COMMONWEALTH OMBUDSMAN

Report to the Attorney-General on agencies' compliance with the *Surveillance Devices Act 2004* (Cth)

Inspections conducted 1 January to 30 June 2023

Australian Commission for Law Enforcement Integrity
Records from 1 January to 30 June 2022

Australian Criminal Intelligence Commission
Records from 1 January to 30 June 2022

Australian Federal Police
Records from 1 January to 30 June 2022

New South Wales Police
Records from 1 July 2021 to 30 June 2022

Victoria Police
Records from 1 July 2021 to 30 June 2022

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

September 2023

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

OUR REPORT – AT A GLANCE

The *Surveillance Devices Act 2004* (Cth) provides law enforcement with the following warrant powers:

A **surveillance device warrant**, which permits law enforcement to use surveillance devices in criminal investigations or to locate and safely recover a child to whom a recovery order relates. 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 of the above devices.

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

A **data disruption warrant** permits the Australian Federal Police or the Australian Criminal Intelligence Commission to frustrate the commission of an offence by modifying, adding, copying, or deleting data.

Key messages from this report

- We made **no recommendations**, **no suggestions** and **3 better practice suggestions** for improvement from our inspections conducted between 1 January and 30 June 2023.
- There was a high level of compliance by the agencies we inspected when using the powers under the *Surveillance Devices Act 2004* (Cth).
- We made fewer findings during this period, compared to the same period last year. Agencies were responsive to our findings and took remedial action to address non-compliance or deficiencies in their compliance framework.
- We conducted our first inspection of the Australian Federal Police's use of data disruption powers. We found that the AFP had robust frameworks and controls in place to exercise powers under the Act. The Australian Criminal Intelligence Commission did not used these same powers.

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 2023 (the reporting period).

During the reporting period we inspected the surveillance device, computer access and data disruption records of the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Criminal Intelligence Commission (ACIC), the Australian Federal Police (AFP), New South Wales Police (NSW Police) and Victoria Police.

Table 1: Summary of the results of each surveillance devices inspection

Agency	Inspection dates	Summary of results of each inspection
ACLEI	14 to 17 March 2023	We made **no** findings during this inspection.
ACIC	17 to 21 April 2023	We made **no** findings during this inspection.
AFP	6 to 10 March 2023	We identified several applications for warrants which did not address privacy considerations in relation to persons likely to be affected by the warrant. We note this was not a systemic issue and the applications we inspected were generally of a high standard.
NSW Police	17 to 20 January 2023	We found that NSW Police had not met the destruction requirements of the Act. This was a repeat finding from our last surveillance devices inspection at NSW Police, which we publicly

Agency	Inspection dates	Summary of results of each inspection
		reported on in our September 2022 report to the Attorney-General.[1]
Victoria Police	2 to 5 May 2023	We found there were delays in providing s 49 reports to the Attorney-General following the revocation of tracking device authorisations. We identified opportunities for Victoria Police to improve their tracking device authorisations templates to improve compliance with the Act.

We also inspected the digital surveillance records (being computer access warrants and data disruption warrants) of the ACIC and AFP.

Table 2: Summary of the results of each digital surveillance inspection (inspections of computer access warrants and data disruption warrants)

Agency	Inspection dates	Summary of results of each inspection
ACIC	17 to 18 April 2023	We identified that the ACIC did not have a declaration instrument in place for certain executive officers to be 'endorsing officers' for data disruption warrants. Although the ACIC is yet to obtain a data disruption warrant, having a declaration in place will prevent the ACIC from being delayed should a need to use the powers arise in the future.
AFP	6 to 10 March 2023	We made no findings during this inspection.[2]

1 Commonwealth Ombudsman, *Report to the Attorney-General on agencies compliance with the Surveillance Devices Act 2004 (Cth)* (September 2022), p 13.

2 We made findings during this inspection in relation to account takeover warrants, which are obtained under Part IAAC of the *Crimes Act 1914* (Cth). These findings will be included in the Commonwealth Ombudsman's

Part 1: SCOPE AND METHODOLOGY

Introduction

1.1. The *Surveillance Devices Act 2004* (the Act) sets out the powers of law enforcement agencies (including specified state and territory agencies) with respect to the use of surveillance devices and access to data held in computers.

1.2. The Act also allows the AFP and ACIC to exercise data disruption powers to frustrate the commission of relevant offences by altering, adding, copying or deleting data.

