COMMONWEALTH OMBUDSMAN

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004* (Cth)

For the period 1 January to 30 June 2021

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July to 31 December 2020

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July to 31 December 2020

VICTORIA POLICE
Records from 1 July 2019 to 30 June 2020

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2020

WESTERN AUSTRALIA POLICE
Records from 1 July 2017 to 30 June 2020

Report by the Acting Commonwealth Ombudsman,
Penny McKay,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

September 2021

Report to the Minister for Home Affairs on agencies' compliance with the *Surveillance Devices Act 2004* (Cth)

For the period 1 January to 30 June 2021

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July to 31 December 2020

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 July to 31 December 2020

VICTORIA POLICE
Records from 1 July 2019 to 30 June 2020

AUSTRALIAN FEDERAL POLICE
Records from 1 July to 31 December 2020

WESTERN AUSTRALIA POLICE
Records from 1 July 2017 to 30 June 2020

Report by the Acting Commonwealth Ombudsman,
Penny McKay,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

September 2021

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: ombudsman@ombudsman.gov.au

CONTENTS

EXECUTIVE SUMMARY

This report presents the results of the Office of the Commonwealth Ombudsman's (the Office) inspections conducted under the *Surveillance Devices Act 2004* (the Act) between 1 January to 30 June 2021 (the reporting period).

During the reporting period we inspected the records of the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Criminal Intelligence Commission (ACIC), Victoria Police, the Australian Federal Police (AFP) and the Western Australia Police Force (WA Police). The Office planned to inspect the New South Wales Police Force's records during the reporting period but delayed this inspection due to the impact of COVID-19 restrictions.

Table 1 – Summary of the results of each inspection

Agency	Inspection dates	Summary of results of each inspection
ACLEI	2–4 March 2021	Inadequate recording of actions taken under a warrant and issues with recording use and disclosure of protected information.
ACIC	19–23 April 2021	Two invalid warrants granted by an ineligible authority. In some instances, the ACIC was not compliant with destruction requirements. Inadequate recording of actions taken under a warrant.
AFP	3–7 May 2021	Five invalid warrants and 3 extensions granted by an ineligible authority. We found the AFP conducted several hours of surveillance without a warrant and disclosed one instance of conducting data surveillance in the absence of a warrant. We also found inadequate recording of actions taken under a warrant.
Victoria Police	3–7 May 2021	Insufficient training or guidance materials to support compliance under the Act.
WA Police	24–27 May 2021	WA Police did not revoke warrants as required by the Act and we found protected surveillance product stored on insecure unencrypted devices.

Part 1: SCOPE AND METHODOLOGY

Introduction

1.1. The *Surveillance Devices Act 2004* (the Act) restricts the use, communication and publication of information obtained by using surveillance devices and through access to data held in computers.

1.2. The Act imposes requirements on agencies to store and destroy protected information they obtain by using surveillance devices or through computer access activities. The Act restricts the way agencies may use, communicate, or publish such information and requires them to provide reports about these covert activities.

Our oversight role

1.3. Section 55(1) of the Act requires the Commonwealth Ombudsman (the Ombudsman) to inspect the records of a law enforcement agency to determine the extent of compliance with the Act.

1.4. Section 61(1) of the Act requires the Ombudsman to provide reports to the Minister for Home Affairs at 6 monthly intervals with the results of each inspection. These reports provide transparency to the Minister and the public about how agencies use these intrusive powers.

How we oversee agencies

1.5. Our Office uses the same inspection methodology across all agencies. This methodology is based on legislative requirements and best practice standards. Further detail about our inspection criteria and methodology is provided in **Appendix A**.

1.6. To ensure procedural fairness, we give agencies the opportunity to respond to our draft inspection findings. We then sanitise and consolidate the significant findings into our report to the Minister.

1.7. We may also report on matters that do not relate to specific instances of non-compliance, such as the adequacy of an agency's policies and procedures to demonstrate compliance with the Act. We do not generally report on administrative issues or instances of non-compliance where the consequences are negligible.

