COMMONWEALTH OMBUDSMAN

Surveillance powers under the microscope

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004* (Cth) for Commonwealth Ombudsman inspections conducted from 1 January to 30 June 2025

Report by the Commonwealth Ombudsman, Iain Anderson under section 61 of the *Surveillance Devices Act 2004* (Cth)

September 2025

ISSN 2209-7511 - Print
ISSN 2209-752X – Online

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

Commonwealth Ombudsman
7 London Circuit
Canberra ACT 2600
Tel: 1300 362 072

Email: media@ombudsman.gov.au

Contents

Commonwealth Surveillance Devices at a glance

A **surveillance device warrant** permits law enforcement agencies to use surveillance devices in criminal investigations or to locate and safely recover a child to whom recovery orders relate.

There are four types of surveillance devices: **tracking devices, optical surveillance devices, listening devices** and **data surveillance devices**. Some devices are a combination of two or more devices.

A **computer access warrant** permits law enforcement to collect information from a computer to obtain evidence for a criminal investigation or to locate and safely recover a child to whom recovery orders relate.

A Data disruption warrant allows the AFP and/or ACIC to disrupt serious crime online.

Protected Information is any information obtained from the use of a surveillance device or from access to a computer. This also includes any information relating to the application, issue or execution of a warrant or authorisation, and any information likely to enable identification of a person, object or premise subject to a warrant or authorisation.

GOOD PRACTICES

We observed most agencies had taken positive steps to implement the recommendations and suggestions made in our previous reports, with significant work on policies, practices and standard operating procedures undertaken over the inspection period.

CONCERNS

We found instances where action was taken without a valid warrant being in place, and instances where data was collected outside warrant parameters. We continue to see insufficient attention and resources being applied to the destruction of protected information.

Executive summary

The *Surveillance Devices Act 2004* (Cth) (the Act) enables 17 law enforcement agencies[1] to apply for and use powers to covertly gather evidence of a relevant offence, or for another specified purpose under the Act, by using a surveillance device or accessing a computer. The Act specifies how agencies will deal with the information obtained and applies restrictions on any unlawful recording, use or communication of this information.

The use of a device to covertly listen, track or observe a person or access their computer is highly intrusive of a person's privacy. Often the person subject to this surveillance is unaware that such a device has been used against them and cannot complain or question an agency's actions.

Every 6 months, the Commonwealth Ombudsman (our Office) inspects each agency's use of the powers. This report presents a summary of our most significant findings from inspections conducted between 1 January and 30 June 2025.

While we inspected each agency, only the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), National Anti-Corruption Commission (NACC) and Western Australian Police Force (WA Police) had used the powers. We made no findings for agencies that had not used the powers.

We are encouraged to see a decrease in the number of findings across most agencies from our previous Biannual report. We also noted the AFP had instigated processes to improve the identification and disclosure of instance of non-compliance with the Act to our Office. This shows that agencies are making increased efforts in compliance and improving their framework to minimise risks of non-compliance.

During this inspection period, we concluded our view on whether the ACIC had adequately demonstrated a connection between the use of surveillance and computer access powers in intelligence operations and the thresholds under the Act. We found that there was a not a insignificant risk that the ACIC would not be able to adequately

[1] ACIC, LECC, NACC, AFP, Victoria Police, NSW Police, WA Police, WA Crime and Corruption Commission, Tasmania Police, SA Police, Queensland Police Service, NT Police, NSW Independent Commission Against Corruption, NSW Crime Commission, SA Independent Commission Against Corruption, Queensland Crime and Corruption Commission and Independent Broad-based Anti-Corruption Commission.

demonstrate they met the necessary thresholds if challenged in court, when using these powers in all instances.

We also found several areas where the AFP, NACC and WA Police could improve.

- We identified instances at the AFP where data had been collected using a surveillance device that was not authorised under a warrant. This included an instance where a surveillance device was deployed prior to the authorisation of a warrant.
- We saw instances at the AFP and NACC where the applicants did not provide the issuing authority with adequate information pertaining to the impact of surveillance devices upon the privacy of persons or third parties when applying for or extending a warrant.
- We found instances at the WA Police and AFP of investigators failing to review the need to retain a warrant, or not revoking a warrant, where it was no longer required.
- We saw instances at the AFP where protected information authorised for destruction was not disposed of within appropriate timeframes. This has been a repeat finding for the AFP since 2015.
- We found that the WA Police had insufficient records to account for their reporting to the Minister and for registering warrants and authorisations.

Our office made **13 recommendations** and **14 suggestions** during the inspection period. Details of our findings are presented by agency in **Appendix A**.

