services should include considerations of the privacy impacts of any potential change to the ping frequency rate.

Victoria Police accepted our recommendation. NSWPF rejected our recommendation, citing a different view on how the legislation should be interpreted, as well as practical difficulties implementing our recommendation based on its operational requirements. We will continue to engage with NSWPF at future inspections.

We found instances at the NSW ICAC where authorisations did not always specify an initial frequency of access to location data, or the circumstances where they may change, and procedures in place for varying the level of access was done verbally by authorised officers without records being kept. We made two suggestions to the NSW ICAC, that it ensure that the frequency of access to locations data, and the circumstances under which it may change, is recorded on authorisations, and that guidance material and training is updated to this effect. The NSW ICAC accepted both suggestions.

Renewed access to prospective telecommunications data

While the TIA Act limits access to prospective telecommunications data to a period not exceeding 45 days under an authorisation, it is silent on an agency's ability to 'renew' access beyond that period. For simplicity, we will refer to renewed authorisations as those that are authorised immediately after the expiration of a related authorisation.

When considered cumulatively, several consecutive authorisations accessing telecommunications data for the same telecommunications service or person represent a considerable intrusion of privacy and should be included in both the requesting and authorising officers' considerations. Each new authorisation, even if it is a continuation of a previous authorisation, should stand on its own merits and acknowledge both the usefulness of the data obtained under the previous authorisation to the investigation of a serious offence, and, the necessity to continue obtaining the data as part of that investigation.

We made suggestions on improving practices around renewed authorisations to the Australian Criminal Intelligence Commission (ACIC), the Law Enforcement Conduct Commission (LECC), the Independent Broad-based Anti-corruption Commission (IBAC), Northern Territory Police Force (NT Police) and Victoria Police across the reporting period. The findings we made at each agency were similar, based on renewed authorisations we inspected that were made based on justifications provided in a previous authorisation, without regard to what may have changed to justify the continued access to data, or consideration of the cumulative privacy impact.

We made suggestions to each agency aimed at addressing the requirement for authorised officers to ensure that each authorisation to renew access to prospective telecommunications data justifies the continued privacy intrusion. We considered this could be achieved by demonstrating how data obtained under previous authorisations was relevant and useful to the investigation, what changes may have occurred since the last authorisation, and explaining how renewed access to data will continue to progress any investigation. Our suggestions were accepted by all agencies, except the LECC.

At the LECC, we identified an instance where 8 consecutive authorisations were made that continued to rely on justifications referenced in the initial authorisation. The LECC disagreed with our views, as it considered that the authorised officer understood the primary requirement for access to the data remained the same, and that privacy was appropriately considered. We do not think the reasoning provided by the LECC is consistent with the requirements of the Act, particularly around record-keeping, and we will continue to engage on this issue at future inspections.

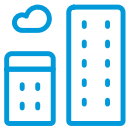
Stored Communications

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 	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 ART 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	Foreign preservation notices (only available to the Australian Federal Police)
		

What we found

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

We made **1 recommendation** and **10 suggestions** across **7 agencies**.[3] The breakdown of the agencies and our findings is in **Appendix A**.

We continue to observe a reduction in the use of stored communications powers. Reporting on the use of the powers by agencies to the Minister responsible for the TIA Act shows a decline from 1,252 stored communications warrants issue in 2018-19[4] to 738 warrants in 2023-24.[5]

Where an agency had not issued a preservation notice or obtained a stored communications warrant, our inspections focused more on compliance with the requirements around using, retaining, destroying, and reporting on stored

[3] The 1 recommendation was made in the 2023-24 reporting period. We notified Western Australia Police that the recommendation would remain open until we were satisfied it had been fully implemented.

[4] Department of Home Affairs, Telecommunications (Interception and Access) Act 1979 Annual Report 2018–19, page 46.

[5] Attorney-General's Department, 2023–24 Annual Report under the Telecommunications (Interception and Access) Act 1979 and Part 15 of the Telecommunications Act 1997, page 52.

communications. The TIA Act limits the use of stored communications only for permitted purposes, such as investigating or prosecuting an offence. Where there is no permitted purpose, agencies are required to destroy the stored communications.

