COMMONWEALTH OMBUDSMAN

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

Inspections conducted 1 January to 30 June 2022

Australian Commission for Law Enforcement Integrity
Records from 1 July to 31 December 2021

Australian Criminal Intelligence Commission
Records from 1 July to 31 December 2021

Australian Federal Police
Records from 1 January to 31 December 2021

New South Wales Police
Records from 1 July 2019 to 30 June 2021

Victoria Police
Records from 1 July 2020 to 30 June 2021

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

September 2022

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

Inspections conducted 1 January to 30 June 2022

Australian Commission for Law Enforcement Integrity
Records from 1 July to 31 December 2021

Australian Criminal Intelligence Commission
Records from 1 July to 31 December 2021

Australian Federal Police
Records from 1 January to 31 December 2021

New South Wales Police
Records from 1 July 2019 to 30 June 2021

Victoria Police
Records from 1 July 2020 to 30 June 2021

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

September 2022

ISSN 2204-4027 - Print
ISSN 2204-4035 - Online

Contact us
Inquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman
Level 5, 14 Childers Street
Canberra ACT 2600
Tel: 1300 362 072

Email: media@ombudsman.gov.au

CONTENTS

EXECUTIVE SUMMARY

This report presents the results of the Office of the Commonwealth Ombudsman's inspections conducted under the *Surveillance Devices Act 2004* (the Act) between 1 January and 30 June 2022 (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), the Australian Federal Police (AFP), New South Wales Police (NSW Police) and Victoria Police.

In September 2021, the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act) introduced 3 new powers: data disruption warrants and network activity warrants into the Act, and account takeover warrants in Part IAAC of the *Crimes Act 1914* (the Crimes Act). Our Office oversees data disruption and account takeover warrants, while the Office of the Inspector-General of Intelligence and Security oversees network activity warrants.

This report provides a summary of inspections under the Act, including regarding the new data disruption warrant powers. A separate report about our inspections of account takeover warrant records, and other powers under the Crimes Act, will be provided to the Attorney-General.

Table 1 – Summary of the results of each inspection

Agency	Inspection dates	Summary of results of each inspection
ACLEI	15 to 17 March 2022	ACLEI had instances of non-compliance with the destruction and retention requirements of the Act.
ACIC	16 to 20 May 2022 (Surveillance devices records inspection)	We confirmed the ACIC took appropriate remedial action in relation to the findings from our previous inspection. We made no significant new compliance findings during our inspection.
	31 May to 2 June 2022 (Computer access warrant records and data disruption	We made no compliance findings in relation to the ACIC's computer access records. We identified some improvements that could be made to the ACIC's data disruption warrant

Agency	Inspection dates	Summary of results of each inspection
	warrant 'health check' inspection)	policy, procedures and guidance during our health check review.
AFP	26 to 29 April 2022 (Surveillance devices records inspection)	The AFP disclosed instances of non-compliance with the destruction requirements of the Act. We found, as we have in previous inspections, that some reports to the Minister were not made in accordance with the requirements of s 49 of the Act.
	2 to 6 May 2022 (Computer access warrant records and data disruption warrant 'health check' inspection)	We identified some improvements that could be made to the AFP's data disruption warrant policy, procedures and guidance during our health check review.
NSW Police	8 to 9 June 2022	We found NSW Police was not compliant with the destruction requirements of the Act.
Victoria Police	23 to 27 May 2022	We found administrative non-compliance with a record because of an absence of targeted policies, guidance and templates aligning to 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 through access to data held in computers.

1.2. The Act also allows the AFP and the ACIC to exercise data disruption powers to frustrate the commission of a relevant offence 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. The Act restricts the way agencies use, communicate, or publish such information and requires them to provide reports about these covert activities.

Our oversight role

1.4. 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.

1.5. 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. 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 inspection methodology is based on legislative requirements and best practice standards. Further detail about our inspection criteria and methodology is at **Appendix A**.

1.7. During the reporting period we conducted 'health check' reviews of agencies (the AFP and ACIC) able to use data disruption warrants, as introduced by the SLAID Act in 2021. The purpose of these reviews is to assess each agency's compliance framework and preparedness to use the data disruption warrant powers. During our health checks we provide compliance feedback to agencies to reduce risks of non-compliance. Our Health Check criteria is at **Appendix B**.

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

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. We do not generally report on administrative issues or instances of non-compliance where the consequences are negligible.