Overview of Inspections

While we inspected each agency's use of the powers under the Act, we only made findings in relation to 4 agencies. We inspected the ACIC twice, which included reviewing records to conclude our view on an unresolved matter from our April-May 2024 inspection. The statistics on our findings across these agencies are included in the table below.

Agency	Inspection Dates	Number of Findings	Number of Recommendations	Number of Suggestions
AFP	March 2025	**6**	**5**	**4**
ACIC	December 2024 – March 2025	**1**	**5**	**3**
	April 2025	**0**	**0**	**0**
WA Police	May 2025	**3**	**3**	**2**
NACC	June 2025	**2**	**0**	**5**

Scope and methodology

Section 55(1) of the Act requires the Ombudsman to inspect the records of a law enforcement agency to determine the extent of their compliance with the Act. The list of agencies we inspect can be found in **Appendix B**.

Section 61(1) of the Act requires the Ombudsman to provide reports to the Minister for Home Affairs at six monthly intervals with the results of each inspection conducted during the reporting period. The Minister is required to table these reports in Parliament within 15 sitting days. These reports provide transparency to the Parliament and the public about how agencies use these intrusive powers.

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 bi-annual report to the Minister for Home Affairs.

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

Good practices

Actions by the agencies to address our previous concerns

We were pleased to see several agencies implementing our recommendations and suggestions to address findings from our previous inspections.

Our 2024 inspection of the WA Police identified several concerning practices leading to non-compliance. Following that inspection we made 7 recommendations and 5 suggestions to address 9 findings of serious or systemic non-compliance. We were pleased to see significant improvements by the WA Police during this inspection, including the completion of 5 recommendations and 2 suggestions. Substantial progress had also been made against the remaining recommendations and suggestions. We acknowledged WA Police had made efforts to address our previous findings and continue to build their compliance knowledge and expertise to use the powers.

At the NACC, we were pleased to see the NACC's responsiveness in taking actions against our previous findings and suggestions. At our September 2024 inspection, we found our previous suggestions were only partially implemented, largely due to the NACC receiving our findings shortly before that inspection. At this inspection we were able to follow up on the NACC's progress and found that all suggestions had been implemented in full.

The AFP during this inspection had proactively disclosed numerous instances of not complying with legislative provisions when using the powers under the Act. We welcome these disclosures as it indicates systems and processes are in place to identify and remedy instances of non-compliance.

Improved record keeping by the WA Police mitigated risks of being non-compliant

In 2024, we recommended that the WA Police immediately review and implement a centralised system and supporting process for record keeping to adhere to the requirements under sections 45, 51 and 52 of the Act.

In May 2025 we observed the WA Police had created and used an electronic compliance system to record actions concerning the use of surveillance devices powers. The introduction of the system was complemented with updated standard operating procedures (SOPs).

The steps taken by the WA Police addressed the risks of not complying with sections 45, 51 and 52 of the Act, and were considered positive steps to building a more robust compliance framework to support their use of the powers.

AFP reviews and self-disclosures of non-compliance

The AFP proactively disclosed numerous instances of not complying with legislative provisions when using the powers under the Act. We welcome these disclosures as it indicates systems and processes are in place to identify and remedy instances of non-compliance.

We also received briefings from the AFP on decisions impacting on the AFP's ability to comply with the legislation, particularly in relation to the destruction of information obtained through use of surveillance devices or when accessing a computer. The AFP had been responsive to our previous findings, recommendations and suggestions, having taken significant steps to implement all of the findings from our August 2024 inspection.

What can agencies improve on?

There is not an insignificant risk that the ACIC would not be able to adequately demonstrate they met the legislative thresholds when using surveillance devices and accessing a computer in all instances

A law enforcement agency can obtain a warrant for a surveillance device or access to data on a computer if there is a reasonable suspicion that the material gathered through the use of a surveillance device or access to data on a computer is necessary to enable evidence to be obtained of a relevant offence, or to identify or locate offenders[2].

We recognise the unique role of the ACIC which encompasses the strategic direction of an intelligence agency while having a legal framework for some powers that is premised on a law enforcement agency. The ACIC primarily exists to perform an intelligence function, providing a range of both focussed and high-level intelligence products to its law enforcement partners. The ACIC generally relies on arrangements with its partners to investigate serious offences or commence proceedings before a court. It is the nature of intelligence that it may or may not lead to or result in a law enforcement outcome.