Good practices

We made no suggestions or recommendations in relation to 8 out of 14 agencies we inspected who obtained stored communications warrants during the reporting period. This included NSWPF, Victoria Police, and QPS. These are agencies that are the most frequent users of the powers based on reporting to the Minister responsible for the TIA Act. This indicates that at those agencies, in our view, internal procedures and practices for applying for warrants, obtaining stored communications, and destroying or retaining stored communications are comprehensive for supporting compliance with the TIA Act.

Delays in assessing whether stored communications should be retained or destroyed

We found that the New South Wales Crime Commission (NSWCC) had not destroyed any stored communications in the last 5 years, and had not considered for approximately 4 years whether stored communications it held were capable of being retained for a purpose permitted under the TIA Act, or were required to be destroyed. We suggested the NSWCC immediately review stored communications in its possession to determine if it is required for a purpose permitted under the TIA Act. The NSWCC accepted our suggestion.

Failing to destroy stored communications forthwith

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, the TIA Act

requires that they must cause that material to be destroyed 'forthwith'. While 'forthwith' is not defined by the TIA Act, we consider a timeframe of up to 28 days to be reasonable. We found instances at Western Australia Police (WA Police) and the South Australian Independent Commissioner Against Corruption (SA ICAC) that did not comply with the 'forthwith' destruction requirement.

After we identified during our 2023-24 inspection that the disposal of stored communications at WA Police occurred 51 days after they were authorised for destruction, we recommended that WA Police ensure destructions are undertaken forthwith. This recommendation had not been fully implemented at the time of our inspection, and we again observed 5 instances where destructions did not occur forthwith, with the number of days to dispose of stored communications ranging from 42 to 276 days after they were authorised for destruction. As WA Police had since adopted a 28-day timeframe for destruction, we advised that our recommendation would remain open until it was fully implemented and we were able to assess the adequacy of actions taken.

SA ICAC disclosed to our Office that records relating to 7 stored communication warrants were certified for destruction but were not destroyed, with some stored communications dating back to information obtained under warrants issued in 2017. SA ICAC accepted our suggestions on ensuring that stored communications authorised for destruction are destroyed forthwith, and that its destructions procedures be updated to reflect this requirement.

Failing to report the destruction of stored communications to the Minister within legislated timeframe

An agency must report to the Minister, within 3 months after the end of the financial year, on any stored communication information or records destroyed by the agency during the financial year. We found that, after completing destructions, the Australian Border Force (ABF) did not report the destruction of stored communications to the Minister as required by the TIA Act.

The ABF accepted our suggestions that it report the destruction to the Minister and provide our Office with a copy of the report, and that it implements policies and procedures to ensure that reporting obligations for stored communications powers are made in accordance with the TIA Act.

International Production Orders

The International Production Order (IPO) framework under Schedule 1 of the TIA Act (IPO Schedule) 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[6] (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, monitoring a person subject to a control order to protect the public from terrorist acts, prevent support for terrorist or hostile acts overseas, detect control order breaches, and monitoring a person subject to a Part 5.3 supervisory 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	An order relating to access to telecommunications data
		

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

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 designated agreement).

Before using the IPO powers, an agency must apply for and be granted certification from the Australian Designated Authority (ADA) to use powers under the designated agreement. This certification process occurs independently of our oversight of the agency's use of the powers. In July 2024, the Australian Federal Police (AFP) became the first agency to receive certification from the ADA, followed by NSWPF receiving certification in October 2024. No other Australian agencies have been certified to use an IPO within this reporting period.

To assess an agency's operational readiness to use the powers, we conduct a health check inspection on an agency who is preparing to become certified. The purpose of a health check inspection is to assess the agency's level of preparedness in relation to the development of their IPO framework. We use these health check inspections to engage with agencies and provide assistance or guidance where necessary. Over the reporting period we conducted health check inspections on the ACCC, ASIC, IBAC, NSW ICAC, SA ICAC, and the Western Australia Corruption and Crime Commission (WA CCC). Since 2021, our Office has completed health check inspections on ADA and each of the 22 agencies that can access the powers under Schedule 1 of the TIA Act.

