COMMONWEALTH OMBUDSMAN

2021-22 Report to the Attorney-General on agencies' compliance with the *Crimes Act 1914*:

Controlled Operations
Delayed Notification Search Warrants
Account Takeover Warrants

Report by the Commonwealth Ombudsman, Iain Anderson, under sections 15HO of Part IAB, 3ZZGH of Part IAAA and 3ZZVX of Part IAAC of the *Crimes Act 1914* (Cth)

November 2022

COMMONWEALTH OMBUDSMAN

2021-22 Report to the Attorney-General on agencies' compliance with the *Crimes Act 1914*:

Controlled Operations
Delayed Notification Search Warrants
Account Takeover Warrants

Report by the Commonwealth Ombudsman, Iain Anderson, under sections 15HO of Part IAB, 3ZZGH of Part IAAA and 3ZZVX of Part IAAC of the *Crimes Act 1914* (Cth)

November 2022

ISSN 2653-6498 - Print
ISSN 2653-6501 - 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

Key concepts

A **controlled operation** permits participants to engage in certain conduct that would otherwise be unlawful for the purpose of investigating a serious offence.

A **delayed notification search warrant** (DNSW) allows a covert search of premises to investigate certain terrorism offences, with the occupier of the premises being notified later.

An **account takeover warrant** (ATW) allows law enforcement to take control of an online account when investigating a serious offence.

Findings

We made **no formal recommendations** for remedial action.

We made **13 suggestions** and **13 better practice suggestions**:

- **7 suggestions** and **2 better practice suggestions** in relation to use of controlled operations
- **6 suggestions** and **6 better practice suggestions** in relation to use of DNSW powers
- **5 better practice suggestions** in relation to agency preparedness to use ATW powers.

Key messages from this report

- We made fewer suggestions for improvement regarding use of controlled operations in 2021-22 compared with the previous year, demonstrating ongoing improvement in compliance.
- We conducted our first inspection of the Australian Federal Police's (AFP) use of DNSW powers. The AFP undertook substantial work to prepare to use this power. We did not identify any serious or systemic non-compliance but found insufficient record keeping impacted the AFP's ability to demonstrate compliance.

- We conducted ATW health check reviews of the AFP and Australian Criminal Intelligence Commission (ACIC) to determine readiness to use the new powers. Both agencies undertook substantial work to prepare to use these new powers and we did not identify any significant compliance issues.

EXECUTIVE SUMMARY

This report presents the results of the Office of the Commonwealth Ombudsman's (the Office) inspections conducted under Part IAAC of the *Crimes Act 1914*[1] (the Act) between 3 September 2021 and 30 June 2022,[2] Part IAB of the Act between 1 July 2021 and 30 June 2022, and Part IAAA of the Act between 1 January 2022 and 30 June 2022 (the reporting period).

During the reporting period we conducted one inspection each of the Australian Criminal Intelligence Commission's (ACIC) and the Australian Federal Police's (AFP) use of controlled operations under Part IAB of the Act. Overall, we consider both the ACIC and AFP generally compliant with the requirements of Part IAB of the Act. The number of serious or systemic compliance findings has decreased compared to previous reporting periods.

We did not conduct an inspection under Part IAB of the Act of the Australian Commission for Law Enforcement Integrity (ACLEI) during the reporting period as no relevant authorities ceased to be in force in the period 1 January 2021 to 31 December 2021. We typically inspect records after the relevant authorities have expired to manage operational sensitivities. Instead of conducting an inspection, we liaised with ACLEI to review its progress since our previous inspection.

We conducted one delayed notification search warrant (DNSW) inspection of the AFP under Part IAAA of the Act in this period. This was our Office's first inspection of the AFP's use of delayed notification search warrants, after the AFP started using these warrants in 2021. We did not identify any significant instances of non-compliance; however, we found a lack of contemporaneous records hindered the AFP's ability to demonstrate compliance. Notwithstanding this, we acknowledge the substantial compliance work undertaken by the AFP preceding our inspection. Our suggestions and better practice suggestions to the AFP were aimed at strengthening record-keeping processes to demonstrate compliance with the Act.