[2] Section 14 and s 27A requires a law enforcement officer to have reasonable suspicion that:

- one or more relevant offences have been, is being, are about to be or likely to be committed
- there is an investigation into those offences; and
- the use of a surveillance device or access to data held in a computer is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.

However, we consider there still needs to be a demonstrated link with the threshold for being able to use surveillance device or computer access powers.

Our September 2024 report to the Attorney-General highlighted our observation that the ACIC's demonstration of the link with the threshold for being able to use surveillance devices or access to a computer was not always clear. At that time we had not yet concluded our views on whether the ACIC had been able to adequately demonstrate a connection between the use of surveillance device or computer access powers and the thresholds under the SD Act. Our observations were based on the records we inspected within 4 ACIC intelligence operations between April and May 2024.

Between December 2024 and March 2025, we re-examined the records for those 4 intelligence operations to conclude our view on whether the ACIC had been able to adequately demonstrate the connection with the thresholds under the Act.

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

We observed differences in the way the surveillance device or computer access powers are accessed by the ACIC in intelligence operations compared to how other law enforcement and integrity agencies use these powers within an investigation. We generally see law enforcement agencies use a surveillance device or access a computer to investigate and prove an allegation of a crime having been, or being, committed. Admissibility of evidence gathered through a surveillance device or access to a computer is the key priority for any law enforcement investigation. In contrast, during an intelligence operation, the ACIC do not directly contribute evidence from using surveillance devices or accessing computers to support an investigation or prosecution of a person for an offence, but rather, provide what they call 'actionable intelligence' or potential investigation leads that another agency that may or may not use to gather their own evidence of that offending.

The connection between the ACIC's use of surveillance device or computer access powers and the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders (an investigative purpose) is less clear. This connection is particularly strained when the ACIC uses surveillance devices or accesses computers and collects evidence, but they may not ever intend to pass that material to a partner law enforcement agency as evidence or

necessarily advise a partner agency of their activities at all. Within the intelligence operations we reviewed, we did not identify any enforcement or Investigative activity focused on a prosecution objective being commenced by either the ACIC or a partner agency from any material gathered by the ACIC through the use of a surveillance device or accessing a computer.

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

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

We made 5 recommendations and 3 suggestions to assist the ACIC with engaging the legal risks when using surveillance device or computer access powers in support of their intelligence mandate.

The ACIC accepted 2 and accepted in part 3 of our recommendations. The ACIC acknowledged that more can be done to record considerations and decisions throughout the life of covert warrants and authorisations and in considering disclosure of evidence. The ACIC acknowledged our recommendations and suggestions on how the ACIC can continue to improve its compliance and risk practices. The ACIC also appreciated that our Office acknowledged the ways in which the ACIC uses covert

powers differ from how other law enforcement and integrity agencies use the same powers.

Collecting data that was not authorised by a warrant or where a warrant did not exist

We identified 3 separate instances where the AFP collected data that was not authorised by a warrant or authorisation. The AFP also disclosed a fourth instance where a data device was deployed before a surveillance device warrant was sworn and in place. This was a repeat finding for the AFP.

The Act provides a framework for law enforcement officers to lawfully use and retrieve surveillance devices or access a computer. The Act does this by providing procedures for law enforcement officers to obtain warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices, or to access to data held in computers. A valid warrant or authorisation must be obtained prior to lawfully using or retrieval of surveillance devices or accessing a computer.

The AFP disclosed several instances where they had continued to collect data that was not authorised by a warrant or authorisation. This included the use of a tracking device which continued to collect data for 22 days past the expiry of the warrant, and an instance of a tracking device that collected data for over 9 hours before the warrant was issued. Although a warrant was ultimately issued, we were concerned that a device was deployed prior to an eligible judge or nominated Administrative Review Tribunal member scrutinising the application and a warrant issued to exercise the surveillance device powers.

Our last 3 inspections of the AFP have identified instances where unauthorised collection of data has been caused by human or technical errors and a failure to up skill key staff. Despite this being a reoccurring issue, we have not seen any guidance materials prepared by the AFP to assist in reducing these errors. We are concerned that the lack of defined processes, guidance material and delivery of training to key staff will presents a systemic compliance risk to collecting data not unauthorised by a warrant or authorisation.

We recommended the AFP comply with the warrant or authorisation, and ensure effective procedures and practices are in place to identify, report and immediately quarantine any data collected outside of the parameters of a warrant or authorisation. We also suggested the AFP put guidelines and processes in place to ensure surveillance devices are only deployed and/or retrieved when a valid warrant exists.

The AFP accepted this recommendation and advised that it has reviewed its holdings and identified that only a very small amount of data was accessed outside of the parameters of the warrant. The AFP took appropriate steps to quarantine this data.