1.3. The Act imposes requirements on agencies to store and destroy protected information obtained by using surveillance devices, through computer access or data disruption activities. Agencies must also comply with reporting requirements.

Our oversight role

1.4. Section 55(1) of the Act requires the Ombudsman (the Ombudsman) to inspect the surveillance device, computer access and data disruption warrant records of a law enforcement agency to determine the extent of compliance with the Act.

1.5. 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

1.6. Our Office's methodology is based on legislative requirements and best practice standards. Further detail about our inspection criteria and methodology is provided in **Appendix A**.

---

forthcoming *2022-23 Report to the Attorney-General on agencies' compliance with the Crimes Act 1914*.

Part 2: AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY[3]

Inspection details

2.1. From 14 to 17 March 2023, we inspected the ACLEI's surveillance device records. We inspected records of warrants and authorisations that expired between 1 January and 30 June 2022.

2.2. The available records consisted of 8 surveillance device warrants.

Table 3: Summary of records for ACLEI inspection

	Records made available	Records inspected
TOTAL	**8**	**8 (100%)**

Progress since our previous inspection

2.3. Our previous inspection of the ACLEI's surveillance device records was conducted in March 2022, with inspections results published in our September 2022 report to the Minister. That report identified non-compliance by the ACLEI with the destruction and retention requirements of the Act.

2.4. ACLEI was responsive to the suggestions in our previous report and commenced a review of all surveillance device warrant records eligible for destruction or retention. ACLEI also reviewed and updated its standard operating procedures to improve compliance with destructions and retention requirements.

Inspection findings

2.5. At this inspection, we made no findings and were satisfied that ACLEI was compliant when using the surveillance device powers.

[3] Please note the ACLEI was subsumed into the National Anti-Corruption Commission on 1 July 2023.

Part 3: AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Inspection details – Surveillance devices records

3.1. From 17 to 21 April 2023, we inspected the ACIC's surveillance device records. We inspected records of warrants and authorisations that expired between 1 January and 30 June 2022.

3.2. The available records consisted of 39 surveillance device warrants (including 10 extensions), 3 tracking device authorisations, 28 retentions and 131 destructions of protected information.

Table 4: Summary of records for ACIC surveillance devices inspection

	Records made available	Records inspected
TOTAL	**201**	**50 (25%)**

Progress since our previous inspection

3.3. We last publicly reported inspection results for the ACIC in our September 2022 report to the Minister. There were no significant compliance findings in that report.

Inspection findings

3.4. At this inspection, we made no findings and were satisfied that the ACIC was compliant when using the surveillance device powers.

Inspection details – Digital surveillance records

3.5. From 17 to 18 April 2023, we inspected the ACIC's digital surveillance records. As the ACIC had no computer access warrants that expired between 1 January and 30 June 2022, and did not use the data disruption warrant powers between 3 September 2021 and 30 June 2022[4], our inspection focused on whether the ACIC

[4] Data disruption warrants were introduced into the *Surveillance Devices Act 2004* on 3 September 2021 with passage of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act).

had appropriately actioned the findings from our previous 'health check' review[5].

3.6. We found the ACIC had not finalised its position on the meaning of "material loss or damage" in the context of data disruption warrants as suggested in our previous 'health check report'. Subsection 49C(2) requires the chief officer of a law enforcement agency to notify the Ombudsman if action taken under a data disruption warrant has caused material loss or damage to one or more persons lawfully using a computer. The ACIC advised that it had been consulting with the AFP to ensure they shared a consistent view of the definition. By the end of the inspection the ACIC was close to finalising this issue, and we expect it to be resolved by the time of our next inspection.

Inspection findings

Finding - Declaration for endorsing officers for data disruption warrants

3.7. We identified that the ACIC did not have a declaration for certain ACIC executive level officers to be 'endorsing officers' for data disruption warrant applications. We suggested, as a matter of better practice, that the ACIC consider making an appropriate declaration prior to a need arising for the power to be used.

3.8. In its response the ACIC advised that they have considered the making of a declaration under section 27KBB of the Act, but have not sought such a declaration from the CEO. The ACIC advised that once training, procedural documents and guideline processes have been developed and finalised, they will progress this declaration.

---

[5] A 'health check' review assesses an agency's compliance framework and preparedness to use a covert or intrusive power. During our health checks we provide compliance feedback to agencies to reduce risks of non-compliance. We typically perform a 'health check' review when an agency is provided access to a covert or intrusive power they have not used before.

