COMMONWEALTH OMBUDSMAN

Surveillance device powers: are agencies complying?

Report to the Attorney-General on agencies' compliance with the *Surveillance Devices Act 2004* (Cth) for Commonwealth Ombudsman inspections conducted from 1 January to 30 June 2024

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

September 2024

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
Level 5, 14 Childers Street
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.

IMPROVEMENTS

We were encouraged by the collaboration and information sharing between agencies to proactively improve compliance.

We continue to see development and review of governance, guidance and policy documents.

CONCERNS

We were concerned an agency's internal safeguards were not adequate for using the powers in intelligence operations.

We were also concerned to discover an agency lost control of protected information in transit.

Executive summary

The *Surveillance Devices Act 2004* (Cth) (the Act) provides law enforcement agencies with the framework to lawfully use covert powers such as surveillance devices. The Act specifies the types of surveillance activities that may be undertaken and what agencies must do when undertaking those activities. The Act also provides clear rules on how agencies must deal with the information obtained using surveillance device powers and applies restrictions on how that information can be lawfully used, communicated, stored and destroyed.

The powers given by the Act are highly intrusive and impact the privacy of individuals. As the authorised activities are covert in nature, those whose privacy has been impacted may be unaware of the actions of law enforcement agencies, thus removing the opportunity to challenge or complain about how they used the powers.

There are 17 law enforcement agencies in Australia that can use the powers under the Act. Every six months, the Ombudsman inspects and reports on each agency's use of the powers. This report presents a summary of our most significant findings from inspections conducted between 1 January 2024 and 30 June 2024.

We found four key areas of non-compliance requiring immediate attention:

- improving internal safeguards to ensure the ACIC use surveillance devices or computer access powers within intelligence operations lawfully (ACIC)
- the loss and potential loss of protected information (AFP and WA Police)
- not reviewing the necessity to retain a warrant and allowing them to expire after 90 days (ACIC, WA Police and the LECC), and
- staff having insufficient training and were unfamiliar with the required legislation (WA Police).

Overview of Inspections

While we conducted an inspection of each agency's use of the powers under the Act, we only made findings at 5 agencies. The statistics on our findings across these agencies are included in the table below. All our inspection findings are presented by agency in **Appendix A**.

Agency	Inspection Dates	No. of Findings	No. of Recommendations	No. of Suggestions
AFP	March 2024	**7**	1	7
ACIC	April 2024	**2**	5	7
Vic Police	April 2024	**0**	0	0
WA Police	April 2024	**9**	7	5
NACC	May 2024	**1**	0	2
NSW Police	May 2024	**0**	0	0
LECC	June 2024	**5**	0	1

Room to improve

We observed four areas of significant non-compliance in some agency practices requiring immediate attention.

Improving internal safeguards to ensure the ACIC use surveillance devices within intelligence operations lawfully

We are concerned the ACIC's planning documents and internal oversight for intelligence operations were not fully effective and that the ACIC failed to use its policy and procedures to support the lawful use of surveillance devices and computer access powers.

The loss of or potential loss of protected information

We found instances at the AFP and WA Police where warrants and applications or information gathered through surveillance devices and access to data from a computer, was lost or at risk of being lost.

Not reviewing the necessity to retain a warrant

At the ACIC, WA Police and LECC, the reviews of unexecuted warrants were inadequate, with warrants remaining in existence for up to 90 days before expiring.

Staff had insufficient training and were unfamiliar with the legislation

At the WA Police, we found insufficient training and unfamiliarity with the legislation contributed to non-compliance with the Act.

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 (the Attorney-General) at 6 monthly intervals with the results of each inspection conducted during the reporting period. These reports provide transparency to the Attorney-General 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 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.

This report presents our findings on the most significant risks we reviewed, particularly risks that:

- a surveillance device is not deployed and used in a manner consistent with the warrant
- the use of a surveillance device or access to a computer was not for a lawful purpose
- surveillance device records (including protected information) and reports are not appropriately used, communicated or reviewed and destroyed
- timelines for destroying protected information are not adhered to
- appropriate considerations were not given to the necessity and proportionality of using a surveillance device or access to a computer prior to the warrants being sought, and
- governance and policy documents across agencies are not fit for purpose.

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 6-monthly report to the Attorney-General.