Part 2: AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

2.1. From 2 to 4 March 2021, we inspected ACLEI's surveillance device records.

Inspection details

2.2. We inspected records of warrants and authorisations that expired between 1 July and 31 December 2020.

Type of record	Records made available	Records inspected
TOTAL	**18**	**14 (78%)**

2.3. The available records consisted of 14 surveillance device warrants and 4 retentions of protected information.

Progress since our previous inspection

2.4. We made no findings of note during our previous inspection of ACLEI records.

Inspection findings

Finding – Not keeping records for each use or communication of protected information

2.5. We identified 3 instances where the ACLEI did not keep accurate records of each use and disclosure of protected information as required by s 52 of the Act.

2.6. We suggested the ACLEI update the 3 warrant records with the missing information. Following the inspection, the ACLEI advised it had updated the 3 files. We will review the ACLEI's remedial action during our next inspection.

2.7. As the ACLEI relies on external assisting agencies to execute surveillance device warrants on its behalf, as a matter of better practice we suggested the ACLEI engage with external assisting agencies to explore avenues to fulfil its record keeping obligations under s 52 of the Act. The ACLEI stated it will update its Standard

Operating Procedures and require Case Officers to engage with external assisting agencies to address this suggestion.

Finding – Inadequate recording of actions taken under a warrant

2.8. The Office relies on contemporaneous records, often called 'action sheets', to verify that actions taken accord with the authority provided by a warrant as covered by s 18 of the Act.

2.9. Action sheets are a key record demonstrating agencies' use of surveillance devices on specified premises or adjoining premises. They are completed by investigators and those carrying out the actions of installing, retrieving, and maintaining a device, or 'activating' and 'de-activating', depending on the type of device. The ACLEI relies on these action sheets to compile reports for the Minister under s 49 of the Act.

2.10. We identified action sheets in relation to 4 surveillance device warrants with insufficient or vague details. This included vague or inconsistent details about the surveillance devices, and the addresses or adjoining premises where devices were installed.

2.11. We suggested the ACLEI remind relevant officers of the importance of including appropriate detail in action sheets so that it can demonstrate all actions authorised by a warrant consistent with s 18 of the Act and ensure the reporting to the Minister under s 49 is accurate.

2.12. The ACLEI accepted this suggestion, advising this would be managed by case officers during engagement with the assisting agency and addressed in its Standard Operating Procedures.

Part 3: AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

3.1. From 19 to 23 April 2021, we inspected the ACIC's surveillance device records.

Inspection details

3.2. We inspected records of warrants and authorisations that expired between 1 July and 31 December 2020.

	Records made available	Records inspected
TOTAL	**135**	**51 (38%)**

3.3. The available records consisted of 72 surveillance device warrants, 3 computer access warrants, one retrieval warrant, 8 tracking device authorisations, 48 destructions of protected information and 3 retentions of protected information.

Progress since our previous inspection

3.4. We last publicly reported inspection results for the ACIC in our March 2021 report to the Minister. That report included findings in relation to non-compliance with destruction provisions.

3.5. We identified further non-compliance with the destruction provisions of the Act during our most recent inspection at the ACIC, with relevant findings included below.

Inspection findings

Finding – Warrants issued by an ineligible authority

3.6. We identified 2 ACIC surveillance device warrants that were invalid because they were issued by a judge who was not an eligible judge.

3.7. The judge who purported to issue the 2 invalid warrants had not consented to being an eligible judge, nor was the judge declared in writing by the relevant Minister to be eligible as required by s 12 of the Act.

3.8. Following the inspection, the ACIC confirmed that no additional warrants, other than the 2 surveillance device warrants identified,

were issued by an ineligible judge. The ACIC quarantined the protected information obtained from the devices and prepared addenda to the previous reports to the Minister.

Finding – Protected information not destroyed as soon as practicable or within 5 years of being made

3.9. The ACIC's non-compliance with destructions requirements was raised with the ACIC at inspections dating back to February 2017 (regarding records from 1 July to 31 December 2016).

3.10. At this inspection, there were 11 instances where the ACIC did not destroy protected information within 28 days of the destruction instrument being signed, which is the ACIC's timeframe for ensuring destructions are completed 'as soon as practicable' in accordance with s 46(1)(b)(i) of the Act.