Part 4: AUSTRALIAN FEDERAL POLICE

Inspection details – Surveillance device records

4.1. From 6 to 10 March 2023, we inspected the AFP's surveillance device records. We inspected records of warrants and authorisations that expired between 1 January and 30 June 2022.

4.2. The available records consisted of 7 refused warrants, 346 surveillance device warrants (including 12 control order and supervisory order surveillance device warrants), 11 retrieval warrants, 5 tracking device authorisations, 74 destructions and 44 retentions of protected information.

Table 5: Summary of records for AFP surveillance devices inspection

	Records made available	Records inspected
TOTAL	**487**	**55 (11%)**

Progress since our previous inspection

4.3. We last publicly reported inspection results for the AFP in our September 2022 report to the Minister. That report included findings in relation to non-compliance with destruction requirements of the Act and instances of section 49 reports not being made to the Minister in accordance with the Act.

4.4. At this inspection we confirmed that the AFP took appropriate remedial action in relation to the previous findings.

Inspection findings

Finding – Insufficient information concerning privacy considerations in applications for surveillance device warrants

4.5. We identified that several applications for surveillance device warrants (including supporting affidavits) did not sufficiently outline the extent to which the privacy of any person would likely be affected by the warrant, for consideration by the eligible judge or nominated Administrative Appeals Tribunal (AAT) member under section 16(2)(c) of the Act. We found that standard template

wording was used for applications involving more than one target and did not outline the potential privacy implications based on the individual circumstances of the case.

4.6. While we recognise that the issuing authority must have regard to privacy, we consider it prudent that the affidavit addresses the extent to which the privacy of any person is likely to be affected to demonstrate that sufficient information was provided to the issuing authority.

4.7. We suggested, as a matter of better practice, the AFP ensure there is sufficient information in applications addressing the privacy considerations of any person likely to be affected by the warrant.

4.8. The AFP accepted our suggestion and committed to reviewing relevant warrant application templates to ensure guidance on addressing privacy considerations is comprehensive and consistent. The AFP also stated that it will provide guidance to applicants and those responsible for quality assurance on when to include additional information to demonstrate the privacy impact has been considered reasonably and proportionately.

Inspection details – Digital surveillance records

4.9. From 6 to 10 March 2023, we inspected the AFP's digital surveillance records. We inspected records of computer access warrants that expired between 1 January and 30 June 2022, and data disruption warrants that expired between 3 September 2021 and 30 June 2022.

4.10. The available records consisted of 6 computer access warrants, 1 data disruption warrant, 2 computer access warrant destructions and 1 computer access warrant retention.

Table 6: Summary of records for AFP digital surveillance inspection

	Records made available	Records inspected
TOTAL	**10**	**10 (100%)**

Inspection findings

4.11. We made no findings and were satisfied that the AFP was compliant when using computer access warrants and data disruption warrants.

Part 5: NEW SOUTH WALES POLICE

Inspection details

5.1. From 17 to 20 January 2023, we inspected the New South Wales Police Force's (NSW Police) surveillance device records. We inspected records of warrants and authorisations that expired between 1 July 2021 and 30 June 2022.

5.2. The available record consisted of one destruction of protected information.

Table 7: Summary of records for NSW Police inspection

	Records made available	Records inspected
TOTAL	1	1 (100%)

Progress since our previous inspection

5.3. We last publicly reported inspection results for NSW Police in our September 2022 report to the Minister. That report identified non-compliance with the destruction and retention requirements of the Act.

5.4. We confirmed that the NSW Police had updated its policies and procedures to ensure protected information would be destroyed or retained in accordance with the Act.

5.5. Notwithstanding, the NSW Police disclosed that protected information for one warrant had not been fully destroyed despite initially believing that it had been. Following our inspection, the NSW Police confirmed it had completed a destruction order for the remaining protected information. We will review this case at our next inspection.

Inspection findings

5.6. We made no new findings at this inspection.

Part 6: VICTORIA POLICE

Inspection details

6.1. From 2 to 5 May 2023, we inspected the Victoria Police's surveillance device records. We inspected records of authorisations that expired between 1 July 2021 and 30 June 2022.

6.2. The available records consisted of 4 tracking device authorisations and 1 destruction of protected information.

Table 8: Summary of records for Victoria Police inspection

	Records made available	Records inspected
TOTAL	5	5 (100%)

Progress since our previous inspection

6.3. We last publicly reported inspection results for the Victoria Police in our September 2022 report to the Minister. That report identified non-compliance with the destruction requirements of the Act, which was caused by the absence of policies, guidance, templates and training specific to the Commonwealth surveillance devices legislation (in comparison to Victoria's state-based surveillance devices legislation).