What we found

We conducted inspections of the ADA, AFP and NSWPF under clauses 142 and 143 of the Schedule. We made **11 suggestions** across the **3 agencies**. We also conducted 6 Health Check inspections.

Along with assessing compliance, our inspections of the AFP, ADA and NSWPF were also an opportunity to better understand the lifecycle of the IPO, the types of risks associated with using IPOs, and the handling of material and records obtained through the IPO process.

Our suggestions were directed at incorporating practical strategies to address issues associated with resourcing and operational activities, ensuring accuracy and consistency across all documents related to IPOs, and including sufficient justifications and details to access telecommunications data under stored communication IPOs.

Good Practices

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

Positive engagement and commitment to compliance

Across all three agencies inspected, we experienced positive engagement with our Office in the lead up to and during our first IPO inspections. All agencies demonstrated an interest in ensuring our Office fully understood their internal processes and the practical elements that go into applying for an IPO.

While we identified non-compliance with their first use of the powers, all agencies were receptive to our findings and are committed to improving their IPO framework as they anticipate an increase in their use of the power, and the likelihood that new compliance issues may emerge with this increase. Given these were our first inspections, we have not yet had the opportunity to review the implementation of proposed remedial action against the findings. We will review this during our inspections conducted in 2025-26.

Proactively disclosing instances of non-compliance

We were pleased to see the AFP proactively disclose two separate instances of non-compliance. The AFP attributed these errors to the learning process with the early use of the powers. We view this as a positive reflection of the AFP's commitment to compliance, indicating a willingness to engage openly with our Office and remain transparent and accountable in their use of the powers. These disclosures also help our Office better understand the potential compliance risks that may arise when other agencies become certified and use the powers.

Applications did not provide sufficient reasons when seeking to access telecommunications data associated with stored communications sought under IPOs

We consider the principles of reasonableness, necessity and proportionality when an agency applies to use a covert and intrusive power.[7] An application to use a power should contain sufficient detail and justification to assist the issuing authority to consider how useful the access to the stored communications and associated telecommunications data would be to the investigation of a serious category 1 offence, which is defined as an offence punishable by imprisonment of 3 years or more, or an offence punishable by imprisonment for life.

When an agency applies for an IPO to access stored communications, they may also request the PCP to disclose any related telecommunications data. We identified instances at the AFP and NSWPF where applications for IPOs to access stored

[7] Clauses 39(3) and 48(5) of the Schedule set out the matters to which an issuing authority must have regard to when deciding whether to issue an IPO for access to stored communications or telecommunication data. This includes considering matters such as the gravity of the conduct being investigated, how much privacy of a person would be interfered with, or whether other methods could instead be used to investigate the offence.. While we do not review decisions made by the issuing authority, we do consider the sufficiency of the information provided by the agency to the issuing authority to make the necessary considerations under the Schedule.

communications also requested the disclosure of related telecommunications data but did not address the reason why the associated telecommunications data was required. This was isolated to one application out of the 6 IPOs we inspected at NSWPF, while for the AFP we found that 17 out of the 20 applications contained insufficient justifications to access the related telecommunications data.

We suggested the AFP ensure sufficient detail and justification is included in affidavits to ensure the issuing authority can consider how access to telecommunications data associated with an IPO to access stored communications would assist in connection with the investigation of a serious category 1 offence. We also suggested the AFP update its procedures and templates to ensure this guidance was provided to investigators when preparing an application. The AFP accepted our suggestions.

The progress of IPOs was delayed because insufficient information was included in the accompanying data schedules

The ADA oversees requesting agencies' compliance with the designated agreement and also serves as the intermediary between requesting agencies and PCPs.