1.10. We follow up on any remedial action agencies have taken to address our findings at our next inspection.

Part 2: AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

Inspection details

2.1. From 15 to 17 March 2022, we inspected ACLEI's surveillance device records. We inspected records of warrants and authorisations that expired between 1 July and 31 December 2021.

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

2.2. The available records consisted of 4 surveillance device warrants.

Progress since our previous inspection

2.3. We last publicly reported inspection results for ACLEI in our September 2021 report to the Minister. That report included findings in relation to not keeping records for each use and communication of protected information and inadequate record keeping of actions taken under a warrant.

Inspection findings

Finding – Non-compliance with destruction and retention requirements

2.4. We found 18 instances where protected information obtained from surveillance device warrants was not destroyed by ACLEI, or retained following consideration of whether the information should be destroyed, within 5 years of being made. This is contrary to s 46(1)(b) of the Act. ACLEI advised that it did not identify these warrants for destruction and retention purposes due to an administrative error and staffing changes.

2.5. We suggested ACLEI take steps to review impacted records to determine whether protected information should be retained or destroyed.

2.6. We also suggested, as a matter of better practice, that ACLEI engage with the other agencies (including assisting agencies) with whom any

impacted data had been shared and explore practical avenues for ensuring s 46(1)(b) of the Act has been complied with.

2.7. We made a further better practice suggestion that ACLEI consider amending its processes to ensure considerations of whether protected information be destroyed or retained begins well in advance of the 5-year time limit contained in s 46(1)(b)(ii) of the Act. Doing so would mitigate the risk of future non-compliance, given the administrative steps required before destruction or retention is completed.

2.8. ACLEI accepted our findings and commenced a review of all surveillance device warrant records eligible for destruction or retention. ACLEI also advised it is reviewing and updating its standard operating procedures, streamlining its processes and improving record keeping practices to improve compliance with destructions and retention requirements.

Part 3: AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Inspection details – Surveillance devices records

3.1. From 16 to 20 May 2022, we inspected the ACIC's surveillance device records. We inspected records of warrants and authorisations that expired between 1 January and 31 December 2021.

	Records made available	Records inspected
TOTAL	**396**	**35 (9%)**

3.2. The available records consisted of 89 surveillance device warrants, 2 retrieval warrants, 6 tracking device authorisations, 17 retentions and 282 destructions of protected information.

Progress since our previous inspection

3.3. We last publicly reported inspection results for the ACIC in our September 2021 report to the Minister. That report included findings in relation to warrants issued by an ineligible authority, protected information not destroyed as soon as practicable or within 5 years of a record or report being made, and inadequate recording of actions taken under a warrant.

Inspection findings

3.4. At this inspection we confirmed that the ACIC took appropriate remedial action in relation to each of the findings.

3.5. We made no significant new compliance findings as a result of our inspection.

Inspection details – Computer access warrant records and data disruption warrant 'health check'

3.6. From 31 May to 2 June 2022, we inspected the ACIC's computer access warrant records and conducted a health check review of data disruption warrant policy, procedures and guidance. We inspected records of computer access warrants that expired between 1 January and 31 December 2021.

	Records made available	Records inspected
TOTAL	**16**	**16 (100%)**

3.7. The available records consisted of 11 computer access warrants and 5 computer access warrant extensions or variations.

3.8. For the health check the ACIC shared relevant templates, policies and procedures, and training materials. We reviewed these documents, and where relevant, provided compliance feedback to reduce risks of non-compliance.

Inspection findings

3.9. We made no compliance findings in relation to the ACIC's computer access warrant records.

Finding – Better practice finding regarding guidance on material loss or damage

3.10. We did not identify non-compliance as a result of our health check review of data disruption warrant policy, procedures and guidance.

3.11. However, the ACIC's guidance material did not define the term 'material loss or damage to one or more persons lawfully using a computer', which must be notified to the Ombudsman under s 49C(2) of the Act. This term is not defined in the Act. Without defining this term in the context of its role and operational activities, or providing other guidance to its officers, it is not clear how the ACIC will consistently assess whether the notification provisions are invoked.

3.12. We suggested, as a matter of better practice, that the ACIC seek legal advice and develop a definition of the term 'material loss or damage' for ACIC purposes so that data disruption warrant notification requirements are complied with consistently. The ACIC sought legal advice and has formed a preliminary view as to what the term means. The ACIC is also developing a template for notifying the Ombudsman that material loss or damage has occurred under a data disruption warrant.