Retrieval of device without warrant

The AFP disclosed they retrieved a device without a valid warrant being in place. Although the object hosting the devices was within the possession of the AFP at the time, the law enforcement officer retrieving the device did not make sufficient enquiries to confirm a valid warrant was in existence prior to exercising a surveillance device power (being the retrieval of a device). The office did not offer an explanation as to why they considered it was appropriate to retrieve the device without a valid warrant, however clarified that no data was obtained after the warrant expired, and that the device was in the AFP's possession at the time. AFP advised it is considered best practice for members to either sight a warrant or confirm a warrant has been issued, prior to undertaking surveillance activities permitted only by legislation. We were alarmed that the officer failed to acknowledge or address the non-compliance and the seriousness of exercising surveillance device powers without first confirming a valid warrant was in place.

Insufficient consideration of privacy impacts on third parties

At the AFP and NACC, we found affidavits to extend surveillance devices that did not contain adequate information on the details of known impacts on the privacy of third parties. These applications relied on the circumstances as detailed in the original application to obtain a warrant, and did not sufficiently outline changes in the investigation or any privacy intrusion from the use of the surveillance device authorised by the original warrant.

The use of a device can be highly intrusive of the privacy of third parties who, although not subject to investigation, may be subject to surveillance. Section 16(2) of the Act requires the issuing authority to have regard to the extent to which the privacy of any person is likely to be affected, as well as the existence of any alternative means of obtaining the evidence or information sought to be obtained under the warrant.

Affidavits for any surveillance device warrant, variation or extension should include details about the privacy impacts on any person, and the existence of alternative means (and/or more traditional forms of surveillance) of obtaining the information or evidence. When using intrusive technologies, the agency must provide sufficient details in its affidavits to enable the issuing authority to have regard to the use and capability of the technology, and the extent to which the privacy of any person is likely to be affected.

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

At the AFP, we found templated wording in affidavits to extend warrants which did not contain circumstances where the AFP was aware that the privacy of third parties had been impacted through the deployment of a surveillance device under the original warrant. This is a repeat finding for the AFP, with our Office making 1 suggestion from our August 2024 inspection and 2 suggestions from our March 2024 inspection to remedial this issue. In March 2023 we also suggested that the AFP ensure there is sufficient information in surveillance device warrant applications (including supporting affidavits) which addresses privacy considerations of any person likely to be affected by the warrant.

We again observed 2 instances where issuing authorities may not have been fully aware of privacy impacts upon third parties before issuing a warrant extension. This was particularly the case in circumstances where the AFP had deployed a device under the original warrant in a public place. We recommended the AFP ensure affidavits accurately reflect the possible impact of any use of the power on the privacy of third parties, including identifying appropriate measures to mitigate or manage these privacy impacts within affidavits seeking, extending and varying warrants.

The AFP accepted this recommendation and advised that the 2 warrants were issued prior to implementing remedial actions to address our earlier suggestion. The AFP has

updated its forms to include additional privacy considerations and the AFP have not since identified any further issues.

At the NACC, we found 2 instances where the information contained in applications and affidavits for surveillance device warrants did not fully reflect the circumstances of the investigation and the impacts on persons or third parties' privacy.

We noted that warrants predated our September 2024 inspection, during which we made a similar finding and the NACC accepted our suggestion to ensure affidavits consistently and accurately reflect the impacts of any use of the power on the privacy of the person or third parties, including identifying appropriate measures to mitigate or manage these privacy impacts.

We reiterated our suggestion from our September 2024 inspection that the NACC ensure affidavits consistently and accurately reflect the current and potential impacts of any use of the power on the privacy of the person, including identifying appropriate measures to mitigate or manage these privacy impacts. We also suggested the NACC ensure any applications or affidavit to renew a warrant include any information related to, or assessment of, the impacts on privacy of a person or third party gathered through the preceding warrant(s).

The NACC accepted these suggestions and advised that the privacy impacts had been discussed with the NACC's Operations and Operations Legal teams to include further consideration while drafting affidavits for renewal of warrant applications. All NACC Operations Legal team were instructed to complete the relevant eLearning modules.

Warrants not reviewed to ensure they remain necessary for the investigation

We found instances where the AFP and WA Police failed to revoke surveillance device warrants in accordance with sections 20 and 21 of the Act.