---

[1] https://www.legislation.gov.au/Series/C1914A00012.

[2] Noting that the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act) commenced on 3 September 2021.

We also conducted 'health check' reviews of the ACIC and AFP to assess each agency's preparedness to use account takeover warrant powers under Part IAAC of the Act. Account takeover warrants were introduced by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*. We did not identify any significant compliance issues and acknowledge the substantial work undertaken by both agencies to prepare for using these powers in compliance with the Act.

Table 1 – Summary of key issues identified during Controlled Operations inspections

Agency	Summary of key issues of each inspection
ACIC	• The ACIC disclosed an issue concerning potential unauthorised conduct. We were satisfied with the ACIC's proactive remedial action in relation to this issue and made no further suggestion.
AFP	• We found non-compliance with requirement to notify Immigration and Border Protection under s 15J of the Act. We suggested the AFP take steps to improve and maintain officers' awareness of the notification requirements under s 15J of the Act.

Table 2 – Summary of key issues identified during the Delayed Notification Search Warrants inspection

Agency	Summary of results of inspection
AFP	• We found a lack of records on file to assess compliance. We suggested the AFP develop and implement processes to ensure consistent and sufficient records are kept regarding the exercise of powers under Part IAAA of the Act. • We found insufficient record-keeping for seizures, copies and photographs. We suggested the AFP provide further guidance to staff on keeping sufficient contemporaneous records. • We found inconsistency in, and absence of, written records authorising 'persons assisting'. We suggested the AFP obtain legal advice on whether written authorisation is required, particularly for actions taken by 'persons assisting'.

Agency	Summary of results of inspection
	• We found destruction of data without chief officer (or delegate) involvement. We suggested the AFP seek legal advice regarding the ability to destroy automatically copied data without consideration by the chief officer or a delegate. • We found a lack of guidance material in identified areas (detailed below). We made a better practice suggestion that the AFP ensure its guidance on identified processes includes practical instructions. • We found an inaccurate occupier's notice. We were satisfied with the AFP's proposed remedial action and made no further suggestion.

Table 3 – Summary of key issues identified during Account Takeover Warrants review

Agency	Summary of results of each inspection
ACIC and AFP	• We found a non-compliance risk due to absence of guidance or policy regarding thresholds for material loss and damage. We suggested the agencies seek legal advice and develop a definition of the term 'material loss or damage' so that activity under an account takeover warrant is not in contravention of the Act.

Part 1: OUR OVERSIGHT ROLE

1.1. Parts IAB, IAAA and IAAC of the Act grant law enforcement agencies access to covert and intrusive powers. Our Office's oversight role is important for ensuring that agencies exercise these powers in accordance with legislative requirements and are accountable for instances of non-compliance. Our Office's reporting obligations provide transparency and a level of assurance to the Attorney-General and the public on the use of these powers.

Part IAB of the Act – Controlled Operations

1.2. A controlled operation under Part IAB permits authorised law enforcement and civilian participants to engage in certain conduct that would otherwise be unlawful for the purpose of investigating a serious offence.

1.3. Under s 15HS of the Act, at least once every 12 months, our Office must inspect the records of authorising agencies (ACLEI, the ACIC and the AFP) to determine the extent to which these agencies and their officers complied with Part IAB of the Act.

1.4. Additionally, our Office must inspect records of the ACIC to determine the extent of the ACIC's compliance with State controlled operations laws, unless the corresponding State controlled operations law provides for such an inspection, and only if the ACIC exercised those powers in the relevant period. ACIC did not exercise these state powers in the period covered by this report.