Part 4: AUSTRALIAN FEDERAL POLICE

Inspection details – Surveillance devices records

4.1. From 2 to 6 May 2022, we inspected the AFP's surveillance device records. We inspected records of warrants and authorisations that expired between 1 January and 31 December 2021.

	Records made available	Records inspected
TOTAL	**111**	**59 (53%)**

4.2. The available records consisted of 33 surveillance device warrants (including 9 control order surveillance device warrants), 7 retrieval warrants, 14 tracking device authorisations, 27 retentions and 30 destructions of protected information.

Progress since our previous inspection

4.3. We last publicly reported inspection results for the AFP in our September 2021 report to the Minister. That report included findings in relation to information collected outside the authority of a warrant, inadequate recording of actions taken under a warrant, non-compliance with destruction requirements, and instances of s 49 reports not being made to the Minister in accordance with the Act.

4.4. That report also included disclosures by the AFP in relation to information collected in the absence of a warrant and warrants issued by an ineligible authority.

4.5. At our May 2022 inspection we identified further instances of the AFP not complying with the destruction requirements of the Act and s 49 reports not being made to the Minister in accordance with the Act.

Inspection findings

Disclosure – Non-compliance with destruction requirements

4.6. On 24 February 2021 the AFP disclosed a significant volume of protected information that had been retained despite orders to destroy the information, contrary to s 46 of the Act. This information related to 131 AFP operations between 2012 and 2020. The AFP

attributed this non-compliance to standard operating procedures not identifying all systems where protected information was stored, as well as ineffective communication between various teams about destruction requirements.

4.7. In response to this disclosure, we conducted additional compliance activities across our May 2021 and May 2022 inspections to gain assurance that the protected information was destroyed. This involved cataloguing a sample of information that should have been destroyed and then confirming that destruction occurred. It also involved reviewing the AFP's updated systems, processes and guidance, with the aim of reducing the risk of this non-compliance occurring again. Notwithstanding, it remains the AFP's responsibility to ensure that protected information is destroyed in accordance with the Act.

4.8. While we anticipated the new destructions processes would help address the inadvertent retention of protected information across disparate systems and teams in the future, at our May 2022 inspection we found the AFP had not destroyed all the information required.

4.9. As a result, we suggested the AFP conduct further review and assessment to provide assurance that no protected information exists that should have been destroyed as part of this disclosure.

4.10. In response the AFP advised that it had commenced a further review of all product included in the disclosure made on 24 February 2021 to ensure it has been destroyed.

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

4.11. In our September 2021 report to the Minister, we reported on several reports to the Minister that were not fully compliant with s 49 of the Act. We suggested the AFP complete s 49 reporting so the report fully details the activities that occurred under a warrant and addresses all matters required under s 49(2)(b) of the Act.

4.12. At our May 2022 inspection we saw improvement in the quality and detail included in the AFP's s 49 reports to the Minister. However, we identified 10 additional instances where s 49 reports to the Minister were non-compliant with the Act, due to deficiencies or inconsistencies in the records.

4.13. As a result, we reiterated the suggestion in our previous report (see paragraph 4.11) and suggested that, where s 49 reports were inaccurate, the AFP provide the Minister with an updated report. The AFP advised that it provided amended reports to the Minister and noted that s 49 reports are required to address all items in s 49(2)(b) of the Act.

Inspection details – Computer access warrant records and data disruption warrant 'health check'

4.14. From 26 to 29 April 2022, we inspected the AFP's computer access warrant records and conducted a health check review of data disruption warrant policy, procedures and guidance. We inspected records of computer access warrants that expired between 1 January and 31 December 2021.

	Records made available	Records inspected
TOTAL	**60**	**35 (58%)**

4.15. The available records consisted of 22 computer access warrants, 35 extensions and variations, and 3 computer access warrant destructions.

4.16. For the health check the AFP shared relevant templates, policies and procedures, and training materials. We reviewed these documents, and where relevant, provided compliance feedback to reduce risks of non-compliance.

Inspection findings

Finding – Better practice finding regarding guidance on material loss or damage

4.17. We did not identify non-compliance as a result of our health check review of data disruption warrant policy, procedures and guidance.