If the use of a surveillance device (including a Computer Access Warrant (CAW)) is no longer required for the purpose it was sought, sections 20 and 21 of the Act require the Chief Officer of the agency to revoke the warrant and take steps to discontinue the use of the surveillance device. We expect agencies to do this as soon as practicable and within 28 days of being satisfied that the surveillance device is no longer required.

Law enforcement officers must also immediately inform the chief officer if they believe the use of a surveillance device including a CAW is no longer necessary for its original

purpose. Similar requirements apply in relation to computer access warrants under sections 27G and 27H of the Act.

During the AFP inspection, the AFP disclosed 29 surveillance device warrants which were not immediately revoked when no longer required or the legislative requirement to use the powers no longer existed. We reviewed these disclosures during the inspection and found two instances where warrants were not revoked for up to two and three months after they were deemed no longer necessary by the investigating officer.

We also observed the practice of 'parking' warrants where the AFP holds onto unexecuted SD warrants for future operational opportunities of deployment. These warrants were not revoked and allowed to expire after 90 days. We understand there are circumstances where warrants are unable to be executed for operational reasons. Where this is the case, we expect to see records demonstrating regular consideration of the reasons why devices cannot be deployed and the need to retain the warrant. We reviewed the records in 2 AFP investigations and found 13 of the 35 surveillance device warrants for these investigations were not executed. We located no records of any considerations or decisions to retain these warrants, or revoke the warrants if they were no longer required for the investigation.

We recommended the AFP ensure surveillance device warrants are immediately revoked where the investigator forms a view that the use of a surveillance device under the warrant is no longer necessary. We also suggested AFP remind investigators of their obligations to revoke warrants when they are no longer necessary, including the requirement to notify the chief officer immediately upon forming the belief that use of a surveillance device is no longer necessary.

The AFP accepted the recommendation and suggestion. The AFP advised that investigators had been reminded of the requirement to revoke warrants that are no longer required. The AFP has also updated it training materials for investigators to reflect this requirement and introduced system generated reminders for investigators to review a warrant during the life of that warrant.

At the WA Police in May 2025, we found 2 unexecuted warrants that were not revoked. We could not locate any records to indicate the WA Police had reviewed these warrants or considered whether it was necessary to retain the warrants for the investigation.

In April 2024, we recommended the WA Police implement measures to ensure warrants are regularly reviewed to consider whether the warrants continue to be necessary for the conduct of the investigation. Where warrants are no longer necessary, they should be revoked. Where warrants are unexecuted, regular reviews should be conducted to

consider whether there remains scope for execution. Where it is determined the warrants are unable to be executed, or are no longer necessary, they should be revoked. All reviews of warrants, and decisions to maintain or revoke them, should be recorded. This recommendation was accepted by the WA Police.

The 2 unexecuted warrants we inspected were issued prior to our April 2024 inspection. That said, at this inspection, we did not consider that WA Police had fully implemented our previous recommendation. We state that the implementation from this previous recommendation, would reduce the risk of not complying with the requirements under sections 20 and 21 of the Act.

In response, WA Police accepted our finding and committed to continue implementing the recommendation.

Protected information was not destroyed as soon as practicable

We saw instances at the AFP where protected information authorised for destruction was not disposed of within appropriate timeframes. We have repeatedly observed these delays by the AFP in disposing of protected information authorised for destruction in 14 inspections conducted on the AFP since 2015.

While the Act enables law enforcement to gather and use such material to support civil or criminal proceedings, it is incumbent on these agencies to destroy this information when it is no longer required for a purpose under the Act. Section 46 is a key safeguard in the legislation and requires agencies to destroy protected information as soon as practicable once the chief officer is satisfied that the material is not required for a civil or criminal proceeding to which it was related. Agencies should have internal guidance on what is an appropriate timeframe to satisfy the destruction requirements. If there is no internal guidance, we consider material authorised for destruction should be disposed of within 28 days of the records being authorised for destruction.

During our August 2024 inspection, the AFP disclosed that limitations in their data management system were hampering their ability to identify and destroy protected information. The AFP suspended the destruction of protected information until the problem was rectified. We recommended that the AFP ensure material authorised for destruction is destroyed as soon as practicable. The AFP accepted our recommendation.

At our March 2025 inspection, the AFP advised this limitation had not been resolved, with no protected information being destroyed since July 2024. The AFP considered a manual solution was impractical and could not guarantee that such a solution would ensure all

relevant protected information would be destroyed. The AFP advised that the data authorised for destruction had been quarantined from any further use or communication as much as possible until destruction resumed.