1.5. Under s 15HO of the Act, our Office must report to the Attorney-General as soon as practicable after 30 June each year on inspections conducted during the preceding 12 months. In this report, the Ombudsman must include comments on the comprehensiveness and adequacy of the reports provided by agencies to the Attorney-General and our Office under ss 15HM and 15HN of the Act.

Part IAAA of the Act – Delayed Notification Search Warrants

1.6. A delayed notification search warrant under Part IAAA allows the AFP to conduct a covert search of premises (meaning a search the occupier is not aware of at the time) to investigate certain terrorism offences. The occupier of the premises is notified of the search later.

1.7. Under s 3ZZGB of the Act, at least once in each 6-month period, our Office must inspect the records of the AFP to determine the extent of the AFP's compliance with Part IAAA of the Act.

1.8. Under s 3ZZGH of the Act, as soon as practicable after each 6-month period, our Office must present a report to the Attorney-General on the results of each inspection.

Part IAAC of the Act – Account Takeover Warrants

1.9. An account takeover warrant under Part IAAC allows law enforcement to take control of an online account when investigating a serious offence. Online accounts include, for example, social media accounts, online banking accounts and accounts associated with online forums.

1.10. Section 3ZZVR of the Act requires our Office to annually inspect the records of the AFP and ACIC to determine the extent of their compliance with Part IAAC of the Act.

1.11. Under 3ZZVX of the Act the Ombudsman is required to provide a report to the Attorney-General at 12 monthly intervals with the results of each inspection.

How we oversee agencies

1.12. Our Office uses a set of inspection methodologies and criteria that we apply consistently across each inspection. These are based on legislative requirements and administrative best practice standards. Further details on our inspection criteria are provided in **Appendix A and B**.

1.13. During the reporting period we conducted 'health check' reviews of agencies' ability to use account takeover warrants (the AFP and ACIC). These reviews assess each agency's compliance framework and preparedness to use the account takeover warrant powers. Our Health Check criteria is at **Appendix C**. We will conduct the first records inspections of the use of account takeover warrants during the 2022-23 financial year.

1.14. We assess an agency's compliance based on a risk-based selection of the agency's records, discussions with relevant agency staff, observations of agency policies and processes, and remedial action taken in response to issues identified.

1.15. Our Office takes a retrospective approach to inspecting an agency's use of powers. We generally inspect authorities or warrants that ceased to be in effect before the inspection. This retrospective approach seeks to minimise the risk associated with the sensitivity of ongoing operations. As a result, our 'inspection periods' (the period within which the inspection occurred) and our eligible 'records periods' (the period of time during which the records we are inspecting were made) differ.

1.16. Our inspections may identify a range of issues from minor administrative errors through to serious non-compliance that affects rights (notably privacy) or whether evidence was validly collected, and systemic issues. If an issue is sufficiently serious or systemic, or was previously identified and not resolved, we may make formal 'recommendations' for remedial action. Where an issue of non-compliance is less serious or systemic, or was not identified before, we generally make 'suggestions' to address the non-compliance and to encourage agencies to take responsibility for identifying and implementing practical solutions. We may also make 'better practice suggestions' where we consider an agency's existing practice may expose it to compliance risks in the future.

1.17. To ensure procedural fairness, and compliance with s 15HO(2) of the Act for our Part IAB inspections, we give agencies opportunity to comment on our findings during and following an inspection. The findings from our inspection reports and agency responses are desensitised and summarised to form the basis of our Office's annual report to the Attorney-General.

1.18. This annual report provides a summary of the most significant findings regarding agencies' compliance with Part IAB, IAAA and IAAC of the Act from inspections conducted in the relevant period. 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 comment in this annual report on administrative issues or instances of non-compliance where the consequences are negligible.

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

Part 2: CONTROLLED OPERATIONS UNDER PART IAB OF THE ACT

Introduction

2.1. Part IAB of the Act enables law enforcement agencies to conduct controlled operations. Controlled operations are covert operations carried out, under internal authorisation, for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious Commonwealth offence.

