COMMONWEALTH OMBUDSMAN

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

For the period 1 July to 31 December 2020

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July 2019 to 30 June 2020

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 January to 30 June 2020

SOUTH AUSTRALIA POLICE
Records from 1 July 2019 to 30 June 2020

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2020

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 2021

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

For the period 1 July to 31 December 2020

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY
Records from 1 July 2019 to 30 June 2020

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
Records from 1 January to 30 June 2020

SOUTH AUSTRALIA POLICE
Records from 1 July 2019 to 30 June 2020

AUSTRALIAN FEDERAL POLICE
Records from 1 January to 30 June 2020

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM,
under s 61 of the *Surveillance Devices Act 2004* (Cth)

March 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 under the *Surveillance Devices Act 2004* (the Act) during the period from 1 July to 31 December 2020 (the reporting period).

During the reporting period we inspected the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Criminal Intelligence Commission (ACIC), South Australia Police (SA Police) and the Australian Federal Police (AFP). The Office planned to inspect Victoria Police during the period but delayed this due to the COVID-19 pandemic and it is now scheduled in May 2021.

Table 1—Summary of inspections during the reporting period

Agency	Date of Inspection	Results of inspection
ACLEI	9–10 September 2020	We did not make any significant findings during the reporting period.
ACIC	26–30 October 2020	We found issues with the ACIC's destruction processes for protected information. We also identified instances where the ACIC's action sheets and its use and communication register contained insufficient information.
SA Police	4–6 November 2020	We found SA Police does not have established destruction procedures and was not able to demonstrate it was destroying protected information in line with the relevant legislative provisions.
AFP	16–20 November 2020	We identified several instances where the AFP collected data outside the terms of the warrant and did not revoke warrants in a timely manner or left warrants to expire, despite having already uninstalled or retrieved the device. We also found instances where the AFP did not comply with the destruction provisions of the Act.

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 access to data held in computers.

1.2. The Act imposes requirements on agencies to securely 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 Ombudsman to inspect the records of a law enforcement agency to determine the extent of compliance with the Act by the agency and its law enforcement officers.

1.4. Section 61(1) of the Act requires the Ombudsman to provide reports to the Minister of Home Affairs at six 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. The Office uses standard inspection methodologies across all agencies. These methodologies are based on legislative requirements and best practice standards, and ensure all agencies are held to the same standard.

1.6. Where we are not able to inspect all records for the period (primarily due to the volume of records) we will, using our standard methodology, create a sample of records for inspection. This generally involves generating a random representative sample. However, we may also select specific types of records for inclusion in the sample on the basis that we consider certain activities pose a heightened risk to compliance, either generally or based on our previous observations of a particular agency's activities.

1.7. Further detail about our inspection criteria and methodology is provided in **Appendix A**.

1.8. To ensure procedural fairness, we give agencies the opportunity to respond to our draft inspection findings. Once we have considered and, where appropriate, incorporated the agency's response, we finalise our inspection results. We then desensitise and consolidate the most significant findings into our report to the Minister.

1.9. 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. However, we do not generally include administrative issues or instances of non-compliance where the consequences are negligible.

Part 2: AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

2.1. From 9 to 10 September 2020 we inspected the Australian Commission for Law Enforcement Integrity's (ACLEI) surveillance device records.

Inspection details

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

Type of record	Records made available	Records inspected
TOTAL	**2**	**2 (100%)**

2.3. The available records consisted of two surveillance device warrants.

Inspection findings

2.4. We did not identify any significant issues during this inspection.

Part 3: AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

3.1. From 26 to 30 October 2020 we inspected the Australian Criminal Intelligence Commission's (ACIC) surveillance device records.

Inspection details

3.2. We inspected records of warrants and authorisations that expired between 1 January and 30 June 2020.

	Records made available	Records inspected
TOTAL	**208**	**50 (24%)**

3.3. The available records consisted of 87 surveillance device warrants, two computer access warrants, 11 tracking device warrants, 61 destructions of protected information and 47 retentions of protected information.