At our inspection of the ADA, we observed a delay of approximately 3 months between the ADA receiving 7 IPOs from the AFP and submitting them to the PCP.

The ADA had identified issues with the AFP's documentation that provides information to the PCPs to help understand the nature of the IPO (known as data schedules). The AFP's documentation requested 'all records' be provided under an IPO, instead of stating a defined records period including a start and end date in which the records were created. These documents were returned to the AFP for amendment to include relevant date ranges, and then the AFP were delayed in returning them to the ADA. The AFP advised that the delays were caused due to resourcing constraints and technical issues with the AGD IPO request portal at the time.

Delays in progressing an IPO to the PCP creates a risk that the supporting grounds behind the IPO applications may have changed or ceased since the issue of the IPO. This includes considerations of usefulness of the information to the investigation and

the intrusion on privacy. The designated agreement also prohibits the targeting of an account used or controlled by a 'Receiving Party Person' (RPP),[8] and where there are delays there are risks that a target's RPP may have changed, resulting in a breach of the designated agreement.

We suggested, in such circumstances, that the AFP consider either revoking the IPO and applying for a new IPO when resources are available to exercise the powers, or have suitable contingencies in place to manage the order in the absence of the applicant and key staff. We also suggested that, where progressing an IPO to a PCP is significantly delayed, the AFP should demonstrate that the reasons for the issue of the IPO remain relevant and accurate, in that it remains necessary to continue with the IPO or that the IPO should be revoked.

We suggested the ADA provide advice and insight on the circumstances where they would cancel an IPO under clause 122(1) the Schedule. We also suggested they include these circumstances in their internal guidance material to ensure staff had clear guidance for when an IPO should be cancelled.

Both the AFP and ADA accepted our findings and were receptive to improving their IPO framework to ensure compliance with the schedule.

Applications for IPOs did not provide adequate reasons for the proposed date range in the IPO's data schedule

At NSWPF, we found 7 IPO applications did not contain sufficient reasons to access stored communications or telecommunications data for a specified period in the data schedules.

[8] The designated agreement prohibits targeting a Receiving Party Person (RPP) of the other country. Australia is prohibited from targeting an account used or controlled by a US RPP under an IPO. A US RPP can include (but not limited to): US government entity, US citizen, national or permanent resident, US corporations and a person located in the territory of the United States.

Under clause 134(1)(c)(vi) of the Schedule, the chief officer of an agency must keep certain records for each IPO issued in response to an application made by the agency and, if a period was specified in the order, the details of that period. Without any records made by the applicant, it is unclear whether the issuing authority was provided with sufficient information to detail the necessity and relevance of the specified period.

We suggested NSWPF implement processes to ensure that when applying for an IPO, records consistently document any considerations of the necessity and relevance for the specific date range included in the data schedule. NSWPF accepted our finding and undertook to update their affidavit templates to ensure applicants include a justification of the relevant date range within the affidavits.

IPO applications not identifying sufficiently the 'particular person' to which the order relates, due to insufficient and inconsistent information in the applications

When an agency applies for a stored communications IPO, clause 13 of the Schedule requires the agency to identify the person by any of the unique identifying details, such as a name or account identifiers. Where a particular person is identified, this should be consistently reflected in all IPO related documentation, including the application, affidavit, IPO and accompanying data schedule. Where multiple unique identifiers are referenced in identifying a person, the agency must clearly demonstrate the link between the particulars of that information and the person.

At the AFP, we identified an IPO application where the 'particular person' (subject of the order) was not sufficiently identified. While the application was made in the name of 'unknown person', the accompanying affidavit and order differed from the application by listing the connected service numbers for a known person.

We also located 2 applications for IPOs which contained inconsistent details in identifying the 'particular person(s)' for each order. The application and order were made in relation to an unknown person using a pseudonym, however, the affidavit and

data schedule supporting the applications included the email address of the particular person.

In all 3 instances, it was evident the AFP had the required information available and had the applicable unique identifiers to define a particular person. These details however, were not consistently reflected across the relevant documentation supporting the order.