2.2. An appropriately authorised controlled operation provides legal protection for authorised law enforcement and civilian participants who engage in certain conduct during the operation that would otherwise be unlawful or lead to civil liability. Participants may engage in different types of conduct, so long as that conduct is directly authorised or appropriately related to authorised conduct. Examples of conduct could include possessing illicit goods, interfering with a consignment, or entering false data into a system.

2.3. Under Part IAB a controlled operation must not involve conduct that will seriously endanger the health or safety of any person; cause the death of, or serious injury to, any person; involve the commission of a sexual offence against any person; or result in significant loss of, or serious damage to, property (other than illicit goods).

2.4. To ensure an appropriate level of transparency about how and when controlled operations are used, Part IAB of the Act imposes several reporting obligations on agencies.

Australian Commission for Law Enforcement Integrity

2.5. We did not inspect ACLEI as there were no authorities or records requiring inspection for the relevant period.

2.6. Our Office liaised with ACLEI during the reporting period to discuss ACLEI's progress in relation to our previous inspection findings. We were satisfied that ACLEI has taken appropriate action to resolve most of our previous suggestions and better practice suggestions.

Australian Criminal Intelligence Commission

2.7. We conducted one inspection of the ACIC during the reporting period, from 2 to 6 May 2022. We inspected a selection of controlled operations authorities that expired or were cancelled between 1 January to 31 December 2021.

2.8. We made 1 suggestion and 2 better practice suggestions to the ACIC (discussed further below). This was a decrease from the 11 suggestions and 5 better practice suggestions we made following our previous inspection in June 2021. Following receipt of our report, the ACIC advised it had taken action in response to our suggestions and better practice suggestions.

2.9. The ACIC advised it did not use corresponding State or Territory controlled operations powers during the records period.

Record type	Records made available	Records inspected
Urgent controlled operations authorities[3]	2	2 (100%)
Formal controlled operations authorities[4]	61	9 (15%)
Internal variation to controlled operations authorities[5]	52	11 (21%)
AAT variation to controlled operations authorities[6]	73	18 (25%)

[3] An authority granted, if the authorising officer is satisfied the delay caused by granting a formal authority may affect the success of the controlled operation.

[4] A formal controlled operation authority is granted by means of a written document, signed by the authorising officer.

[5] Internally authorised variations to the authority. Internal variations may extend a formal authority up to a period of 3 months, add or remove participants, or add or alter the conduct participants may engage in.

[6] Extending the duration of a controlled operation beyond 3 months requires external authorisation by a nominated AAT Member. Each external variation can extend an operation by a maximum of 3 additional months, up to a limit of 24 months in total.

Progress since our previous inspection

2.10. We considered that the ACIC fully implemented 10 of the 16 suggestions and better practice suggestions arising from our previous inspection in June 2021, with action taken on the remaining 6 resulting in partial implementation. The ACIC established new roles within the agency relating to oversight and assurance, which we considered will assist the ACIC to address the remaining outstanding findings from our previous inspection. We will monitor the ACIC's progress in finalising actions to resolve previous findings at our next inspection.

2.11. In the period between our June 2021 inspection and our May 2022 inspection, the ACIC proactively engaged our office to review and provide feedback on updated resources supporting its internal compliance management and quality assurance processes.

Inspection findings

2.12. As a result of our May 2022 inspection, we made one suggestion and 2 better practice suggestions on low-risk compliance and administrative matters relating to: the delivery of variations of authority to the principal law enforcement officer; verifying the authorisation of authorising officers; and demonstrating consideration of whether alternative powers were available to engage in proposed conduct.

Disclosure – Potential unauthorised conduct

2.13. During our inspection, the ACIC disclosed one instance of potential unauthorised conduct.

2.14. The ACIC authorised a controlled operation authority for 90 days. On the incorrect assumption the original authority was in force for 3 calendar months (generally a period longer than 90 days), subsequent extensions were granted. As a result, the subsequent extensions were purported to be granted after the controlled operation had expired. This raised questions about the lawfulness of conduct engaged in, whether participants were protected from criminal and civil liability, and the admissibility of evidence gathered during the affected periods.