Progress since our previous inspection

3.4. We last publicly reported inspection results for the ACIC in our September 2020 report to the Minister, which covered inspections during the period from 1 January to 30 June 2020 of the records of warrants and authorisations that expired between 1 July and 30 December 2019. That report included disclosures the ACIC made about warrants expiring prior to revocation, and instances where retrieval warrants were not revoked when the relevant device was retrieved.

3.5. At this inspection we identified, and the ACIC disclosed, further instances of delays in warrants being revoked. The ACIC advised it would implement a best practice timeframe within which a request for revocation should be made when it is clear a device is no longer needed or has been retrieved.

3.6. In the September 2020 report, we also identified instances where protected information was certified for retention after it was previously authorised for destruction. At this inspection we again identified issues with the ACIC's practices and processes for destroying protected information in accordance with s 46 of the Act.

3.7. The ACIC advised it intends to commence smaller destruction rounds in 2021 and will consider an agency-wide review of its destruction arrangements once it has finalised its organisational restructure.

3.8. We will continue to focus on destructions at future ACIC inspections, noting issues affecting destructions have been a common theme since February 2017.

Inspection findings

Finding/disclosure—Non-compliance with destruction provisions

3.9. We identified three instances where the ACIC did not destroy protected information as soon as practicable as required by s 46(1)(b)(i) of the Act. In each instance there was a significant delay after the destruction authorisation was signed until the ACIC destroyed the protected information.

3.10. We identified one instance where protection information was not destroyed within five years as required by the s 46(1)(b)(ii) of the Act. The ACIC disclosed seven additional instances it did not destroy protected information within five years.

3.11. We also identified several instances where the ACIC certified protected information for retention after it had already been certified for destruction. We first reported this issue in our September 2020 report to the Minister and maintain it poses an ongoing risk to the ACIC's compliance with the Act.

3.12. We suggested the ACIC expedites the review of its destruction process with a particular focus on the difficulty it experiences completing the current process within required timeframes.

Finding—Insufficient information in action sheets

3.13. Agencies maintain records of actions they take under the authority of a warrant or tracking device authorisation to demonstrate that they acted lawfully. Our Office relies on these records, which are usually described as 'action sheets', to assess if the agency's actions were compliant with the warrant or authorisation.

3.14. The computer access warrant action sheets we inspected did not provide sufficient information for us to understand what actions were taken under the warrant, or to confirm that the correct devices were accessed. As a result, we could not verify that the computers

the ACIC targeted were those it was authorised to access under the warrant.

3.15. In another instance, which involved a tracking device authorisation under s 39 of the Act, the action sheet did not refer to the relevant service identifier and we could not confirm the ACIC had targeted the correct service.

3.16. We suggested to the ACIC that, as a matter of better practice, it should remind staff what information is required in action sheets, particularly for computer access warrants. We further suggested the ACIC inform staff who are involved in covert operations about their obligations to record particulars of the device accessed, the install and retrieval times, and device serial numbers.

3.17. The ACIC advised it would update the relevant action sheet reports and could provide further records regarding the computer access warrants. We will review these records at our next inspection.

Finding—Incomplete and unspecified records on each use and communication

3.18. The Act requires agencies to keep records of each use (or access for computer access warrant information) and communication of information obtained under a surveillance device or computer access warrant. The ACIC meets the requirements of ss 52(1)(e), (f) and (g) of the Act by completing an "SD Log and Report" for each warrant or authorisation.

3.19. In one instance, we identified that the use and communication logs within the SD Log and Report did not include information the ACIC had given as evidence under s 52(1)(g) of the Act. In another instance, the log did not include information about internal use under s 52(1)(e) of the Act or external communication under s 52(1)(f) of the Act. In these instances, we consider the ACIC did not meet the requirements under the Act.

3.20. During the inspection we identified a practice whereby staff completed use and communication logs using generic descriptions such as "daily", "weekly" or "monthly". In one instance, the use and communication log described disclosures as occurring "irregularly" for both internal use and external communications. In our view generic time periods do not satisfy the requirement under s 52(1) of

the Act to keep records of “each use” or “each communication” of protected information.

3.21. We suggested to the ACIC that, as a matter of better practice, it should enhance its guidance to staff about managing, using and communicating protected information, to support investigators to satisfy the record-keeping requirements under s 52 of the Act.