The AFP also disclosed another 57 instances where the disposal of protected information, authorised by the chief officer for destruction, had been significantly delayed prior to July 2024. These delays ranged from 63 to 203 days after being authorised for destruction, with protected information from 38 warrants being disposed of over 100 days after authority was provided. The AFP advised that the delays were largely due to insufficient resourcing.

Following our March inspection, the AFP advised that the issue impacting the data management system had been rectified and that the destructions of protected information had recommenced.

The findings from our August 2024 inspection were presented to the AFP in February 2025. Although the AFP had limited opportunity to implement our August 2024 recommendations prior to our March 2025 inspection, we considered the AFP could do more to better understand the reasons for the repeated delays in disposing protected information. We recommended the AFP conduct a comprehensive review of its destruction process for surveillance device records to ensure records that are no longer required for a purpose under these Acts are identified and authorised for destruction at the earliest opportunity. We also recommended the AFP destroy any records authorised for destruction within the legislated time period under the relevant Act.

The AFP accepted the recommendation and advised that the AFP had reviewed its destruction process. The AFP recommenced destroying protected information authorised for destruction in May 2025. The AFP expects the backlog of protected information authorised for destruction will be disposed of by June 2026.

Inadequate record keeping arrangements

We found WA Police had insufficient records to account for their reporting to the Minister and for registering warrants and authorisations.

Law enforcement agencies need to keep adequate records to account for their usages of the powers under the Act. Section 53 of the Act requires the agency to create and maintain registers of any warrants or authorisations issued to that agency. Section 49 requires the chief officer to make a report to the Minister as soon as practicable after a warrant or authority ceases to be in force. These records are important to account for the usage of the powers under the Act and to enable Ministerial oversight of the agency's

use of powers under the Act.

We found the WA Police register for surveillance device warrants, emergency authorisations and tracking devices did not adequately record all of information required to be maintained by the agency under the Act. WA Police's register did not record details of the responsible law enforcement officer or details related to any recovery orders, integrity operation or international assistance authorisations. Although WA Police had not been issued with a warrant to access a computer, they had not created the necessary register to record any warrants that may be issued to access a computer. These are requirements under s 53 of the Act.

We also found that the WA Police had no records to demonstrate that reports made under s 49 of the Act had been submitted to the Minister. This included no records confirming the Minister had been advised of inaccuracies or corrections to reports that may have been previously submitted to the Minister.

We recommended the WA Police ensure all relevant s 49 reports were submitted to the Minister and further, advise the Minister of any inaccuracies in any incorrect reports that have been submitted. We also recommended that the WA Police update their register to record the information required to be maintained by an agency under the Act. The WA Police accepted these recommendations.

Appendix A

Table of reported inspection findings by agencies for the period 1 January 2025 to 30 June 2025

The 4 tables below outline **all** findings from our inspections of the AFP, NACC and WA Pol between 1 January 2025 and 30 June 2025. We made no findings relating to surveillance device powers at the ACIC at our most recent April 2025 inspection.

A recommendation reflects a serious compliance issue. A suggestion reflects less serious and/or isolated issues where we consider an agency should take action to improve, or where agencies may refine its practices to demonstrate compliance in future. We also make suggestions or comments where we consider an agency's existing practice may expose it to compliance risks in the future.

Table 1: Findings at the AFP Inspection

	Findings	Agency Response
1	**AFP investigators did not immediately inform the chief officer when SD warrants were no longer necessary.** **Recommendation:** Where an investigator believes that the use of a surveillance device under a warrant is no longer necessary, the investigator must immediately notify the chief officer and seek revocation of that SD warrant. **Suggestion**: AFP remind investigators of their obligations to immediately inform the chief officer, or their delegate, when they believe that a surveillance device under a warrant is no longer necessary. This include seeking revocation of the warrant from the chief officer.	AFP accepted this finding, recommendation and suggestions.

	Findings	Agency Response
	Suggestion: Where no action has been taken under a warrant for an extended period, or where the device has been retrieved or uninstalled, the AFP should review the necessity for the warrant and record any justification for ongoing retention of the warrant.	
2	**The AFP deployed a data device before a sworn surveillance devices warrant had been issued (Disclosure).** **Suggestion:** The Police Technical Team should put guidelines and processes in place to ensure surveillance devices are only deployed and/or retrieved when a sworn warrant exists.	AFP accepted this finding and suggestion.
3	**Data collected outside warrant parameters (Disclosure). (REPEAT FINDING).** **Recommendation:** AFP must ensure compliance with warrants and police technical teams have effective procedures and practices in place to identify, report and immediately quarantine any data collected outside of the parameters of a warrant or authorisation.	AFP accepted this finding and recommendation.
4	**The AFP continues to experience significant delays in disposing of protected information authorised for destruction (REPEAT FINDING).** **Recommendation:** The AFP conduct a comprehensive review of its destruction process for records connected with the use of powers under the SD Act to ensure	AFP accepted this finding and recommendations.