3.11. The ACIC disclosed 9 instances of protected information not being destroyed within 5 years of being made as required under section 46(1)(b)(ii) of the Act.

3.12. We suggested the ACIC expedite its review of its surveillance device destructions process and in the interim implement specific measures to address difficulties completing destructions within required timeframes once a destruction order is in place.

3.13. As a matter of better practice, we also suggested the ACIC improve investigators' awareness about destruction requirements by improving training and by clearly stating a deadline to finalise the destruction within the destruction order record.

3.14. The public is entitled to expect the collection, analysis, sharing and retention of protected data is balanced and proportionate. The Act provides clear expectations around agencies' collection, retention and use of data, including that this data is destroyed within 5 years if no longer needed for a permitted purpose.

Finding – Inadequate recording of actions taken under a warrant

3.15. The Office relies on contemporaneous records, often called 'action sheets', to verify that actions taken accord with the authority provided by a warrant as covered by s 18 of the Act.

3.16. Action sheets are a key record demonstrating agencies' use of surveillance devices on specified premises or adjoining premises.

They are completed by investigators and those carrying out the actions of installing, retrieving, and maintaining a device, or 'activating' and 'de-activating', depending on the type of device. The ACIC relies on these action sheets to compile reports for the Minister under s 49 of the Act.

3.17. We identified 3 instances where action sheets did not provide sufficient information about actions taken under the warrant. As such, we could not determine whether the devices were used in accordance with the authority of the warrant.

3.18. We suggested the ACIC inform staff involved in covert operations of their obligations to record particulars of the device/s deployed, the installation, maintenance and retrieval times, and device serial numbers. Recording such information will assist the ACIC in ensuring its s 49 reports to the Minister are accurate.

Part 4: AUSTRALIAN FEDERAL POLICE

4.1. From 3 to 7 May 2021, we inspected the AFP's surveillance device records.

Inspection details

4.2. We inspected records of warrants and authorisations that expired between 1 July and 31 December 2020. We also inspected records relating to the AFP's management of protected information during this period.

	Records made available	Records inspected
TOTAL	**1043**	**107 (10%)**

4.3. The total available records included 489 surveillance device warrants, 7 control order warrants, 4 computer access warrants, 9 retrieval warrants, 19 tracking device authorisations, 332 "destructions"[1] of protected information and 183 retentions of protected information.

Progress since previous inspection

4.4. We last publicly reported inspection results for the AFP in our March 2021 report to the Minister. In that report we made several compliance findings, some of which we made again at our May 2021 inspection.

Inspection findings

Disclosure – Information collected in the absence of a warrant

4.5. The AFP disclosed one instance where a data surveillance device was deployed in the absence of a warrant (under an internal tracking device authorisation (TDA)).

4.6. The AFP advised tracking information returned from the device was used to progress an investigation because it enabled AFP to identify a

[1] The number of "destructions" reported to our Office included warrants where the surveillance device warrant was either not executed or no product was obtained and therefore, there was no protected information to destroy.

nexus to another investigation. Information was also used to map location in daily situational reports. The AFP acknowledged and disclosed the issue noting that combination or data devices require a warrant.

4.7. We suggested the AFP seek advice about how to manage use of tracking information from data devices or combination devices in circumstances where these were deployed through internal authorisations instead of warrants.

Finding – Information collected outside authority of warrant

4.8. There were 2 further instances where the AFP collected data outside the authority of a warrant.

4.9. In the first instance the AFP deployed the surveillance device on the target more than 8 hours prior to a warrant being issued. We suggested the AFP quarantine information obtained in the absence of a warrant and cease any further use and communication of the protected information.

4.10. The AFP advised the initial deployment did not require a warrant because it did not involve trespass and was undertaken pursuant to s 37 of the Act as the optical surveillance device was used in an outside common area of an industrial complex open to and used by the public.

4.11. The AFP further advised it subsequently obtained a warrant because while the device was deployed in a similar location, it was assessed that the use could be interpreted as a trespass as the device remained overnight in an area that was locked outside of business hours.