3.22. In response, the ACIC advised it was updating its relevant logs and reports. It was also considering updates to its system to centralise use and disclosure details and better meet its record-keeping requirements.

Part 4: SOUTH AUSTRALIA POLICE

4.1. From 4 to 6 November 2020 we inspected South Australia Police's (SA Police) surveillance device records.

Inspection details

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

	Records made available	Records inspected
TOTAL	**4**	**4 (100%)**

4.3. The total available records consisted of four surveillance device warrants.

Progress since our previous inspection

4.4. We last publicly reported inspection results for SA Police in our March 2020 report to the Minister. In that report we did not make any significant compliance findings in relation to SA Police.

Inspection findings

Finding—No process for destroying records

4.5. During this inspection we identified that SA Police does not have destruction procedures to assess whether records are required for a purpose permitted under the Act or should be destroyed in accordance with s 46(1)(b) of the Act.

4.6. SA Police could not confirm the date on which it had most recently assessed whether records it obtained by using a surveillance device were required for a purpose permitted under the Act.

4.7. SA Police informed us it does not have staff delegated to perform the functions of the chief officer under s 46(1)(b) of the Act. SA Police advised it requested internal legal advice about its delegations more than 12 months prior to our inspection and had been told not to proceed with any destructions until that advice was given.

4.8. In our view it is necessary for SA Police to review its files periodically to determine whether destructions are required under the Act. It

should also establish procedures to ensure it conducts destructions in accordance with the relevant legislative provisions. We suggested to SA Police that it act on these tasks as a matter of priority.

4.9. In response, SA Police acknowledged it should prioritise implementing a destruction regime. It advised it was acquiring the relevant delegation under s 46(1)(b) of the Act and would commence destructions as soon as the SA Police Office of General Counsel ratified the instruments.

4.10. We also suggested that SA Police review any protected information it holds that is more than five years old to determine whether it has met its obligations under s 46(1)(b)(ii) of the Act.

4.11. Following an audit of its records, SA Police advised it does not hold any protected information that is more than five years old.

Part 5: AUSTRALIAN FEDERAL POLICE

5.1. From 16 to 20 November 2020 we inspected the Australian Federal Police's (AFP) surveillance device records.

Inspection details

5.2. We inspected records of warrants and authorisations that expired between 1 January and 30 June 2020. We also inspected records relating to the AFP's management of protected information during this period.

	Records made available	Records inspected
TOTAL	**579**	**144 (25%)**

5.3. The total available records included 269 surveillance device warrants, two control order warrants, four computer access warrants, 11 retrieval warrants, 20 tracking device authorisations, 167 "destructions"[1] of protected information and 106 retentions of protected information.

Progress since previous inspection

5.4. We last publicly reported inspection results for the AFP in our September 2020 report to the Minister. In that report we made several compliance findings, some of which we made again following this inspection. We identified further instances of:

- insufficient or inaccurate information recorded in action sheets
- delays in revoking warrants and warrants left to expire
- a surveillance device being operated extra-territorially without consent
- reports that were not made to the Minister in accordance with the Act.

[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.

Inspection findings

Finding—Non-compliance with destruction provisions

5.5. Under s 46(1)(b)(i) of the Act, the chief officer must cause the destruction of any record or report comprising protected information as soon as practicable if satisfied that no civil or criminal proceeding to which the material relates has been, or is likely to be, commenced and that the material is not likely to be required in connection with an activity or purpose prescribed under the Act.

5.6. Contrary to s 46(1)(b)(i) of the Act, the AFP did not destroy protected information "as soon as practicable" after it was authorised for destruction. In four instances the AFP did not destroy the information until more than a month after the certification for destruction was given. This included one instance where the AFP did not destroy the information until more than five months after the certification for destruction was given.

5.7. Further, the AFP did not destroy protected information or certify it for retention within five years. This was not compliant with s 46(1)(b)(ii) of the Act. In three instances the AFP did not destroy the records until more than five years after the warrant was issued and could not provide files to demonstrate the protected information was certified for retention within five years. In the remaining instance, the AFP certified the protected information for destruction within five years but did not complete the destruction until after the five year period.