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

Good practices

Positively working together to improve compliance

We were pleased to see most agencies continued to positively engage with our Office during the planning and conduct of our inspections. Most agencies were receptive to our feedback on areas for improvement, including instigating remedial actions to implement recommendations and suggestions made from our inspections.

Some agencies were also forthcoming in demonstrating their capabilities and enhancing our awareness of how the powers are applied. The AFP and NACC were two such agencies where technical teams engaged in discussions with our Office to help us better understand the technology used in conjunction with the powers.

Many agencies were open and frank in their conversations with our Office. Where non-compliance was identified by the agency, we found many agencies were proactive in disclosing these instances and had commenced remedial measures to manage the non-compliance risks, including improvements to their processes and practices. We consider proactive disclosure of non-compliance and self-initiation of remedial actions to be indicators of a good compliance culture.

Continuous review and updating of governance and procedures

We were pleased to observe the AFP, Victoria Police and the LECC continued to review and update their governance, procedures and templates in response to our feedback and instigate processes for internal continuous improvement. For example, the AFP were proactive in reviewing their governance, training and internal quality controls to ensure they remained fit for purpose.

At Victoria Police, we noted the agency had updated templates to demonstrate the necessary considerations when using and retrieving tracking devices without a warrant. Although Victoria Police did not use the powers during our inspection period, we were pleased by the action taken in response to our previous feedback, and their proactive approach towards improving their compliance and maintaining operational readiness to use the powers.

Sharing lessons in compliance

We saw several instances of information sharing between agencies on lessons learnt and better practices in administering the powers. This included sharing technical and procedural advice to benefit the collective understanding of, and compliance with, the Act. Agencies consulted with each other to improve consistency in compliance activities, particularly by reviewing or developing policy and procedure documents. This behaviour promotes a positive compliance culture which reduces the risk of non-compliance and helps to ensure the powers are administered consistently.

Our March 2024 report noted considerable efforts by the NACC to review and update its governance framework, training and procedures during its transition from the Australian Commission for Law Enforcement Integrity (ACLEI). We considered this was indicative of a maturing compliance culture. We were pleased to see the NACC was working with other agencies to review and improve their procedures and training. This included assisting agencies to update their policy, procedures and templates.

Similarly, the AFP were proactive in sharing information with other police technical teams to improve compliance controls. Lessons learnt by the AFP through the use of certain technologies was shared to help reduce the risks of other agencies inadvertently not complying with the Act.

Progress in reviewing and destroying protected information

Our March 2024 report highlighted our concerns about the inadequate review and destruction of protected information held by the ACIC. We did not agree with the ACIC's previous position that it would take up to 7 years to review legacy protected information for which the ACIC was unlikely to have a lawful purpose to retain.

We were pleased with the efforts by the ACIC to respond to our recommendations. During our inspection, the ACIC advised that all legacy protected information had been identified and was scheduled to be reviewed and, where necessary, destroyed by 30 June 2024.

On 28 June 2024, the ACIC confirmed that all identified records had been reviewed, with records no longer required for a purpose under the Act being destroyed. We will examine the ACIC's records to retains or destroy these records during our next inspection.

What can agencies improve on?

We observed six areas of non-compliance in some agency practices requiring attention.

Improving internal safeguards to ensure the ACIC use surveillance devices or access data on a computer within intelligence operations lawfully

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 the identity or location of the offenders[1].

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

At past inspections, we were satisfied that the information contained in the applications and affidavits specified that the surveillance devices or accessing data on a computer would be used for an investigative purpose. This inspection was the first time we compared the applications and affidavits with the decisions and plans made by investigators and requesting officers for their intended use of surveillance devices or computer access powers.

[1] 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.

We found the ACIC had a robust governance and policy framework in place to allow officers to use these powers in connection with investigating a relevant offence. This framework reinforced the need for any surveillance device or access to data on a computer, to enable evidence to be obtained of a relevant offence, or the identity or location of the offenders.

However, in practice, we found planning documents and internal oversight were not fully effective.