2.15. The ACIC took immediate remedial action to restrict access to records of the controlled operation and reported the issue in its

6-monthly report under 15HM of the Act. The ACIC implemented additional quality assurance controls to ensure accurate calculation and tracking of expiry dates in the future.

2.16. We were satisfied with the ACIC's proactive remedial action in relation to this issue and made no further suggestion.

Comprehensiveness and adequacy of reports

2.17. The ACIC submitted its 6-monthly reports under s 15HM of the Act for the periods 1 January to 30 June 2021 and 1 July to 31 December 2021, and its 2020-21 annual report to our Office in accordance with the Act.

2.18. We inspected each of these reports and did not find any discrepancies. We consider the ACIC has adequate processes in place to achieve compliance with the reporting requirements of Part IAB of the Act.

Australian Federal Police

2.19. We conducted one inspection of the AFP during the reporting period, from 4 to 8 April 2022. We inspected a selection of controlled operations authorities that expired or were cancelled between 1 January to 31 December 2021.

2.20. We made 6 suggestions to the AFP (discussed further below). This was a decrease in suggestions from the 9 suggestions and 7 better practice suggestions we made to the AFP following our previous inspection in June 2021. Following receipt of our report, the AFP advised it had taken action in response to each of our suggestions.

	Records made available	Records inspected
Urgent controlled operations authorities	0	0
Formal controlled operations authorities	119	20 (17%)
Internal variation to controlled operations authorities	41	23 (56%)
AAT variation to controlled operations authorities	38	21 (55%)

Progress since our previous inspection

2.21. We considered that the AFP fully implemented all 16 suggestions and better practice suggestions arising from our previous inspection conducted in June 2021. We acknowledged the significant work undertaken by the AFP to improve compliance with Part IAB of the Act and noted a decrease in the number of significant or systemic findings made in this reporting period.

Inspection findings

2.22. As a result of our April 2022 inspection, we made 5 suggestions concerning low-risk or administrative matters, such as minor inconsistencies or insufficient detail in records and reports, and changing a controlled operation's principal law enforcement officer.

Key finding – Non-compliance with notification requirements of s 15J of the Act

2.23. We identified 2 instances where there was no evidence to show that notifications that illicit goods were expected to be dealt with by an officer of Customs were sent to the Secretary of the Department of Home Affairs as soon as practicable after the controlled operation authority was granted, as required by s 15J of the Act. Where records are not available to demonstrate compliance, assurance regarding an agency's practices is limited.

2.24. We acknowledged the records demonstrated that the AFP maintained an open line of communication with Customs regarding relevant planned operations and had sufficient policy documents and templates to communicate the requirements of s 15J of the Act.

2.25. We suggested the AFP take steps to improve and maintain officers' awareness of the notification requirements under s 15J of the Act. The AFP advised it has taken steps to address this issue including disseminating advice to investigators and adding guidance text to controlled operation application and authority templates.

Comprehensiveness and adequacy of reports

2.26. The AFP submitted its 6-monthly reports under s 15HM of the Act for the periods 1 January to 30 June 2021 and 1 July to 31 December 2021, and its 2020-21 annual report to our Office in accordance with Part IAB of the Act.

2.27. We inspected each of these reports and identified one inaccuracy in a s 15HM report regarding the date of cessation of an authority. We consider this an isolated instance and that the AFP has adequate processes in place to comply with the reporting requirements of Part IAB of the Act.

Part 3: DELAYED NOTIFICATION SEARCH WARRANTS UNDER PART IAAA OF THE ACT

Introduction

3.1. Part IAAA of the Act enables the AFP to apply for and execute delayed notification search warrants (DNSWs) to investigate terrorism offences punishable by imprisonment for 7 years or more. A DNSW allows a covert search of a premises, with the occupier of that premises being notified at a later time.