5.8. The AFP advised it would continue to educate officers on the destruction requirements and timeframes, 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.

5.9. Furthermore, the number of "destructions" the AFP reported to our Office included warrants where the warrant was either not executed or no product was obtained and there was no protected information for it to destroy. This may have affected whether our sample for the inspection was representative of the broader records.

Finding—Insufficient or inaccurate information on action sheets

5.10. 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, in turn, inform its reports to the Minister under s 49 of the Act. We consider action sheets are an important mechanism for the AFP to demonstrate its compliance with the Act when using surveillance devices.

5.11. At this inspection we identified 24 action sheets that did not contain sufficient information for us to assess AFP's compliance with the Act. We also identified two instances where action sheets were inaccurate and a further two instances where no action sheet was on file.

5.12. In our previous public report to the Minister in September 2020 we identified four instances where action sheets did not contain sufficient information about how the AFP executed warrants and authorisations. We suggested the AFP remind its officers of the importance of including appropriate detail in action sheets, particularly for computer access warrants.

5.13. Following our last inspection, the AFP took action to raise staff awareness about the importance of good record-keeping. However, noting the above instances, following this inspection we suggested the AFP establish formal quality assurance processes for action sheets.

Finding—Incomplete and unspecified records on each use and communication

5.14. The Act requires agencies to keep records of each use (or access for computer access warrant information) and communication of information it obtains under a surveillance device or computer access warrant. The AFP meets the requirements of s 52(1) of the Act by completing a *Use made of protected information form*.

5.15. During the inspection we identified a practice where staff recorded use of protected information using generic descriptions such as 'daily' and recorded use across a date range rather than specifying each individual use of the information. In our view generic terms and time periods do not satisfy the requirement to keep records of each

use and communication of protected information under ss 52(1)(e) and (f) of the Act.

5.16. We suggested the AFP remind its investigators about their record keeping obligations and ensures that staff record sufficient information to detail each use of protected information.

5.17. The AFP advised it would take steps to further educate staff about their reporting obligations and amend its form templates. We will check this at our next inspection of the AFP.

Finding—Delayed revocation of warrants and warrants left to expire

5.18. In our previous public report to the Minister in September 2020 we included a disclosure the AFP made that it had not revoked a retrieval warrant in a timely manner under s 27(2) of the Act. In that instance the AFP revoked the retrieval warrant approximately five weeks after it retrieved the relevant device, which we agreed did not meet the requirement under s 27(5) of the Act to act "immediately" once satisfied the grounds for issuing the retrieval warrant no longer existed.

5.19. During this reporting period, there were several instances where we could not ascertain whether the AFP was satisfied that the use of a surveillance device under the warrant was required, or whether the warrant should have been revoked in line with the mandatory revocation requirements under s 20(2) of the Act. In these instances, the period between the last action the AFP took under the warrant and the warrant expiring ranged from three weeks to six months.

5.20. We suggested:

a. the AFP should update its procedures to include a better practice timeframe for a request for revocation to be made after it is clear a device is no longer needed and/or has been retrieved

b. where no action has been taken under a warrant for a period of four weeks or more, or where the device has been retrieved or uninstalled, the AFP should keep records to demonstrate it maintained an intention to use a surveillance device, to demonstrate compliance with s 20(2) of the Act.

5.21. In response, the AFP advised it would continue to educate officers about the revocation requirements of the Act, noting it considers the Act does not oblige it to justify why a warrant was not revoked prior to expiry. The AFP also advised it would add a new field to the relevant form to prompt investigators to explain why a warrant was left to expire in cases where the device has been retrieved or uninstalled or where no action has occurred for four weeks or more.

5.22. The AFP advised its policy is to revoke a warrant as soon as practicable after it identifies the warrant is no longer required. The AFP advised that, while it endeavours to have the revocation instrument endorsed within five days, a range of extenuating circumstances means this timeframe is not always attainable.

Finding—Not immediately notifying the chief officer that the grounds for a retrieval warrant no longer exist

5.23. We identified three instances where the law enforcement officer to whom a retrieval warrant had been issued did not promptly notify the chief officer that the grounds for the retrieval warrant no longer existed. This was inconsistent with s 27(5) of the Act which states that the chief officer must be informed "immediately". In all three instances the AFP retrieved the devices two or more weeks before it made the revocation.