4.12. In the second instance, a warrant expired however the surveillance devices continued recording for approximately 3 days after the expiration. On our advice, the AFP quarantined the unauthorised data during the inspection.

Disclosure – Warrants issued by an ineligible authority

4.13. The AFP disclosed 5 invalid warrants that were issued by a judge who was not an eligible judge as required by the Act.

4.14. The judge who purported to issue the invalid warrants had not consented to being an eligible judge, nor were they declared in

writing by the relevant Minister to be eligible as required by s 12 of the Act.

4.15. We made 3 suggestions to the AFP because of this finding:

- The AFP quarantine all information obtained under the invalid surveillance device warrants, cease any further use and communication of the protected information, and seek advice. AFP responded that information was quarantined and not used or communicated.

- The AFP review its surveillance devices register to identify any further surveillance device warrants issued by the ineligible judge. The AFP conducted a review and advised the ineligible judge also authorised 3 extension warrants. The AFP is continuing to review this issue and will provide advice at the next surveillance device inspection.

- The AFP submit addenda to the s 49 reports to the Minister for all warrants and extensions identified as invalidly issued. We will review action taken at the next inspection.

Finding – Inadequate recording of actions taken under a warrant

4.16. The AFP uses action sheets to document how its staff use surveillance devices. All investigators and officers installing, retrieving and maintaining a device, or 'activating' or 'deactivating' a device must complete an action sheet. The AFP relies on action sheets to compile 'Final Effectiveness Reports' which informs its reports to the Minister under s 49 of the Act.

4.17. In our previous report of March 2021, we identified 24 action sheets that did not contain sufficient information for us to assess AFP's compliance with the Act. In our report to the Minister of September 2020 we identified 4 instances where action sheets did not contain sufficient information about how the AFP executed warrants and authorisations. In response to these findings the AFP advised it had enhanced its action sheet quality assurance processes and provided guidance and reminders to staff about the importance of accurately completing action sheets.

4.18. We identified further issues with action sheets during our most recent inspection. In one instance there was no action sheet on file,

while in 6 other instances we found incorrect or insufficient details in action sheets.

4.19. As a matter of best practice, we suggested the AFP improve its action sheet guidance and template to better account for surveillance technologies that are deployed remotely across multiple locations and ensure s 49 reporting to the Minister is accurate.

Finding – Non-compliance with destruction requirements

4.20. At our previous inspection we identified several instances of non-compliance with destruction requirements under s 46(1)(b) of the Act.

4.21. In response the AFP advised it would continue to educate officers on the destruction requirements and timeframes of the Act, noting its internal policy allows one month for staff to complete a destruction once an authorisation is signed. The AFP further advised there are circumstances when this timeframe is not attainable.

4.22. At our most recent inspection we identified 2 instances of protected information not being destroyed or retained within 5 years of being made, contrary to s 46(1)(b)(ii) of the Act.

Finding – Section 49 reports not made to the Minister in accordance with the Act

4.23. We identified several reports to the Minister that were not fully compliant with the requirements of s 49 of the Act.

4.24. One report did not fully address s 49(2)(b)(ix) of the Act because it failed to note the arrest made through use of the warrant. Another report did not detail its inadvertent overseas use over a 2 day period in November 2020. Under ss 49(2)(b)(iv) and (b)(vii) of the Act, the report to the Minister must detail the period and the place the surveillance device was used.

4.25. Five reports did not sufficiently address matters required by s 49(2)(b)(vii) of the Act (details of any premises on or any place at which the device was used) and s 49(2)(b)(viii) of the Act (details of any premises where the object was located when the device was installed).

4.26. The report to the Minister, on the warrant or authorisation ceasing, should be a complete and accurate record of actual surveillance activity under the warrant.

4.27. As a result, we suggested the AFP complete s 49 reporting so the report fully details the actual activities that occurred under a warrant and addresses all matters required under s 49(2)(b) of the Act. This requirement stands for inadvertent non-compliant activity as well as effective operational practice.

