COMMONWEALTH OMBUDSMAN

Through the Surveillance Lens:

From Recommendations to Results

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004* (Cth) for Commonwealth Ombudsman inspections conducted from 1 July to 31 December 2025

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

March 2026

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 (CAW)** permits law enforcement to collect information from a computer to obtain evidence for a criminal investigation or to locate and safely recover a child.

A Data Disruption Warrant (DDW) allows the AFP and/or ACIC to disrupt serious crime online by accessing and altering, adding, copying, or deleting data on computers.

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

Agencies are taking positive steps to implement our previous recommendations and suggestions with significant work on policies, practices and standard operating procedures undertaken over this inspection period.

Concerns

Guidance documents for investigators in one agency did not accurately reflect the requirement to continually review the necessity to retain protected information. This can result in protected information being retained for longer than required.

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 use of a surveillance 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 findings from inspections conducted between 1 July and 31 December 2025 (the inspection period).

While our Office inspected all 17 agencies, only the Australian Federal Police (AFP), the National Anti-Corruption Commission (NACC), New South Wales Crime Commission (NSW CC), Western Australia Police Force (WA POL) and Australian Criminal Intelligence Commission (ACIC) had used the powers. Our Office made no findings at the NACC, NSW CC, WA POL and ACIC and no findings against agencies that had not used the Surveillance Device powers.

Our Office was pleased to see improvements in how agencies complied with the Act and were encouraged to see a decline in the instance of non-compliance. Agencies are making increased efforts to be compliant and improve their framework to minimise the risks of non-compliance. We made fewer findings across all agencies.

We found areas where the AFP could improve. We found an error in the AFP's guidance material provided to investigators on the requirements to destroy protected information under the Act. We made **2 suggestions** to address this error and improve the automated prompts to investigators to regularly review the need to retain protected information gathered through a warrant. Details of our findings are presented by agency in **Appendix A**.

[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.

Overview of Inspections

Our Office inspected 17 agencies' use of the Surveillance Device powers under the Act during this inspection period. We attended and reviewed the records at 4 agencies that used the powers during the inspection period and made findings in relation to only 1 of these agencies. We conducted inspections remotely of the remaining 13 agencies, comprising of 1 that used, and 12 that did not use, the powers during this period. We made no findings in relation to these agencies. In general, we found that agencies used the powers less than what they did in the previous reporting period.

The statistics on inspections for the agencies that used the powers are included in the table below.

Agency	Inspection Dates	Number of Findings	Number of Recommendations	Number of Suggestions	Number of Comments
AFP	August 2025	**1**	**0***	**2**	**0**
NACC	Sept 2025	**0**	**0**	**0**	**0**
NSW CC	Oct 2025	**0**	**0**	**0**	**0**
ACIC	Oct 2025	**0**	**0**	**0**	**0**
WAPOL	Oct 2025	**0**	**0**	**0**	**0**

* Recommendation 3 from our May 2025 inspection report remains open.

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.

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

In response to findings from previous inspections, we were pleased to see that several agencies had implemented our recommendations. We observed that the actions taken to implement our recommendations addressed several systemic risks to agencies not complying with legislative requirements.

We made significantly fewer findings of non-compliance during this inspection period. Between 1 January and 30 June 2025, we made 11 recommendations. During this inspection period (1 July and 31 December 2025), we made no recommendations, with only one previous recommendation remaining open. The following table outlines the decrease in recommendations and suggestions in contrast to the previous 6-month period.

Recommendations and Suggestion across inspection periods

	Recommendations		Suggestions	
AGENCY	**1 Jan – 30 Jun 2025**	**1 Jul -31 Dec 2025 (Current)**	**1 Jan – 30 Jun 2025**	**1 Jul - 31 Dec 2025 (Current)**
AFP	5	0	4	2
ACIC	3	0	0	0
WA POL	3	0	2	0
NACC	0	0	5	0

At this inspection we were able to follow up on the NACC's progress and found that all suggestions had been implemented in full.

Several agencies also proactively disclosed to us numerous instances of not complying with legislative provisions when using the powers under the Act. We welcome these

disclosures as it indicates those agencies have systems and processes in place to identify and remedy instances of non-compliance.

Improvements to the ACIC's use of the powers

Our Office previously found that there was a not insignificant risk that the ACIC would not be able to adequately demonstrate they met the legislative thresholds if challenged in court when using Surveillance Device powers in all instances. We also raised concerns that the ACIC had not taken sufficient actions to review and, if required, destroy Surveillance Device records that were no longer required for a purpose under the Act.

At our most recent inspection, we reviewed a number of disclosures of non-compliance made by the ACIC and the actions taken by the ACIC to remediate our previous findings. We found the ACIC was proactive in identifying potential instances of non-compliance and was taking adequate steps to disclose and respond to instances of non-compliance. The non-compliances were minor or administrative in nature. We were encouraged that the ACIC had reviewed each disclosure to determine whether there were any systemic causes to the non-compliance and instigated remedies to prevent potential non-compliance in the future.