5.24. We suggested the AFP ensure law enforcement officers are aware of their obligation to notify the chief officer immediately upon forming the belief that the grounds for issuing the retrieval warrant no longer exist.

5.25. The AFP explained these instances were an administrative oversight and it would continue to educate officers about the revocation requirements for retrieval warrants.

Finding/disclosure—Extraterritorial operation of surveillance device without consent

5.26. In previous public reports to the Minister in March and September 2020 we included disclosures the AFP made about unauthorised extraterritorial surveillance it conducted contrary to s 42 of the Act.

5.27. During this inspection, the AFP again disclosed two periods during which it conducted surveillance activities in a foreign country prior to

receiving approval from an appropriate consenting official of that country.

5.28. While the AFP disclosed this instance of non-compliance, it did not quarantine the associated data until prompted to do so during our inspection. We suggested the AFP quarantine any unlawfully obtained data as soon as it identifies it.

5.29. We identified that, while the surveillance device was first used extraterritorially on 17 December 2019, the AFP did not send written correspondence to the Attorney-General until 19 May 2020. This was a significant delay and we do not consider this meets the requirement under s 42(6) of the Act to notify the Attorney-General as soon as practicable after commencing surveillance in a foreign country.

5.30. Following the inspection, the AFP advised it had quarantined, and not reviewed the affected files.

Disclosure—Data collected outside the warrant

5.31. The AFP disclosed two instances where it collected data outside the warrant.

5.32. In the first instance, the warrant expired in December 2019, but the device remained installed. In September 2020 the AFP became aware the device had collected 12 files since the warrant expired. Upon receipt of the product the AFP removed the device and quarantined the 12 files.

5.33. The AFP advised it now issues an uninstall command when a warrant expires, regardless of whether the surveillance device appears to be installed or not. We will consider this at future inspections.

5.34. In the second instance, a tracking device authorisation (TDA) was issued in September 2020. In late October 2020 the AFP became aware a surveillance device had been deployed on two occasions, purportedly under the authority of the TDA, where a surveillance device warrant should have been obtained.

5.35. The AFP advised that, before deploying surveillance devices in future, investigators would personally check to confirm the type of authorisation/warrant required to use it. Following the inspection,

the AFP confirmed that, in both instances, it had quarantined unlawful product.

Finding—Application not on file

5.36. In one instance the application for an extension to a surveillance device warrant was not present on the file. In the absence of this application, we could not determine whether the requirements of s 14(5) of the Act were met. In that instance we were also not satisfied the AFP met its record-keeping obligation under s 51(g)(ii) of the Act.

5.37. The AFP advised that, despite extensive checks, it could not locate the application and it seemed likely an application was not included in the document package submitted to the issuing authority.

Finding/disclosure—Reports not made to the Minister in accordance with the Act

5.38. The AFP disclosed two instances, and we identified two additional instances where the AFP did not send a s 49 report to the Minister within three months of the warrant or authorisation ceasing to be in force.

5.39. We also identified three instances where there were inconsistencies in the information recorded on the s 49 report when compared to the Final Effectiveness Report (FER), action sheet and/or the use of protected information form.

5.40. We suggested the AFP review these files and, if necessary, amend the s 49 reports. The AFP confirmed it submitted amended s 49 reports to the Minister.

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
- applications for extensions and/or variations to surveillance device warrants were made in accordance with s 19
- applications for retrieval warrants were made in accordance with s 22
- 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
- written records for emergency authorisations were properly issued in accordance with s 31
- applications for tracking device authorisations and retrieval of tracking devices were made in accordance with s 39
- tracking device authorisations were properly issued in accordance with s 39, and recorded in accordance with s 40

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
- applications for extensions and/or variations to computer access warrants were made in accordance with s 27F
- 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
- 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
- computer access warrants were revoked in accordance with s 27G, and discontinued in accordance with s 27H

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

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

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).

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

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.
- 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.

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.
- 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 officers exercising powers?
- 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?
- Has the agency engaged with the Commonwealth Ombudsman's office as necessary?