	Findings	Agency Response
	records that are no longer required for a purpose under this Act are identified and authorised for destruction at the earliest opportunity. **Recommendation:** AFP must destroy any records authorised for destruction within the legislated time period under the relevant Act. AFP staff who are then responsible for and witness the destruction of records are to confirm the destruction by noting the date, time and location of the destruction.	
5	**Impacts on the privacy of third parties was not accurately reflected in affidavits to extend SD warrants (REPEAT FINDING).** **Recommendation:** The AFP ensure affidavits accurately reflect the possible impact of any use of the power on the privacy of third parties, including identifying appropriate measures to mitigate or manage these privacy impacts within affidavits seeking, extending and varying warrants.	AFP accepted this finding and recommendation.
6	**Failure to notify the Commonwealth Ombudsman of actions taken under a Data Disruption Warrant (DDW) within 7 days (Disclosure).** **Suggestion:** AFP review its notification procedures and implement frameworks to ensure that notifications and actions under a DDW are sent to the Commonwealth Ombudsman within their legislative 7-day requirement.	AFP accepted this finding and suggestion.

Table 2: Findings at the WA Police Inspection

	Findings	Agency Response
1	**WA Police were unable to determine if s 49 reports to the Minister or any errors in a report were submitted to the Minister (Repeat finding).** **Recommendation:** WA Police must ensure all s 49 reports are submitted to the Minister and advise the Minister of any inaccuracies in reports that have been submitted. This includes keeping sufficient records evidencing accurate reporting to the Minister has taken place.	WA Police accepted this finding and recommendation.
2	**SD warrants being allowed to expire instead of revoked when no longer necessary (Repeat finding).** **Recommendation:** WA Police implement measures to ensure warrants are regularly reviewed to consider whether the warrants continue to be necessary for the conduct of the investigation. Where warrants are no longer necessary, they should be revoked Where warrants are unexecuted, regular reviews should be conducted to consider whether there remains scope for execution. Where it is determined the warrants are unable to be executed, or are no longer necessary, they should be revoked. All reviews of warrants, and decisions to maintain or revoke them, should be recorded.	WA Police accepted this finding and recommendation.

	Findings	Agency Response
3	**Deficiencies were identified in registers used by WA Police to demonstrate their compliance with certain requirements under the Act.** **Recommendation:** WA Police must amend their SD register to ensure the responsible officer's name is recorded against each warrant and whether the warrant relates to a recovery order, mutual assistance authorisation, or integrity operation. **Suggestion:** WA Police implement a CAW register to record when CAWs are notified to the Commonwealth Ombudsman. We accept that the WA Police have yet to issue a CAW but we encourage the proactive step of implementing this register. **Suggestion:** WA Police finalise and implement its register for recording the use, disclosure and destruction of PI.	WA Police accepted this finding, the recommendation and two suggestions.

Table 3: Findings at the NACC Inspection

	Findings	Agency Response
1	**An application for a surveillance device warrant did not sufficiently detail restrictions likely to be applied to data captured through a surveillance device.** **Suggestion:** The NACC should consider circumstances where material may be captured which is subject to restrictions and bring these circumstances to the attention of the issuing authority to allow them to make an informed assessment of the request. **Suggestion:** The NACC ensure all instances of non-compliance are disclosed to us as part of the inspection process. **Suggestion:** The NACC should build its own subject knowledge on technical capabilities used by its partners to ensure that any support provided or data capture by that partner agency is covered by the authority or warrant.	The NACC accepted this finding and the 3 suggestions. With respect to the first suggestion, the NACC advised that this was currently the agency's practice. The NACC did not consider the warrant we exampled in the finding and related to this suggestion was an instance of non-compliance with the Act. With respect to the third suggestion, the NACC did not agree with our view that there was limited knowledge held by the NACC of the specific technical capability used by a partner agency. The NACC considered this to be an isolated incident where the capability was not deployed to its optimal potential, resulting in the capture of material subject to restrictions.

	Findings	Agency Response
2	**Information contained in applications and affidavits for surveillance device warrants did not adequately address privacy considerations.** **Suggestion:** The NACC ensure affidavits consistently and accurately reflect the current and potential impacts of any use of the power on the privacy of the person, including identifying appropriate measures to mitigate or manage these privacy impacts. **Suggestion**: The NACC should ensure any applications or affidavit to renew a warrant include any information related to, or assessment of, the impacts on privacy of a person or third party gathered through the preceding warrant(s).	The NACC accepted this finding and the two suggestions.