We suggested the AFP ensure IPO applications identify a particular person as required under clause 13 the Schedule and ensure record keeping consistently and accurately reflects the particulars of individual subject to the IPO. The AFP accepted our finding and suggestions.

Industry Assistance

The Industry Assistance framework was created for intelligence and law enforcement agencies to obtain assistance either through requesting or compelling 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 1997* (the Telecommunications Act).

Intelligence and Law Enforcement agencies can obtain assistance through 3 mechanisms:

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 issues by the chief officer compelling a DCP to provide assistance to an interception agency, and

Technical Capability Notices (TCNs), being a notice issues by the Attorney-General compelling a DCP to develop the capability to assist an interception agency.

The Industry Assistance powers under Part 15 of the Telecommunications Act are available to interception agencies, as defined in s 317B of the Act. These powers do not replace the warrants and authorisations required under the TIA Act, Surveillance Devices Act 2004 (Cth), or other state or territory laws. Rather they give assistance to an existing warrant or authorisation.

What we found

We inspected 6 agencies that had either used or considered using Industry Assistance powers from 1 July 2024 to 30 June 2025. We made **7 suggestions** across **6 agencies**.

The volume of TARs issued by agencies has remained constant from the previous year's reporting periods, with NSWPF continuing to be the largest user of TARs (constituting 65% of the usage) across all of the agencies we oversee. The number of findings we have made has remained largely unchanged over these 3 reporting periods.

Good Practice

We found that the QPS and the AFP have developed policy guidelines to support decision making for authorised officers. We noted QPS are infrequent users of the IA powers, however they have developed comprehensive policies and guidance materials to support their use as it increases. We were pleased that QPS informed us they will update their policy documents and delegation information annually to maintain currency.

We found that the AFP had taken steps to address concerns in previous inspections by updating its internal policies. We were encouraged by the improvements to the policies, as well as the initiative the AFP took to update guidance material in relation to our finding of insufficient record-keeping by authorising officers.

Inadequate records made of Authorised Officers' considerations of reasonableness and proportionality prior to issuing a TAR

At the WA Police we found that authorised officers were unable to adequately demonstrate the necessary considerations of reasonableness and proportionality prior to issuing a TAR.

To determine whether a TAR meets these requirements, authorised officers must consider 9 requirements under s 317JC(a)-(i) of the Act. This includes, but is not limited to, the interests of law enforcement, the availability of other means to achieve the request, whether the request is necessary, and the legitimate expectations of the Australian community relating to privacy.

We consider authorised officers should provide sufficient records of their considerations and not rely on templated wording to demonstrate that they made the necessary considerations required under the Telecommunication Act before issuing an Industry Assistance instrument.

Failure to adequately demonstrate these considerations limits the WA Police's assurance that the authorised officers have turned their mind to the legislative considerations under section 317JC of the Telecommunications Act before authorising the TAR. Additionally, before issuing a TAR, section 317JAA(4) of the Telecommunications Act requires the chief officer to be satisfied that the request is reasonable and proportionate, and that compliance with the request is practicable and technically feasible. We rely on the records of considerations made by the authorised officer to demonstrate that these matters were considered prior to issuing the TAR.

We suggested the WA Police ensure authorised officers adequately record their considerations required under section 317JC of the Telecommunication Act when authorising TAR requests, which was accepted. We also made a finding that insufficient training and guidance material was available to staff. The WA Police accepted our suggestion that it immediately finalise and release its Industry Assistance training package to all users of the powers.

We could not attribute the considerations written on the Technical Assistance Notice (TAN) to the authorised officer

During our inspection of the AFP, we reviewed 2 TANs that were issued where the powers compelled the carrier to assist. We were unable to attribute the hand-written notes recorded in an authorised officer's decision to the authorised officer that issued the TANs, as they were not accompanied by a name or signature recorded within the documents. We made one suggestion to improving the record keeping to ensure the author of any handwritten alterations, additions or deletions to an original application or accompanying notice is clearly identified, along with the time and date of making that record for authorised officers. The AFP accepted our suggestion.