4.18. However, the AFP's guidance material did not define the term 'material loss or damage to one or more persons lawfully using a computer', which must be notified to the Ombudsman under s 49C(2) of the Act. This term is not defined in the Act. Without defining this term in the context of its role and operational activities, or providing other guidance to its officers, it is not clear how the AFP

will consistently assess whether the notification provisions are invoked.

4.19. We suggested, as a matter of better practice, that the AFP seek legal advice and develop a definition of the term 'material loss or damage' so that data disruption warrant notification requirements are complied with consistently.

4.20. In response to our report the AFP confirmed it had sought legal advice and updated its guidance material accordingly.

Part 5: NEW SOUTH WALES POLICE

Inspection details

5.1. From 8 to 9 June 2022, we inspected NSW Police's surveillance device records. We inspected records of warrants and authorisations that expired between 1 July 2019 and 30 June 2021.

	Records made available	Records inspected
TOTAL	7	7 (100%)

5.2. The available records consisted of one surveillance device warrant, 2 retentions and 4 destructions of protected information.

Progress since our previous inspection

5.3. We last publicly reported inspection results for NSW Police in our March 2020 report to the Minister. The report identified a compliance risk in relation to miscalculating the period of effect of a warrant.

5.4. At this inspection we confirmed that NSW Police took appropriate action to remediate this and other compliance issues from our previous inspection.

Inspection findings

Finding – Non-compliance with destruction and retention requirements of the Act

5.5. We found four instances where records did not indicate the chief officer of NSW Police, or their delegate, caused protected information to be destroyed in accordance with the chief officer's obligations under s 46(1)(b) of the Act. In these instances the protected information was destroyed by staff of NSW Police who did not have delegation by the chief officer.

5.6. We also found two instances where protected information was certified for retention, under the ostensible authority of s 46(1)(b)(ii) of the Act, by NSW Police staff who did not have delegation by the chief officer.

5.7. We suggested that NSW Police should:

- establish appropriate delegations for the destruction and retention of surveillance data;
- keep records about what was destroyed (e.g. the warrant number and type of surveillance data) and when destruction was finalised.

5.8. In its response to our report NSW Police committed to implementing our suggestions.

Part 6: VICTORIA POLICE

Inspection details

6.1. From 23 to 27 May 2022, we inspected Victoria Police's surveillance device records. We inspected records of warrants and authorisations that expired between 1 July 2020 and 30 June 2021.

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

6.2. The available record consisted of one destruction of protected information during the eligible period.

Progress since our previous inspection

6.3. We last publicly reported inspection results for Victoria Police in our September 2021 report to the Minister. In that report we identified that Victoria Police had 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.

6.4. At this inspection we confirmed that Victoria Police took action to address the findings from our previous inspection. This included updating templates, developing guidance, and providing addendums to address inaccuracies in previous reports to the Minister under s 49 of the Act.

Inspection findings

Finding – Administrative non-compliance with destruction requirements due to absence of templates specific to the Commonwealth legislation

6.5. We found one instance where a destruction record authorised the destruction of protected information under the wrong legislation. In this instance the destruction was purportedly authorised under s 30H of the *Surveillance Devices Act 1999* (Victoria) rather than the Commonwealth Act.

6.6. We suggested, as a matter of better practice, that Victoria Police update its policies, guidance, templates and training to support compliance with the Commonwealth Act – prioritising updates and additions to guidance, templates and training where the Act departs from the Victorian legislation.

6.7. In response, Victoria Police advised that it updated its destruction template to refer to the destruction of protected information under the correct reference, being s 46 of the Commonwealth legislation.

APPENDIX A – SURVEILLANCE DEVICES INSPECTION CRITERIA

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 made 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 of the Act.

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 was 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 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?

APPENDIX B – HEALTH CHECK CRITERIA[1]

Objective: To assess the 'health' of the agency in establishing its compliance framework and to determine any compliance risks with the *Surveillance Devices Act 2004* (SD Act) and Part IAAC of the *Crimes Act 1914* (Crimes Act) only as they relate to data disruption warrants and account takeover warrants.

1. Compliance preparedness

1.1 Organisational context

a) Has the agency identified any issues, especially those related to compliance risks, that affect its ability to establish processes for, and use the dark web powers in a manner that complies with each Act?

b) Does the agency have measures in place to manage and identify relevant considerations in applying for data disruption warrants and account takeover warrants?

c) Has the chief officer delegated any functions under each Act?

d) If a delegation instrument is position-based, do procedures include mitigations for the compliance risks associated with organisational change?

e) Has the agency declared relevant officers to be endorsing officers for data disruption warrants in accordance with s 27KBA or s 27KBB of the SD Act?