6.4. At this inspection we confirmed that the Victoria Police took appropriate action to address the finding from our previous inspection by creating and updating materials to support compliance with the Act.

Inspection details

Finding – Greater clarity required in tracking device authorisations to satisfy legislative requirements

6.5. We found the terminology used to describe the primary executing officer in the tracking device authorisations was not clear. Authorisations stated that the officer "remains the law enforcement officer whether or not physically present for any step in the

execution of the authorisation", rather than the terminology in section 40(1)(i) of the Act (being "primarily responsible for executing the authorisation").

6.6. Each tracking device authorisation did not include a clear statement that it was not subject to any conditions. Although it did not appear that the tracking devices authorisations were subject to any conditions, this should be reflected in the authorisation to meet the requirements of section 40(1)(j) of the Act. This also created inconsistencies between Victoria Police's internal action reports and reports made to the Minister pursuant to section 49 of the Act about whether the authorisations were subject to any conditions.

6.7. Additionally, each authorisation did not reflect the requirements under section 39(8) of the Act, which recognises that an authorising officer must not give permission for the use, installation or retrieval of a tracking device if the installation of the device, or its retrieval, involves entry onto premises without permission or an interference with the interior of a vehicle without permission.

6.8. We suggested, as a matter of better practice, that the Victoria Police update its tracking device authorisation template to ensure all requirements under sections 39 and 40 of the Act are clearly reflected.

6.9. The Victoria Police advised they had updated their tracking device authorisation templates to provide greater clarity of these legislative requirements. We will review these templates at our next inspection.

Finding – Delay in providing section 49 reports to the Minister

6.10. Section 49 of the Act requires agencies to provide a report to the Minister on each warrant or authorisation as soon as practicable after the warrant or authority ceases to be in force. The Act does not define 'as soon as practicable', however, we consider a period of up to three months satisfies this requirement.

6.11. The section 49 reports for each tracking device authorisation were not provided to the Minister until 5 months after the authorisation was revoked. The Victoria Police advised that it has updated its processes to ensure this timeframe is met in the future.

Leave this page blank

APPENDIX A – INSPECTION METHODOLOGY AND CRITERIA

Using a risk-based approach, we assess an agency's compliance by reviewing a selection of the agency's records, having discussions with relevant agency staff, observing agency policies and processes, and assessing remedial action taken in response to issues we have previously identified.

Our inspections may identify a range of issues, from minor administrative errors through to serious or systemic non-compliance. To ensure procedural fairness, we give agencies the opportunity to respond to our inspection findings. We then consolidate our significant findings and agency responses into this 6 monthly report to the Attorney General. We follow up on any remedial action agencies have taken to address our findings at our next inspection.

The criteria for our surveillance device and digital surveillance inspections are below.

Surveillance Devices

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 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. 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 for ensuring that use of surveillance devices is discontinued, and are they sufficient?

Records based checks

We inspect agency records, to assess whether:

- warrants were revoked in accordance with s 20, and discontinued in accordance with s 21.

2. Was surveillance 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.

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. 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?

Digital Surveillance (Computer Access Warrants and Data Disruption Warrants)

Objective: To determine the extent of an agency's compliance with the *Surveillance Devices* Act *2004* (the Act) as it relates to the use of computer access and data disruption powers.

1. Was appropriate authority in place for computer access and data disruption activities?

1.1. Did the agency have proper authority for computer access and data disruption activities?

Process checks:

- What are the agency's procedures to ensure that warrants, extensions, and variations are properly applied for, and are they sufficient?
- What are the agency's procedures to ensure that emergency authorisations are properly issued, 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 and data disruption warrants include accurate and sufficient information for the issuing authority to determine whether to issue the warrant under s 27C or s 27KC of the Act.
- applications for computer access warrants were made in accordance with s 27A or s 27B of the Act if a remote application
- applications for extensions and/or variations to computer access warrants were made in accordance with s 27F of the Act
- the making of an application for a data disruption warrant has been endorsed by an endorsing officer in accordance with s 27KBA or s 27KBB of the Act
- applications for data disruption warrants were made in accordance with s 27KA or s27KB of the Act if a remote application
- applications for extensions and/or variations to data disruption warrants were made in accordance with s 27KF of the Act
- emergency authorisations issued by an eligible Judge or a nominated Administrative Appeals Tribunal member comply with the requirements in ss 28, 29, 30, 32, 33, 34, 35A and 35B of the Act
- computer access warrants and data disruption warrants contained the information required by s27D or 27KD of the Act
- written records for emergency authorisations were properly issued in accordance with s 31 of the Act.