Appendix A

List of recommendations

Table 1 - Telecommunications Data

Agency	Findings	Agency Response
Northern Territory Police	**Repeat instances of inaccurate numbers being provided in Ministerial reporting.** **Recommendation (remained open from 2023-24)**: Recommendation 3 from our previous report, that NT Police implement a system and/or process which will accurately record and report telecommunications data authorisations to the Minister, remains open. We will assess its implementation at our next inspection.	Accepted
Queensland Police Service	**Authorising officers did not adequately record their considerations when authorising access to telecommunications data.** **Recommendation (remained open from 2023-24)**: Recommendation 1 from our previous report, that Queensland Police implement processes to ensure that requesting officers and authorising officers consistently document their considerations when making historic telecommunications	Accepted

Agency	Findings	Agency Response
	data authorisations, remains open. We will further assess its implementation at our next inspection. This relates to non-compliance with sections 180F and 186A(1)(a)(i) of the Act – which require consideration be given to whether any interference with privacy is justifiable and proportionate, and the recording of whether each authorisation to use telecommunications data is properly made. We have made this finding across 7 consecutive reports, and while we have made fewer findings since Queensland Police advised it accepted our recommendation in December 2024, the findings in this report remain of concern to our Office.	
Queensland Police Service	**Mitigation of risks of unauthorised disclosure of telecommunications date to external agencies with direct access to QPRIME remain incomplete.** **Recommendation (remained open from 2023-24)**: Recommendation 3 from our previous report, that Queensland Police establish which agencies have direct access to QPrime and Chapter 4 authorisation information or telecommunications data protected under ss 181B and 182 of the Act, remains open. We will further assess its implementation at our next inspection.	Accepted

Agency	Findings	Agency Response
	While we are satisfied that Queensland Police has taken appropriate action since accepting Recommendation 3 of our previous report in December 2024, further actions were required to support its full implementation.	
New South Wales Police Force	**NSW Police Force were unable to adequately demonstrate that the thresholds and required privacy consideration under the TIA Act were met when authorising access to prospective telecommunication data connect with investigating public order offences.**	
	Recommendation: NSWPF should not rely on the common law offence of conspiracy where the substantive offence under investigation does not meet the definition of a serious offence under the Act, when authorising access to prospective telecommunications data.	Not accepted
	Recommendation: NSWPF ensure that a request or authorisation to access to prospective telecommunications data provide sufficient information to demonstrate how the person of interest and telecommunication service subject of the request is connected to the investigation of a serious offence.	Not accepted

Agency	Findings	Agency Response
New South Wales Police Force	**Authorised Officers are not considering the privacy impacts of any potential change to the frequency of access to prospective location-based telecommunications data.** **Recommendation:** Requests and authorisations for access to location-based services should include considerations of the privacy impacts of any potential change to the ping frequency rate.	Not accepted
Victoria Police	**Victoria Police have not yet implemented our previous recommendations which has contributed to repeat findings in our 2024-25 inspections** **Recommendation (remained open from 2023-24):** 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 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. **Recommendation (remained open from 2023-24):** Victoria Police ensure that all	Accepted Accepted

Agency	Findings	Agency Response
	historic and prospective telecommunication data authorisations and disclosures under Chapter 4 of the Act are made for the purposes expressly under the Act. **Recommendation (remained open from 2023-24):** Victoria Police implement mandatory training for Requesting Officers who seek to access telecommunications 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 telecommunications data) enforcement of the criminal law or (for prospective telecommunications data) the investigation of a serious offence.	Accepted
Victoria Police	**Victoria Police requests and authorisations to access prospective location-based data do not record the frequency of access and the circumstances where access may increase and its impacts on privacy considerations.** **Recommendation:** Requests and authorisations for access to location-based services should include considerations of the	Accepted

Agency	Findings	Agency Response
	privacy impacts of any potential change to the ping frequency rate.	