Part 5: VICTORIA POLICE

5.1. From 3 to 7 May 2021, we inspected Victoria Police's surveillance device records.

Inspection details

5.2. We inspected records of warrants and authorisations that expired between 1 July 2019 and 30 June 2020.

	Records made available	Records inspected
TOTAL	**3**	**3 (100%)**

5.3. The total available records consisted of one tracking device authorisation and 2 destructions of protected information.

Progress since our previous inspection

5.4. At our previous inspection we made only minor administrative findings.

Inspection results

5.5. Victoria Police has minimal training, policy, guidance, or procedural material about how Commonwealth surveillance device powers are applied for and used and how tracking device authorisations are assessed and given.

5.6. If Victoria Police intends to continue accessing powers under the Act (in addition to using state-based surveillance devices legislation which is not overseen by the Office), it should develop adequate training, guidance, and procedural material to support applying for and using these powers.

Part 6: WESTERN AUSTRALIA POLICE FORCE

6.1. From 24 to 27 May 2021, we inspected WA Police's surveillance device records.

Inspection details

6.2. We inspected records of warrants and authorisations that expired between 1 July 2017 and 30 June 2020.

	Records made available	Records inspected
TOTAL	**12**	**12 (100%)**

6.3. The total available records consisted of 12 surveillance device warrants.

Progress since our previous inspection

6.4. We last publicly reported inspection results for WA Police in our September 2018 report to the Minister. In that report we identified WA Police used unencrypted USB devices to store protected information, and suggested WA Police encrypt USB devices used for storing protected information. WA Police had not taken action to address this suggestion as at our May 2021 inspection.

Inspection findings

Finding – Storing protected information on insecure and unencrypted devices

6.5. During our May 2021 inspection we found protected information was still being stored on unencrypted storage devices. This is contrary to s 46(1) of the Act requiring the chief officer to ensure that every record comprising protected information is kept in a secure place that is not accessible to people who are not entitled to deal with the information.

6.6. We suggested WA Police encrypt its storage devices or use some other means of viewing and sharing protected information returned from a device. WA Police advised data returned from a surveillance device is now stored securely, with only appropriately credentialled

investigators granted access. We will verify WA Police's remedial action at our next inspection.

Finding – Failing to revoke warrants when no longer required

6.7. We observed gaps in WA Police's Standard Operating Procedures (SOPs) in relation to the revocation requirements of the Act. Their SOPs did not define expected timeframes for notifying the chief officer once investigators are aware a device is no longer required, timeframes for revoking a warrant where there is prolonged inactivity or where devices have already been retrieved.

6.8. We identified one executed warrant that should have been revoked under s 20(2) of the Act as it was no longer required for the purpose of obtaining evidence.

6.9. We also found 7 non-executed warrants that were left inactive and expired after 90 days. We were unable to ascertain whether WA Police had a continued need for these warrants.

6.10. We suggested WA Police officers immediately inform the chief officer (or a delegate) if they believe use of a surveillance device under the warrant is no longer necessary for its original purpose. WA Police must also take steps necessary to ensure use of a surveillance device authorised by a warrant is discontinued, consistent with s 21(2) of the Act.

6.11. As matters of better practice, we also suggested WA Police:

- educate relevant officers and investigators about revocation requirements, and
- update its SOPs to include expected best practice timeframes for notifying the chief officer once investigators are aware a device is no longer required, and for revoking a warrant where there has been prolonged (4 weeks or more) inactivity, or a device has already been retrieved or deactivated and there is no intention to re-deploy the device.

6.12. WA Police advised it has taken steps to address our suggestions and better practice suggestions. Actions advised by WA Police include adopting a revocation template, providing investigators with a monthly prompt to ascertain if the warrant is still required and updating its SOPs.

Finding – Non-compliance with requirements to keep records

6.13. During the inspection there were 3 instances where we were not satisfied WA Police kept details of each internal use of information obtained using a surveillance device as required by s 52(1)(e) of the Act.

6.14. We suggested WA Police keep records about each use of protected information to satisfy the requirements in s 52(1)(e) of the Act, and further educate investigators about this requirement and highlight this record keeping requirement in its SOPs.

6.15. In response to this finding WA Police updated its SOPs and 'Final Investigators Report' example to reflect the requirement to keep details of each use of protected information.