1.2 Planning for and addressing compliance risks

a) Does the agency have processes and procedures to ensure compliance with each Act, and a register for recording instances of non-compliance?

b) Has the agency sought legal or other advice in establishing processes and systems for using the dark web powers?

c) Has the agency sought assistance from relevant agencies or entities, in establishing processes and systems for using dark web powers?

d) Has the agency established plans to ensure compliance with legal requirements before using dark web powers?

e) What are the outstanding actions, if any, and anticipated timeframes for implementation?

[1] Our SLAID Act 'health checks' were of the 2 powers we oversee, being data disruption and account takeover warrants. This report includes the results of our health check for data disruption warrants that are in the Act, while the results of our health check for account takeover warrants will be included in our forthcoming Crimes Act report.

2. Communication, resources, and training

2.1 Resources

a) Has the agency developed support resources and guidance documents for its use of dark web powers?

b) Have these resources been appropriately communicated to staff who exercise the powers?

c) If resources are currently in development, what are the outstanding actions and anticipated timeframes for completion?

2.2 Competence and training

a) Does the agency (or does the agency have an established plan to):

- hold mandatory and periodic compliance training for officers using and administering dark web powers?
- engage with officers involved in using dark web powers to advise on relevant issues/compliance concerns?

b) If not established, what are the outstanding actions and anticipated timeframes for implementation?

2.3 Awareness and communication

a) How will the agency ensure that officers involved in using dark web powers maintain awareness of their compliance responsibilities?

b) Has the agency established policies and procedures for complying with the reporting and record-keeping requirements under each Act?

c) For data disruption warrants, does the agency have processes in place and guidance for staff to notify the Ombudsman under s 49C of the SD Act?

d) How will the agency adequately communicate with relevant external stakeholders about these powers?

3. Operational preparedness

3.1 Operational planning

a) Has the agency established appropriate templates, processes and guidance for staff applying for data disruption warrants and account takeover warrants (including remote, emergency and/or urgent applications)?

b) Does the agency have processes and policies about assistance orders under s 64B of the SD Act and s 3ZZVG of the Crimes Act?

c) Does the agency have established guidelines and policies for concealment of access activities under a data disruption warrant (s 27KE of the SD Act) and account takeover warrant (s 3ZZUR of the Crimes Act)?

d) Has the agency established appropriate guidance for staff applying for variations to or extensions of data disruption warrants and account takeover warrants?

e) Has the agency established processes and guidance for staff for revoking and discontinuing use of data disruption warrants under ss 27KG and 27KH of the SD Act, and account takeover warrants under ss 3ZZUT and 3ZZUU of the Crimes Act?

f) Has the agency established processes and procedures for storing, accessing, retaining, and destroying protected information (including data disruption intercept information) in accordance with s 46 of the SD Act and s 3ZZVJ of the Crimes Act?

g) Does the agency have policies and guidance regarding recording use and communication of protected information?

h) Has the agency established appropriate policies and procedures for facilitating Ombudsman inspections under s 55 of the SD Act and s 3ZZVR of the Crimes Act?

i) Where the above policies and procedures are not yet established, what are the outstanding actions and anticipated timeframes for implementation?

3.2 Establishing controls and procedures

a) Does the agency have appropriate quality assurance and control measures in relation to use of dark web powers?

b) Does the agency have appropriate procedures to demonstrate that the actions it took under data disruption or account takeover warrants were in accordance with each Act?

c) Has the agency established appropriate data management, storage, vetting and quarantining procedures?

d) Where quality assurance and control measures are not yet established, what are the outstanding actions and anticipated timeframes for implementation?

4. Performance evaluation and improvement

4.1 Monitoring, measurements, analysis and evaluation

a) Does the agency have systems in place for capturing and responding to internal and external feedback on agency compliance performance?

b) How will the agency identify and manage emerging compliance issues?

c) Does the agency have processes in place to facilitate continual improvement with legislative requirements?

4.2 Audit and management review

a) Does the agency conduct, or intend to conduct, any form of internal audit or routine management review of legislative compliance and/or compliance with internal policies and guidance?

4.3 Non-compliance identification and corrective action

a) Has the agency established systems and processes to identify and respond to compliance issues?