1.2. Were computer access and data disruption warrants properly revoked and discontinued?

Process checks:

- What are the agency's procedures to ensure that warrants are properly revoked, and are they sufficient?
- What are the agency's procedures for ensuring that activity under a warrant is discontinued, and are they sufficient?

Records based checks

We inspect agency records, to assess whether:

- computer access warrants were revoked in accordance with s 27G, and discontinued in accordance with s 27H of the Act
- data disruption warrants were revoked in accordance with s 27KG, and discontinued in accordance with s 27KH of the Act.

2. Were computer access and data disruption activities in accordance with the Act?

2.1. Were computer access and data disruption 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 and data disruption activity is conducted lawfully, and are they sufficient?
- Does the agency have an auditable and centralised system for managing computer access or data disruption activities?
- How does the agency demonstrate and provide assurance that the agency's systems and/or mechanisms for accessing and disrupting data are in accordance with the Act and the terms of the warrant?
- 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 computer access and data disruption activities against corresponding authorisations and warrants, to assess whether:

- computer access activity under a warrant was in accordance with s 27E of the Act, including:
    - concealment of access under a computer access warrant was in accordance with ss 27E(7) to (9) of the Act

- data disruption activity under a warrant was in accordance with s 27KE of the Act, including:
    - concealment of access under a data disruption warrant was in accordance with ss 27KE(9) to (11) of the Act
- computer access activity under an emergency authorisation was in accordance with ss 32 and 27E of the Act
- data disruption activity under an emergency authorisation was in accordance with ss 32 and 27KE of the Act
- the warrant execution was likely to or actually materially interfered with, interrupted, or obstructed a communication in transit or caused material loss or damage to persons lawfully using a computer (ss 27E(5), 27E(8), 27KE(7) and 27KE(10) of the Act – noting the relevant exceptions provided for in under the Act)
- any extraterritorial surveillance was in accordance with s 43A or 43C of the Act.
- assistance orders complied with s 64A or 64B of the Act.

3. Is protected information (including general computer access intercept information and data disruption intercept information) collected under a warrant 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 collected under a warrant, and are they sufficient?
- What are the agency's procedures for ensuring the proper use and communication 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 communication of protected information that are required under the Act to assess whether the agency has used or communicated protected information for a purpose other than one outlined in s 45 or s 45A of the Act (for computer access warrants sought for an integrity operation).

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 and/or 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 should be retained or destroyed (s 46 of the Act).
- We inspect records to ensure all protected information is destroyed within 5 years of its creation, and within each period of 5 years thereafter unless the chief officer makes the decision to retain the data (s 46(1)(b) of the Act).

4. Did the agency comply with its record-keeping, reporting and notification obligations?

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 to assess whether the agency met 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 reported against corresponding original records.

4.3. Did the agency notify the Ombudsman of relevant 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 and data disruption activity and are they sufficient?

Records based checks

- Did the chief officer of the relevant law enforcement agency notify the Ombudsman within 6 months of the issuing of a Part 5.3 warrant, and give the

Ombudsman a copy of the warrant, in accordance with s49A(1) of the Act?

- Did the chief officer of the relevant law enforcement agency notify the Ombudsman as soon as practicable, of a contravention of relevant conditions or provisions of a Part 5.3 warrant, in accordance with s 49A(2) of the Act?
- Did the chief officer of the relevant law enforcement agency notify the Ombudsman within 7 days, about 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 s 49B the Act?
- Did the chief officer of the relevant law enforcement agency notify the Ombudsman within 7 days of data disruption activity conducted under a warrant in accordance with s 49C(1) of the Act?
- Did the chief officer of the relevant law enforcement agency notify the Ombudsman of material loss or damage to a person lawfully using a computer, which occurred in the execution of a data disruption warrant, within 7 days in accordance with s 49C(2) of the Act?

5. Does the agency have a culture of compliance

Process checks:

- Does the agency undertake regular training for officers exercising the powers (including endorsing officers under ss 27KBA and 27KBB of the Act)?
- 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?
- Does the agency have processes to ensure compliance, including:
    - quality control processes are supported by policy and practical guidance documents
    - effective procedures to measure compliance and identify and action issues as they arise
    - processes and training to identify and track issues that occur
    - protocols for advising relevant officers of issues that arise?