Australian Federal Police

3.2. We conducted one inspection of the AFP during 2021-22, from 21 to 24 March 2022. We inspected all executed and non-executed DNSWs issued between 1 January to 31 December 2021.

3.3. We made 6 suggestions and 6 better practice suggestions to the AFP (discussed further below). The AFP was responsive to our findings and advised our Office that it has fully or partially implemented all suggestions, with the AFP expecting to have all suggestions fully implemented by early 2023.

	Records made available	Records inspected
DNSW applications made in person[7]	7	7 (100%)
Non-executed DNSWs[8]	4	4 (100%)
Executed DNSWs[9]	3	3 (100%)

[7] Applications for Delayed Notification Search Warrants (DNSWs) made by the normal process, where the eligible officer applies in person to the issuing officer (eligible judge or tribunal member).

[8] DNSWs which were issued, but not executed (i.e. covert searches were not undertaken).

[9] DNSWs which were issues and executed (i.e. covert searches were undertaken).

Progress since our previous inspection

3.4. This was our Office's first inspection of the AFP's use of powers under Part IAAA of the Act.

Inspection findings

3.5. As a result of our March 2022 inspection, in addition to the key findings detailed below, we made 1 suggestion and 3 better practice suggestions concerning low-risk or administrative matters, such as the format of internal reports, timeliness of reports to the Ombudsman, and ambiguities in record-keeping practices.

Key finding – Lack of records on file to assess compliance

3.6. A key focus of our inspections under Part IAAA of the Act is determining whether law enforcement and persons assisting and the activities undertaken were authorised. In assessing compliance, we rely on agency record-keeping practices. Due to a lack of contemporaneous records on file, for all executed DNSWs, we were unable to determine whether certain actions occurred and if any actions that did occur were compliant. Examples of relevant actions could include whether:

- a person involved in executing the warrant impersonated another person, and if so, whether this was only done to the extent reasonably necessary as required under s 3ZZCA(1)(c) of the Act
- any actions were taken to conceal the fact that anything had been done under the warrant, and if so, whether the actions were reasonably necessary as required under s 3ZZCA(1)(k) of the Act
- any force was used against things or persons, and if so, only as was necessary and reasonable as required under ss 3ZZCD(1)(b) and (c) of the Act
- damage was caused to equipment, data or programs and whether this was due to insufficient care being taken; and if damage occurred, whether compensation was paid as required under s 3ZZCI of the Act

- the chief officer arranged for the destruction of data upon being satisfied the data was not, no longer, or not likely to be required for a permitted purpose as required under ss 3ZZCF(3) and 3ZZCG(3) of the Act.

3.7. The AFP advised that, based on accounts from AFP members involved in execution of the DNSW, several of these activities did not occur. However, without contemporaneous records we could not be satisfied as to what actions did or did not occur and whether these actions were compliant.

3.8. To demonstrate compliance in future, we suggested the AFP develop and implement processes to ensure consistent and sufficient records are kept regarding the exercise of powers under Part IAAA of the Act. The AFP advised it is undertaking several initiatives, including drafting new DNSW-specific guidance material and developing a DNSW execution booklet to support contemporaneous recording of things permitted or required under Part IAAA of the Act.

Key finding – Insufficient record-keeping for seizures, copies and photographs

3.9. Section 3ZZBE(1)(j) of the Act requires a DNSW to detail the kinds of things that may be searched for, seized, copied, photographed, recorded, marked, tagged, operated, printed, tested, or sampled under the warrant. We identified 3 instances where there were insufficient records to demonstrate that the relevant 'things' complied with the parameters of the warrant.