Table 2 - Stored Communications

Agency	Findings	Agency Response
WA Police	**Stored Communications material not being destroyed 'forthwith' in accordance with the Act.** **Recommendation (remained open from 2023-24):** WA Police ensure that authorised destructions are undertaken 'forthwith' in accordance with s 150(1) of the Act.	Accepted

Table 3 - Overall Findings

	Telecommunication Data				Stored Communications				International Production Orders				Industry Assistance			
Agency	**Recommendations**		**Suggestions**		**Recommendations**		**Suggestions**		**Recommendations**		**Suggestions**		**Recommendations**		**Suggestions**	
	23-24	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**
Australian Border Force	0	0	4	0	0	0	0	2	-	-	-	-	-	-	-	-
ACT Integrity Commission	0	0	1	0	-	-	-	-	-	-	-	-	-	-	-	-
Australian Competition and Consumer Commission	0	0	0	0	0	0	0	0	-	-	-	-	-	-	-	-
Australian Criminal Intelligence Commission	5	0	7	5	0	0	0	0	-	-	-	-	0	0	0	0
Australian Designated Authority	-	-	-	-	-	-	-	-	-	0	-	2	-	-	-	-
Australian Securities and Investments Commission	0	0	3	0	0	0	0	0	-	-	-	-	-	-	-	-
Australian Federal Police	0	0	0	3	0	0	4	0	-	0	-	8	0	0	0	1
Crime and Corruption Commission (QLD)	0	0	0	0	0	0	0	0	-	-	-	-	-	-	-	-
Corruption and Crime Commission (WA)	0	0	0	0	0	0	0	0	-	-	-	-	-	-	-	-

	Telecommunication Data				Stored Communications				International Production Orders				Industry Assistance			
Agency	Recommendations		Suggestions		Recommendations		Suggestions		Recommendations		Suggestions		Recommendations		Suggestions	
	23-24	24-25	23-24	24-25	23-24	24-25	23-24	24-25	23-24	24-25	23-24	24-25	23-24	24-25	23-24	24-25
Independent Broad-based Anti-Corruption Commission (VIC)	1	0	3	1	0	0	0	0	-	-	-	-	-	-	-	-
Independent Commission Against Corruption (NSW)	0	0	0	2	0	0	0	0	-	-	-	-	-	-	-	-
Independent Commission Against Corruption (SA)	0	0	3	0	0	0	0	2	-	-	-	-	-	-	-	-
Law Enforcement Conduct Commission (NSW)	0	0	0	3	0	0	0	0	-	-	-	-	-	-	-	-
National Anti-Corruption Commission	0	0	0	5	0	0	0	0	-	-	-	-	-	-	-	-
New South Wales Crime Commission	0	0	0	0	0	0	0	1	-	-	-	-	-	-	-	-
Corrective Services (NSW)	0	0	1	0	-	-	-	-	-	-	-	-	-	-	-	-
New South Wales Police Force	0	3	3	4	0	0	0	0	-	0	-	1	0	0	2	3
Northern Territory Police	3	1	3	4	1	0	1	1	-	-	-	-	-	-	-	-
Queensland Police Service	4	2	6	0	0	0	0	0	-	-	-	-	0	0	4	0

	Telecommunication Data				Stored Communications				International Production Orders				Industry Assistance			
Agency	**Recommendations**		**Suggestions**		**Recommendations**		**Suggestions**		**Recommendations**		**Suggestions**		**Recommendations**		**Suggestions**	
	23-24	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**	**23-24**	**24-25**
South Australia Police	0	0	2	7	0	0	1	2	-	-	-	-	-	-	-	-
Tasmania Police	2	0	5	8	0	0	2	1	-	-	-	-	-	-	-	-
Victoria Police	5	4	4	4	0	0	1	0	-	-	-	-	0	0	0	0
Western Australia Police	0	0	3	0	1	1	1	1	-	-	-	-	0	0	0	3
TOTAL:	**20**	**10**	**48**	**46**	**2**	**1**	**10**	**10**	**0**	**0**	**0**	**11**	**0**	**0**	**6**	**7**