An internal operations committee considers submissions for the commencement, prioritisation, extension, review, change or cessation of ACIC projects, and approves the intention to use any covert powers (including the use of surveillance devices or access to data on a computer) when it endorses the project proposal prior to commencing an Intelligence Operation. The project proposal must specify the powers that are intended to be used and the purposes (being project objectives and outputs) for which the powers will be applied. The project proposal that is endorsed by the committee does not authorise the particular use of surveillance devices or computer access powers. That is done through a separate authorisation process.

We reviewed endorsed planning project proposals and project extensions across 2 intelligence operations that used surveillance devices or computer access powers. We thought there needed to be a better linkage between the use of surveillance devices or accessing data on a computer, to assist in connection with investigating a relevant offence with the intended deliverables set out in these proposals.

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

During our inspection, we made some general observations which indicated that the link with the threshold for being able to use surveillance devices or accessing data on a computer was not always clear. We also appreciate that the line which can distinguish between intelligence activities and the investigation of offences is not clear. Accordingly, we have not yet concluded our view on whether the ACIC has been able to adequately

demonstrate a connection between the use of surveillance devices or accessing data on a computer, and the thresholds under the Act. We will explore this further at our next inspection.

We made 5 **recommendations** to improve the ACIC's internal safeguards to ensure surveillance devices or computer access powers are used lawfully within intelligence operations.

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

Failing to secure and account for protected information

Protected information is any information relating to the existence of, or obtained from, a surveillance device or by accessing a computer with a warrant. In broad terms, it includes:

- any information obtained from the use of a surveillance device or access to a computer under a warrant or authorisation
- 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.

Section 46 of the Act provides an important safeguard through the requirement for a chief officer to ensure all records and reports comprising protected information are kept in a secure place. An agency must demonstrate they have adequate controls in place to secure protected information.

The AFP disclosed two incidents of protected information being lost in transit, the first being in 2022 and another in 2023. One incident involved the loss of information relating to AFP members and a law enforcement investigation. The second contained sensitive and personal information.

We found the AFP's efforts to investigate the incidents were inconsistent and insufficient. The AFP conducted a harm assessment with one incident, deciding that no further action was required. The second incident was not subject to any harm assessment.

The loss of this protected information was serious non-compliance. We were not satisfied the AFP made adequate efforts to understand the causes of the non-compliance, review the adequacy of existing controls or implement measures to reduce the risk of reoccurrence.

We **recommended** that the AFP conduct a full investigation into the incidents of loss of protected information and review all processes relating to the secure storage, transportation of all physical records.

In response to our findings, the AFP advised they accepted our recommendation and noted that some of the warrants have since been located.

At WA Police, we were concerned that protected information gathered through surveillance devices or accessing data held on computers, could be lost or misused through their practice of using insecure and untraceable storage devices. WA Police could not monitor or limit the downloading, sharing or use of protected information downloaded onto these devices. Additionally, WA Police could not account for any use or communication of information downloaded onto these devices or assure that the devices would be held in secure and auditable locations.

We **recommended** that WA Police immediately cease providing and securing protected information on insecure, untraceable and unaudited external storage devices. We also **recommended** that WA Police identify and account for the use, disclosure, destruction and retention of any protected information that has been provided to WA Police staff or other agencies on an external storage device.

We were not satisfied WA Police's practices met the conditions under section 51 of the Act, which requires protected information obtained by using a surveillance device or accessing a computer, to be kept in a secure place that is not accessible to people who are not entitled to deal with the information.

This is a repeat finding for WA Police and we remain concerned with the use of external devices to store and transport protected information. We made 3 recommendations to improve their controls around storing, using and accounting for protected information in their possession.

We **recommended** WA Police immediately review and update its policies and procedures to ensure technical teams and investigators are aware of their obligations and the process for using, disclosing, destroying or requesting retention of protected information.

The WA Police accepted our recommendations and is taking steps to address this issue.

Not investing in building and retaining compliance knowledge

Developing compliance expertise through training and knowledge sharing is vital to ensuring an agency understands and applies practice that are compliant with Act.

At WA Police we found that investigative and compliance staff were unfamiliar with their Standard Operating Procedures (SOPs), and training in the use of the powers was insufficient, irregular and optional. We noted compliance staff and investigators held inconsistent and inaccurate understandings of their obligations under the Act. For example, some areas did not understand their obligations with respect to revoking warrants and were unable to locate records of any warrant revocations.