3.10. We suggested the AFP provide further guidance to staff to contemporaneously record things seized, copied, photographed, recorded, marked, tagged, operated, printed, tested, or sampled under a DNSW, and how the executing officer or persons assisting determined that any such actions complied with the parameters of the relevant DNSW. In response, the AFP advised it has updated guidance material and is developing mandatory training to increase awareness of compliance obligations and record keeping expectations associated with using DNSW powers.

3.11. We also identified a lack of clarity in records regarding whether an action undertaken under a DNSW was classed as copying, photographing, or seizing. Given the rules under Division 5 of Part IAAA of the Act governing using, sharing and returning things seized,

we suggested the AFP seek legal advice to determine what action constitutes a 'seizure' under a DNSW, and whether things 'copied' or 'photographed' are considered a 'seizure' under Part IAAA of the Act. In response the AFP advised it had sought legal advice on the appropriate categorisation of activities conducted while executing a DNSW, and this advice will inform updates to guidance material.

Key Finding – Records authorising persons assisting

3.12. We identified 3 warrants where records inconsistently indicated which 'persons assisting' were involved in the execution of the warrant. We also could not identify any written records from executing officers authorising persons to assist in the execution of those warrants.

3.13. The AFP advised of its view that:

- the authorisation of 'constables assisting' in relation to search warrants under s 3E of Part IAA of the Act does not have to be in writing, and does not have to be expressed but can be implied by conduct, and

- this position equally applies to warrants under Part IAAA of the Act.

3.14. We suggested the AFP obtain advice on whether written authorisation is required, particularly for actions taken by 'persons assisting'. Following our suggestion, the AFP informed us it is seeking advice on this matter.

3.15. While there is no legislative requirement to document and keep record of authorising 'persons assisting' as defined under s 3ZZAC of the Act, as a matter of improved administrative record keeping, we suggested the AFP incorporate guidance into its Better Practice Guide that any person other than an AFP member assisting with the execution of a DNSW be recorded as being authorised by the executing officer as a 'person assisting' for the specific warrant. The AFP has since advised it has implemented several processes to address this, including the development of a new 'Persons Assisting' form.

Key Finding – Destruction without Chief Officer or delegate involvement

3.16. We identified one instance where data was destroyed, as required in specified circumstances under s 3ZZCF(3) of the Act, without consideration and instruction from the chief officer or their delegate.

3.17. The AFP advised it did not consider automatic copies created to be a 'copy' for the purposes of Part IAAA of the Act. We suggested the AFP seek legal advice regarding the ability to destroy automatically copied data without consideration by the chief officer or a delegate. Following our suggestion, the AFP informed us it is seeking advice on this matter.

Key finding – Lack of guidance material

3.18. We identified that the AFP lacked specific guidelines to assist members on some processes related to the use of powers under Part IAAA of the Act, including:

- seeking oral internal authorisations
- applying for and being issued an urgent DNSW and, supporting record-keeping processes
- returning a thing seized
- obtaining an order to retain, forfeit, sell or destroy a thing seized
- using electronic equipment at a warrant premises
- using moved electronic equipment at other places, and
- providing compensation for damage to equipment, data or programs (including how to determine and record what caused any damage or corruption).

3.19. We made a better practice suggestion that the AFP ensure its guidance on these processes includes practical instructions for identifying when each process is relevant, record keeping around those circumstances, and, in the case of compensation for damage to equipment, how to agree and pay compensation. In response, the

AFP noted guidance on these matters would be incorporated into relevant guidelines, templates and other resources.

Key Finding – Inaccurate occupier's notice

3.20. As soon as practicable after executing a DNSW, the AFP must notify the occupier of the premises, and any adjoining premises entered to execute the warrant. The delivery of the occupier's notice is the point at which the use of DNSW powers becomes overt and known to the occupier of the premises that was searched.

3.21. Section 3ZZDA(2)(e) of the Act requires the number of persons who entered the warrant premises for the purpose of executing, or assisting in the execution of a DNSW, to be listed in an occupier's notice. We identified one instance of inconsistency between the occupier's notice and other records on file regarding the number of persons who entered the warrant premises.