We observed the ACIC had undertaken, or were in the process of implementing, internal reforms to improve how the agency demonstrates they met the legislative thresholds when using the powers. This included significant changes to the ACIC's governance, policies, procedures, systems and training supporting the use of the powers to progress our recommendations and suggestions. We will return to the ACIC in the first half of 2026 to review how these changes have been applied in the ACIC's practices and use of the powers.

What can agencies improve on?

Continuing to improve the authorised destruction of protected information as soon as practicable

Protected information is information that has been obtained from the use of a surveillance device or from access to a computer and includes information relating to the application, issue, or execution of a warrant or authorisation and any information that could identify a person, object or premises subject to that warrant or authorisation.

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.

We reported concerns in our September 2025 report to the Minister with the AFP not disposing of protected information authorised for destruction within appropriate timeframes. The AFP accepted our recommendation to conduct a comprehensive review of its destruction process for records connected with the use of powers under the Act to ensure records that are no longer required for a purpose under the Act are identified and authorised for destruction at the earliest opportunity. While we again saw instances of delays in the disposal of protected information at our most recent inspection, the AFP had only received our recommendation just prior to the inspection and were in the process of implementing remedial actions. We will continue to monitor the AFP's progress in implementing our recommendation at future inspections.

At our most recent inspection, we also found the guidance material being provided to investigators was incorrect and required correction. In particular, the legacy flow charts within guidance material required updating to reflect the requirement to review and

destroy protected information as soon as practicable when it is no longer required for a permitted purpose under the Act. We suggested the AFP review and amend the guidance material to ensure it is consistent with the requirements under s46 of the Act. This includes ensuring records are reviewed, and if required destroyed, on a warrant-by-warrant basis.

Additionally, we found investigators were only being prompted by an automated notification to review protected information obtained under a warrant just prior to the expiry of the initial 5-year threshold to retain records under the Act. We were concerned that the prompts were not encouraging investigators to regularly review the need to retain the protected information and seeking its destruction when it was no longer required for a lawful purpose under the Act. We suggested the AFP could improve its automated prompts to investigators reminding them of their obligations to ensure protected information is reviewed regularly and destroyed in accordance with s46 of the Act, rather than at a time close to the initial 5-year threshold to retain records under the Act.

The AFP accepted our suggestions and responded that they have updated their guidance material and are in the process of testing an automatic reminder system that will regularly prompt a review in relation to retention.

Appendix A

Table of reported inspection findings by agencies for the period 1 July 2025 to 31 December 2025

The table below outlines the finding for which we suggested remedial action from our inspection of the AFP between 1 July 2025 and 31 December 2025.

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	**The AFP continues to experience significant delays in destroying protected information and telecommunication intercept records that are no longer required for a purpose under the Act (Repeat finding)** **Recommendation 3 from our August 2025 inspection report remains open.** The Recommendation was that the AFP conduct a comprehensive review of its destruction process for records connected with the use of powers under the SD Act	The AFP accepted this finding, recommendation and suggestions.

Findings	Agency Response
to ensure records that are no longer required for a purpose under the Act are identified and authorised for destruction at the earliest opportunity. **Suggestion 1**: The AFP review and amend the guidance material supporting investigators with reviewing and destroying records under the SD Act is consistent with the provision under s46(1)(b) of the SD Act. This includes ensuring records are reviewed, and if required destroyed, on a warrant-by-warrant basis. **Suggestion 2:** The AFP review the use of automatic reminders to investigators during the life cycle of a SD warrant to encourage investigators to regularly review the need to retain protected information under the warrant.	

Appendix B

Table 1 – Agencies inspected remotely with no Findings during this inspection period

Agency	
Victoria Police	South Australia – ICAC
Crime and Corruption Commission – Western Australia	Independent Broad-based Anti-corruption Commission
Tasmania Police	Queensland Crime and Corruption Commission
South Australia Police	New South Wales Police Force
Queensland Police Service	Law Enforcement Conduct Commission
Northern Territory Police Force	Western Australia Police Force
New South Wales – ICAC	

Table 2 – Summary of Surveillance Device records used during this inspection period

Agency	SDs used in this period	SDs used in previous period
AFP	115	445
ACIC	2	10
WAPOL	10	10

Table 3 – Summary of Computer Access Warrants used during this inspection period

Agency	CAWs used in this period	CAWs used in previous period
AFP	25	11
NACC	2	3
ACIC	0	1
NSW CC	1	0
WAPOL	14	0

Table 4 – Summary of Data Disruption Warrants used during this inspection period

Agency	DDWs used in this period	DDWs used in previous period
AFP	1	2
ACIC	0	0