Table 4: Findings at the inspection of the ACIC (December 2024 – March 2025)

	Findings	Agency Response
1	**The risk that the ACIC would not be able to adequately demonstrate they met the thresholds when using surveillance devices or access data on a computer in all instances was not insignificant.** We restate our previous recommendation which stated "The ACIC implement measures to ensure that it can demonstrated that the powers (except for access to historical telecommunication data) are use within a continuum of 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 legal proceedings."	The ACIC notes that is has previously accepted this recommendation in part. The ACIC has taken significant steps to ensure that it is both demonstrating appropriate use of covert and intrusive powers and is reducing the risk of potential inappropriate use of covert and intrusive powers. The ACIC acknowledged that more can be done to record considerations and decisions throughout the life of covert warrants and authorisations and in considering disclosure of evidence. The ACIC acknowledges the Ombudsman's recommendations and suggestions on how it can continue to improve its compliance and risk practices.

Findings	Agency Response
Additional recommendations:	
Recommendation: The ACIC consider the legal risk more comprehensively before using a power, including how the nexus to legislative thresholds will be demonstrated consistently through any planned use of the power, applications to use the power and monitoring and reviewing the use of that power.	The ACIC accepted this recommendation.
Recommendation: The ACIC seek guidance from the AGS on practical ways the ACIC can adequately demonstrated they are applying the powers lawfully. This should include seeking advice on ways to sufficiently mitigate the risk of an indirect connection to the threshold not being established or being considered tenuous.	The ACIC accepted this recommendation in part
Recommendation: Ensure applications and affidavits to use a power provide the issuing authority with sufficient information to demonstrate how the ACIC intends to directly or indirectly meet the legislative threshold.	The ACIC accepted the recommendation in part.
Recommendation: The ACIC record any decisions to not communicate or use evidence obtained using a power, including any reasons that would preclude its disclosure under section 12 of the Australian Crime Commission Act 2001 (ACIC Act).	The ACIC accepted this recommendation.

Findings	Agency Response
Recommendation: the ACIC obtain legal advice on their obligations under s 12 of the ACIC Act, and whether the ACIC's current practice of not disclosing evidence is consistent with those obligations.	The ACIC accepted this recommendation in part.
Suggestion: The ACIC provide greater detail in the Disclosure Checklist of how the use or communication of information gathered through a power will progress the ACIC investigation or enable a partner agency to take actions on the information.	The ACIC accepted this suggestion
Suggestion: The ACIC should consider developing or using tools to assist with connecting decisions and actions related to the use of a power with a chronology of the investigation or intelligence operation.	The ACIC accepted this suggestion in part. The ACIC seeks the following statement be included in the published re "The ACIC accepts this recommendation in part. Noting is has already taken steps to implement this recommendation".
Suggestion: 'Actionable intelligence' provided to a partner agency(s) containing information gathered through the use of the powers be accompanied with clear advice on the reason for the disclosing the information and how the disclosure is intended to progress the ACIC or a partner agency's investigation.	The ACIC did not accept this suggestion.

Appendix B

Table 1 – Agencies inspected remotely

Agency
Independent Broad-based Anti-corruption – Victora
New South Wales Police Force
Western Australia Police Force
Corruption and Crime Commission - Western Australia
Tasmania Police
South Australia Police
Queensland Police Service
Northern Territory Police Force
Independent Commission Against Corruption – New South Wales
New South Wales Crime Commission
Independent Commission Against Corruption – South Australia
Crime and Corruption Commission – Queensland

Table 2 – Summary of records inspected on site

Agency	Records available	Records inspected
AFP	108 x SD 141 x D 2 x RW 11 x CAW	17 x SD 13 x D 0 x RW 0 x CAW
ACIC (April 2025)	2 x SD 1 x TDA	2 x SD 1 x TDA
ACIC (Dec – March 2025)	12 x SD 1 x RW	12 x SD 1 x RW
WA Police	10 x SD	10 x SD
NACC	5 x SD 14 x R 3 x CAW	5 x SD 0 x R 3 x CAW
Key SD Surveillance device warrant		

Agency		Records available	Records inspected
CAW	Computer access warrant		
RSD	Refused surveillance device warrant		
SO	Supervisory orders		
RW	Retrieval warrants		
TDA	Tracking device authorisations		
D	Destructions		
DNE	Destructions – not executed		
R	Retentions		