We **recommended** WA Police immediately develop and deliver mandatory training for investigators and compliance staff on their obligations under the Act.

The WA Police accepted our recommendation and is taking steps to address this issue.

Failure to review unexecuted warrants

We saw instances at the ACIC, WA Police and LECC where the necessity to retain unexecuted warrants was not regularly considered.

The execution of a surveillance device or computer access warrant can rely upon circumstances at the time and may not be executed shortly after the warrant is issued. Law enforcement officers using the powers should regularly turn their mind to the ongoing necessity of the warrant and the viability of being able to execute the warrant prior to its expiry (particularly in case where the warrant is issued for a lengthy period).

If the use of a surveillance device under a warrant 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 under a warrant 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.

At WA Police we found 6 of the 11 warrants obtained were unexecuted, with 3 left to expire after 45 days and 8 left to expire after 90 days. No warrants were revoked and there were no records of any reviews or decisions to retain the unexecuted warrants.

WA Police did not have adequate procedures for investigators to review unexecuted warrants. We noted instances where investigators believed warrants had been revoked but there was no record to show they had been, and the report to the Minister under section 49 of the Act stated the warrant had expired. Further to the need to increase investigator and compliance staff's knowledge of revocation requirements, we also noted deficiency in records kept of warrant revocations under the Act.

We **recommended** WA Police conduct comprehensive process updates for compliance and investigation teams as they relate to revocations to ensure warrants are revoked correctly and sufficient records are kept demonstrating compliance with revocation requirements.

The WA Police accepted our recommendation and is taking steps to address this issue.

The ACIC advised that investigators regularly review warrants and record any decisions to revoke or retain a warrant. Of the 5 warrants we inspected 3 warrants were left to expire having not been executed during the 90-day period. There were no records of any review or decision to retain the unexecuted warrants or explanation of why the warrants had not been executed.

We suggested the ACIC should conduct regular reviews of unexecuted warrants and record decisions to retain or revoke them. The ACIC accepted our suggestion and committed to reviewing and updating its warrant management practices.

We identified 2 warrants at the LECC that had expired after having not been executed during the 90-day warrant period. The LECC's records did not sufficiently demonstrate the warrants were reviewed and needed to be retained. We acknowledge these warrants

expired prior to LECC updating its processes, which now require these considerations and decisions to be recorded.

Delays in destroying protected information

We noted delays in the destruction of protected information at the NACC caused by reliance on third parties to carry out the destruction.

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 of the Act is a key safeguard in the legislation, and we consider it responsible practice by agencies to review the need to retain such information at the completion of any related civil or criminal proceedings. If the material is retained post these proceedings for a purpose under the Act, then the agency should review the material within 5 years of obtaining the protected information.

Where an agency has decided it no longer requires the information, they must destroy it as soon as practicable. We expect agencies to destroy the information within 28 days of the records being authorised for destruction.

We observed an instance at the NACC where protected information was held by a partner agency and not destroyed for 61 days after its destruction was authorised. We suggested the NACC work with its partner agencies to ensure material authorised for destruction is destroyed within 28 days. We also suggested the NACC update their procedures to include this timeframe for destroying records. The NACC accepted our suggestions.

Our March 2024 report noted limitations in some case management systems to permanently delete protected information and records, including at the LECC. While we noted these limitations had not been resolved at the time of our inspection, the LECC advised after the inspection that this functionality has been delivered and is fully operational. We will review the functionality of the system at the next inspection.

Delays and inaccuracies in reports to the Minister

As soon as practicable after a warrant or authority ceases to be in force, section 49(1) of the Act requires the Chief Officer to make a report to the Minister. During our inspections we identified instances of either delays or inaccuracies within some reports provided to the Minister.

The LECC disclosed that reports to the Minister were not sent until up to 159 days after the warrant or authority had ceased. The LECC advised they identified the issue and implemented measures to ensure reports would be submitted in time. This included amending LECC's policy and guidance material to comply with the Act.

We identified 2 instances at WA Police where information reported to the Minister was inconsistent with the information on WA Police records. This included incorrect information about the revocation of warrants. We suggested WA Police amend these reports and resubmit to the Minister. WA Police accepted our suggestions and are taking steps to address the issues identified.