APPENDIX A – INSPECTION CRITERIA AND METHODOLOGY

Objective: To determine the extent of compliance with the *Surveillance Devices Act 2004* (the Act) by the agency and its law enforcement officers (s 55).

1. Was appropriate authority in place for surveillance or data access activity?

1.1. Did the agency have the proper authority for using and/or retrieving the device?

Process checks:

- What are the agency's procedures to ensure that surveillance device warrants and retrieval warrants are properly applied for, and are they sufficient?
- What are the agency's procedures to ensure that tracking device authorisations and emergency authorisations are properly issued, and are they sufficient?
- What are the agency's procedures for seeking extensions and variations of warrants, and are they sufficient?
- What are the agency's procedures for revoking surveillance device and retrieval warrants, and are they sufficient?

Records based checks

We inspect applications, warrants, authorisations, variations, and other agency records to assess whether:

- applications for surveillance device warrants were made in accordance with s 14 of the Act
- applications for extensions and/or variations to surveillance device warrants were made in accordance with s 19 of the Act
- applications for retrieval warrants were made in accordance with s 22 of the Act
- applications for emergency authorisations and subsequent applications to an eligible judge or a nominated Administrative Appeals Tribunal member were made in accordance with ss 28, 29, 30 and 33 of the Act
- written records for emergency authorisations were properly issued in accordance with s 31 of the Act
- applications for tracking device authorisations and retrieval of tracking devices were made in accordance with s 39 of the Act
- tracking device authorisations were properly issued in accordance with s 39 of the Act, and recorded in accordance with s 40 of the Act

1.2. Did the agency have proper authority for computer access/data access activities?

Process checks:

- What are the agency's procedures to ensure that computer or data access warrants, authorisations, extensions, and variations are properly applied for, and are they sufficient?
- What are the agency's procedures to ensure that emergency authorisations for computer access activity are properly issued, and are they sufficient?
- What are the agency's procedures for seeking extensions and variations of warrants, and are they sufficient?

Records based checks

We inspect applications, warrants, authorisations, variations, and other agency records, to assess whether:

- applications for computer access warrants were made in accordance with s 27A or s27B if a remote application of the Act
- applications for extensions and / or variations to computer access warrants were made in accordance with s 27F of the Act
- applications for emergency authorisations and subsequent applications to an eligible judge or a nominated Administrative Appeals Tribunal member were made in accordance with ss 28, 29, 30 and 33 of the Act
- written records for emergency authorisations were properly issued in accordance with s 31

1.3. Were warrants and authorisations properly revoked?

Process checks:

- What are the agency's procedures to ensure that surveillance device warrants are properly revoked, and are they sufficient?
- What are the agency's procedures to ensure that computer access warrants are properly revoked, and are they sufficient?
- What are the agency's procedures for ensuring that use of surveillance devices is discontinued, and are they sufficient?
- What are the agency's procedures for ensuring that computer access/data access activity is discontinued, and are they sufficient?

Records based checks

We inspect agency records, to assess whether:

- surveillance device warrants were revoked in accordance with s 20, and discontinued in accordance with s 21 of the Act
- computer access warrants were revoked in accordance with s 27G, and discontinued in accordance with s 27H of the Act

2. Was surveillance or data activity in accordance with the Act?

2.1. Were surveillance devices used and/or retrieved in accordance with the authority of warrants or in accordance with the provisions of the Act?

Process checks:

- What are the agency's procedures to lawfully use surveillance devices, and are they sufficient?
- What are the agency's procedures for using surveillance devices without a warrant, and are they sufficient?
- Does the agency have an auditable system for maintaining surveillance devices?
- What are the agency's systems and /or records capturing the use of surveillance devices, and are they sufficient?
- What are the agency's procedures for ensuring warrant conditions are adhered to, and are they sufficient?

Records based checks

We inspect the records and reports relating to the use of surveillance devices against corresponding authorisations and warrants, to assess whether:

- use of surveillance devices under a warrant was in accordance with s 18 of the Act
- use of surveillance devices under an emergency authorisation was in accordance with s 32 of the Act
- retrieval of surveillance devices or tracking devices was carried out in accordance with ss 26 and 39(11) of the Act
- use of devices without a warrant were in accordance with ss 37 and 38 of the Act
- use of tracking devices under a tracking device authorisation was in accordance with s 39 of the Act
- any extraterritorial surveillance was in accordance with s 42 of the Act

In making this assessment, we may also test the veracity of the records by, for example, comparing the details of the records to the information maintained in the systems used by the agency to capture information from surveillance devices. We may also rely on what we understand of an agency's processes and procedures in determining the veracity of such records and take into consideration whether the records were made contemporaneously.

2.2. Were computer access (data access) activities conducted in accordance with the authority of warrants or an authorisation under the Act?

Process checks:

- What are the agency's procedures for ensuring computer access activity is conducted lawfully, and are they sufficient?
- Does the agency have an auditable system for managing computer access or data access activities?
- What are the agency's systems and/or record capturing activities under a computer access warrant, and are they sufficient?

- What are the agency's procedures for ensuring computer access warrant conditions are adhered to, and are they sufficient?

Records based checks

We inspect the records and reports relating to the use of computer access (data access) activities against corresponding authorisations and warrants, to assess whether:

- computer/data access activity under a warrant was in accordance with s 27E of the Act
- concealment of access under a computer access warrant was in accordance with ss 27E(7) to (9) of the Act
- computer/data access activity under an emergency authorisation was in accordance with ss 32 and 27E of the Act

3. Is protected information properly managed?

3.1. Was protected information properly stored, used, and disclosed?

Process checks:

- What are the agency's procedures for securely storing protected information, and are they sufficient?
- What are the agency's procedures for ensuring the proper use and disclosure of information, and are they sufficient?
- What are the agency's procedures for protecting privacy?

Records based checks

- We inspect the records and reports regarding the use and disclosure of protected information that are required under the Act to assess whether anything indicates the agency has used and/or communicated protected information for a purpose other than one outlined in s 45(4) of the Act.

3.2 Was protected information retained or destroyed in accordance with the Act?

Process checks:

- What are the agency's procedures for ensuring that protected information is destroyed in accordance with the Act, and are they sufficient?
- What are the agency's procedures for ensuring that protected information is retained in accordance with the Act, and are they sufficient?
- Does the agency regularly review its protected information to ensure compliance with the Act?

Records based checks

- We inspect records relating to the review, retention, and destruction of protected information, including records that indicate whether the chief officer or their delegate was satisfied that protected information can be retained or destroyed (s 46 of the Act).

4. Was the agency transparent and were reports properly made?

4.1. Were all records kept in accordance with the Act?

Process Checks:

- What are the agency's record keeping procedures, and are they sufficient?
- Does the agency maintain a general register and is it accurate?

Records based checks

- We inspect records presented to assess whether the agency has met its record-keeping requirements under ss 51 and 52 of the Act.
- We assess information contained in the original records against what is contained in the general register to check whether the agency has met the requirements under s 53 of the Act.

4.2. Were reports properly made?

Process checks:

- What are the agency's procedures for ensuring that it accurately reports to the Minister and the Commonwealth Ombudsman, and are they sufficient?

Records based checks

- We inspect copies of reports to assess whether the agency has met its reporting requirements under ss 49 and 50 of the Act.
- In conducting this assessment, we cross-check the information contained in the reports against the corresponding original records.

4.3. Did the agency notify the Ombudsman of relevant computer access activities in accordance with the Act?

Process checks:

- What are the agency's policies and procedures to ensure it accurately notifies our Office of relevant computer access activity and are they sufficient?

Records based checks

- Did the chief officer of the relevant law enforcement agency notify the Ombudsman in relation to the concealment of access activities under a computer access warrant, where those activities took place more than 28 days after the warrant ceased to be in force, in accordance with the Act?

4.4. Does the agency have a culture of compliance?

Process checks:

- Does the agency undertake regular training for officers exercising powers?
- Does the agency provide support and appropriate guidance material for these officers?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose compliance issues to the Commonwealth Ombudsman's office?
- Were issues identified at previous inspections addressed?