Appendix A

Table of reported inspection findings by agencies for the period 1 January 2024 to 30 June 2024

The 5 tables below, outline significant findings for our inspections for the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC), the Western Australian Police Force (WA Police), the National Anti-Corruption Commission (NACC) and the Law Enforcement Conduct Commission (LECC) between 1 January 2024 and 30 June 2024.

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.

The following findings do not include administrative issues or instances of non-compliance where the consequences are low risk and of minimal impact to the community.

Table 1: Findings at the AFP – significant findings only

AFP - March 2024 Inspection

	Findings	Agency Response
1	**We identified incidents where protected information was lost in transit between AFP Offices.** **Recommendation 1:** The AFP immediately conduct a full investigation into the incidents and review its procedures for the secure storage, transportation and tracking of physical warrants, affidavits and any other records containing protected information. This includes implementing measures to ensure physical records are not lost or unaccounted for while being transported. **Suggestion 1:** AFP should ensure that it has a clear understanding of what amounts to a notifiable data breach to the Office of the Australian Information Commissioner (OAIC), and that when a breach occurs, an assessment is made as to whether the breach is notifiable.	The AFP accepted the recommendation and suggestion.
2	**AFP surveillance device affidavits did not accurately reflect the impacts on the privacy of third parties.** **Suggestion 2:** The AFP review its affidavit templates to ensure sufficient prompts are in place to enable applicants to identify impacts on third parties. This includes ensuring applicants provide sufficient explanation of how any impacts on the privacy of a third party will be mitigated or managed.	The AFP accepted this finding and the suggestions.

	Findings	Agency Response
	Suggestion 3: The AFP should ensure that affidavits accurately reflect the impacts of any use of the powers on the privacy of the target and third parties, and that the affidavit identifies appropriate measures to mitigate or manage these privacy impacts.	
3	**Collection of data outside warrant parameters was not communicated to the appropriate internal team.** **Suggestion 4:** The AFP should take steps to prevent over collection of data and ensure all instances of non-compliance identified are disclosed to the appropriate internal team.	The AFP accepted this finding and suggestion.
4	**Failure to record and adequately respond to considerations made by the AFP internal oversight body.** **Suggestion 5:** AFP review the reasons why the outcomes from the AFP internal oversight body were not actioned before proceeding with an application for a warrant. This should include examining the role and authority of the body to limit affidavits and warrants from proceeding where: - insufficient grounds exist to support the issuing of a warrant - the warrant is not necessary to achieve the investigation outcome, or - a more proportionate and reasonable alternative line of inquiry could be pursued by the investigation.	The AFP accepted this finding, suggestion and comment.

	Findings	Agency Response
5	**Failure to revoke duplicated warrants.** **Suggestion 6:** AFP should review the causes of the duplicate warrants not being immediately revoked when the error was identified. This should include mitigating any risks of a duplicate warrant being produced and ensuring procedures are in place to immediately revoke the duplicate warrant.	The AFP accepted this finding and suggestion.
6	**Decision to retain data made after expiry of the five-year retention period.** **Suggestion 7:** AFP should implement notification mechanisms to review material and make a decision on its retention or destruction prior to the expiry of the initial 5-year retention period.	The AFP accepted this finding and suggestion.

Table 2: Findings at the ACIC – significant findings only

ACIC - April 2024 Inspection

	Findings	Agency Response
1	**Internal safeguards should be improved to ensure the ACIC use covert powers within Special Operations lawfully**	
	Recommendation 1: The ACIC review its framework of governance, policies and procedures to ensure that staff do not use surveillance device and computer access powers for intelligence purposes that would not meet legislative thresholds.	The ACIC accepted our recommendation.
	Recommendation 2: If an intelligence operation uses surveillance device and computer access powers, the ACIC ensure that it can demonstrate that the deliverables from the operation include an investigative purpose.	The ACIC accepted our recommendation in part.
	Recommendation 3: The ACIC Operations Strategy Forum must ensure any extensions to an Intelligence Operation expressly include the approval to continue using the surveillance device and computer access powers.	The ACIC accepted our recommendation.
	Recommendation 4: ACIC should review and, where necessary, update its training to ensure staff are aware of and understand the boundaries of the lawful purposes for which surveillance device and computer access powers can be used.	The ACIC accepted our recommendation.
	Recommendation 5: The ACIC implement measures to ensure that it can demonstrate that the use of surveillance device and computer access powers are used within a	The ACIC accepted our recommendation in part.

Findings	Agency Response
continuum of investigating and prosecuting a relevant offence. This should include reviewing how the ACIC records its use of the powers, and supports partner agencies investigation of relevant offences.	
Suggestion 1: The ACIC obtain legal advice specifically upon the actual use of surveillance device and computer access powers in the operations we inspected and whether those uses had in practice a sufficient connection to the legislative thresholds.	The ACIC accepted our suggestion in part.
Suggestion 2: The ACIC engage with the Attorney-General's Department to assess options for legislative reform to reduce the risk of non-deliberate unlawful use of surveillance device and computer access powers associated with the gathering and reporting of intelligence.	The ACIC accepted our suggestion.
Suggestion 3: In support of **Recommendation 2,** the intended outputs in project proposals and extensions for Intelligence Operations should include deliverables that at a non-theoretical level enable an investigative purpose.	The ACIC accepted our suggestion in part.
Suggestion 4: ACIC should ensure all staff receive training on the application of the ACIC Intelligence Operations Management Model and related policy and procedures.	The ACIC accepted our suggestion.
Suggestion 5: Senior Responsible Officers (SRO) or other key decision makers should record decisions and outcomes on the Intelligence Operations Management System (IOMS) from meetings relating to the use, monitoring and review of more intrusive powers, including surveillance devices and computer access powers.	The ACIC accepted our suggestion.

	Findings	Agency Response
	Suggestion 6: ACIC compliance staff should be included in SRO and intelligence team planning and management meetings for Intelligence Operations. Compliance staff should provide advice to the SRO and intelligence team on matters impacting the lawful use of surveillance device and computer access powers within the Intelligence Operation.	The ACIC accepted our suggestion.
2	**Warrants were not reviewed and were allowed to expire instead of being revoked** **Suggestion 7:** The ACIC develop and implement regular reviews of unexecuted warrants, including recording the outcomes from the review and any decisions and considerations to retain or revoke a warrant.	The ACIC accepted our suggestion.

Table 3: Findings at the Western Australian Police Force (WA Police) – significant findings only

WA Police - April 2024 Inspection

	Findings	Agency Response
1	**WA Police do not have sufficient records connected with surveillance device warrants, including how they use and disclose protected information (PI).** **Recommendation 1:** WA Police immediately review and implement a centralised system and supporting process to keep records to satisfy the requirements under sections 45, 51 and 52 of the Act.	WA Police accepted the recommendation.
2	**Serious risk of Protected Information being lost through the use of unsecure external storage devices and an inadequate ability to audit or trace Protected Information downloaded from WA Police systems (repeat finding).** Recommendation 1 also applies to this finding. **Recommendation 2:** WA Police immediately cease providing and securing protected information on unsecure, untraceable and unaudited external storage devices. **Recommendation 3:** WA Police identify and account for the use, disclosure, destruction and retention of any protected information that has been provided to WA Police staff or other agencies on an external storage device	WA Police accepted the recommendations and suggestions.

	Findings	Agency Response
	Recommendation 4: WA Police immediately review and update its policies and procedures to ensure teams are aware of their obligations and the process for using, disclosing, destroying or requesting retention of protected information **Suggestion 1:** WA Police should commence an internal process to audit access to their storage system, including accounting for any material downloaded from the system. **Suggestion 2:** WA Police should review the device retrieved by another law enforcement agency and ensure any protected information captured has been accurately recorded and managed (including any use of protected information). **Suggestion 3:** WA Police should immediately communicate to staff their obligations under the Act and need to record any use, disclosure, destruction or requested retention of protected information.	
3	**Insufficient training to investigative and compliance staff, with staff being unfamiliar with Commonwealth Surveillance Device legislative requirements or WA Police policies and procedures (repeat finding).** **Recommendation 5:** WA Police immediately develop and deliver mandatory training packages for staff in relation to all the compliance requirements under the Act. Records should be kept of the training and be produced at the next inspection.	WA Police accepted the recommendation.

	Findings	Agency Response
4	**WA Police staff were uncertain of revocation procedures for surveillance device warrants and applied inconsistent practices when revoking surveillance device warrants (repeat finding).** **Recommendation 6:** WA Police update its compliance processes to ensure requests to revoke warrants are received, recorded and actioned	WA Police accepted the recommendation.
5	**Warrants were not being reviewed and were allowed to expire instead of being revoked (repeat finding).** **Recommendation 7:** 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 the recommendation.
6	**Errors in the report that is required to be sent to the Minister when using a surveillance device warrant** **Suggestion 4:** WA Police should advise the Minister of the inaccuracies in the s 49 reports.	WA Police accepted the suggestion.

	Findings	Agency Response
7	**Inadequate compliance knowledge and expertise within the compliance team** **Suggestion 5:** The compliance team immediately receive training, and development opportunities to build their subject matter expertise and knowledge of legislative requirements under the Act.	WA Police accepted the suggestion.

Table 4: Findings at the National Anti-Corruption Commission (NACC) – significant findings only

NACC - May 2024 Inspection

	Findings	Agency Response
1	**The destructions of protected information from SD Warrants did not occur 'as soon as practicable'** **Suggestion 1:** The NACC work with relevant partners to implement an agreement or contingency to ensure material authorised for destruction is destroyed 'as soon as practicable'. **Suggestion 2:** The NACC update their Surveillance Device and Destructions procedures to include an internal timeframe for destroying records 'as soon as practicable'.	The NACC acknowledged this finding and accepted the suggestions

Table 5: Findings at the Law Enforcement Conduct Commission (LECC) – significant findings only

LECC – June 2024 Inspection

	Findings	Agency Response
1	**LECC case management systems limitations in being able to destroy SD records (repeat finding)** **Suggestion 1:** The LECC should develop a firm plan of what is required for the destruction capability to become operational within their record management system and provide a timeline of when this will occur.	LECC acknowledged this finding and accepted the suggestion. The capability is now operational and fully functional.
2	**Errors in the report that is required to be sent to the Minister when using a surveillance device warrant** **Comment 1:** We acknowledge the nature of the error and note the response by the LECC in amending policy and procedure documents. We will monitor the effectiveness of these measures at our next inspection.	LECC acknowledged this finding and accepted the comment
3	**Insufficient records of decisions relating to reviewing and retention of an surveillance device warrant** **Comment 2:** We acknowledge the steps the LECC has made to address our concerns and have critical decisions captured within the records. We note that the warrants reviewed expired prior to the implementation of these changes and therefore we were unable to	The LECC had implemented procedural and technical changes prior to the inspection.

	Findings	Agency Response
	observe the changes in practice. We will monitor the progress of this finding at our next inspection.	
4	**The warrant register did not accurately calculate the 5-year retention period for material gathered through surveillance device warrants** **Comment 3:** It is our view that the LECC should amend the Commonwealth SD warrant register and any associated documentation to calculate the 5-year period from the commencement of the warrant.	LECC acknowledged this finding and accepted the comment

Appendix B:

Table 1 – Agencies inspected remotely

Agency
Queensland Police Service (QLD Police)
South Australia Police (SA Police)
Tasmania Police (Tasmania Police)
Northern Territory Police Force (NT Police)
Crime and Corruption Commission Queensland (CCC QLD)
Corruption and Crime Commission Western Australia (CCC WA)
Independent Broad-based Anti-Corruption Commission (IBAC)
Independent Commission Against Corruption NSW (ICAC NSW)
Independent Commission Against Corruption SA (ICAC SA)
NSW Crime Commission (NSW CC)

Table 2 – Summary of records inspected on site

Agency	Records available	Records inspected
Law Enforcement Conduct Commission (LECC)	2 x SD	2 x SD
NSW Police	1 x SD	1 x SD
National Anti-Corruption Commission (NACC)	13 x SD	13 x SD
Australian Criminal Intelligence Commission (ACIC)	12 x SD 1 x TDA 1 x CAW	5 x SD 1 x CAW

Vic Police	2 x SD	2 x SD
AFP	343 x SD 1 x RSD 4 x SO 11 x RW 49 x D 51 x DNE 148 x R	29 x SD 1 x RSD 4 x SO 2 x RW 2 x D 3 x DNE 3 x R
WA Police	11 x SD	11 x SD

Key	SD	Surveillance device warrant
	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	Retained