3.22. The AFP advised the occupier's notice likely required amending and undertook to issue a revised occupier's notice with the amended figure. The AFP also advised it will include instructions in its Better Practice Guide for members to accurately record these figures. We advised the AFP that we were satisfied with its proposed remedial action and will review action taken at our next inspection.

Part 4: ACCOUNT TAKEOVER WARRANTS UNDER PART IAAC OF THE ACT

Introduction

4.1. In September 2021, the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* added Part IAAC to the Act. Part IAAC of the Act allows the AFP and ACIC to use an account takeover warrant to take control of a person's online account to gather evidence about a serious Commonwealth offence or a serious State offence that has a federal aspect.

4.2. The Act imposes requirements on the AFP and ACIC when applying for and executing account takeover warrants. It also imposes requirements for how the AFP and ACIC store and destroy protected information obtained through an account takeover warrant. The Act restricts the way these agencies use, communicate, or publish such information and requires them to keep records and provide reports about these covert activities.

Australian Criminal Intelligence Commission

4.3. From 31 May to 2 June 2022, we performed a health check review of the ACIC's account takeover warrant policy, procedures and guidance. We reviewed these documents, and where relevant, provided compliance feedback to reduce risks of future non-compliance by the ACIC in using account takeover warrants.

4.4. We found that the ACIC's draft policies, procedures and guidance contained appropriate detail that, when combined with existing compliance frameworks, will support use of the new account takeover warrant powers. We made 3 better practice suggestions to the ACIC to address areas for improvement. The ACIC was responsive to our findings and advised our Office of actions taken in response.

Australian Federal Police

4.5. From 26 to 29 April 2022, we performed a health check review of the AFP's account takeover warrant policy, procedures and guidance. We reviewed these documents, and where relevant, provided compliance feedback to reduce risks of future non-compliance by the AFP in using account takeover warrants.

4.6. We noted the proactive engagement by the AFP with our Office in developing its templates, policies, procedures and training since the introduction of these powers. We made 2 better practice suggestions to the AFP to address areas for improvement. The AFP was responsive to our findings and advised our Office of actions taken in response.

Health check review findings

Finding – Non-compliance risk due to absence of guidance or policy regarding thresholds for material loss and damage

4.7. Sections 3ZZUR(5) and 3ZZUR(7) of the Act provide that an account takeover warrant does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to cause material loss or damage to other persons lawfully using a computer.

4.8. The ACIC's and AFP's respective guidance documents do not define the term 'material loss or damage'. There may be ambiguity as to how this requirement will be applied in practice, resulting in potential unlawful execution of a warrant (affecting evidence admissibility).

4.9. We suggested, as a matter of better practice, that the ACIC and AFP seek legal advice and develop a definition of the term 'material loss or damage' so that activity under an account takeover warrant is not in contravention of the Act.

4.10. The ACIC informed us that it will seek legal advice about what may be considered material loss or damage when actioning an account takeover warrant. The ACIC also advised it would develop a policy to provide guidance to staff.

4.11. The AFP informed us it had sought advice and updated its guidance material accordingly.

APPENDIX A – INSPECTION CRITERIA
CONTROLLED OPERATIONS

Audit Objective: To determine the extent of compliance with Part IAB of the *Crimes Act 1914* (Part IAB) by the agency and its law enforcement officers (s 15HS(1)).

1. Were controlled operations conducted in accordance with Part IAB of the Act?

1.1. Did the agency obtain the proper authority to conduct the controlled operation?

1.1.1. What are the agency's procedures to ensure that authorities, extensions and variations are properly applied for and granted, and are they sufficient?	**1.1.2.** What are the agency's procedures for seeking variations from a nominated Tribunal member and are they sufficient?	**1.1.3.** What are the agency's procedures to ensure that ongoing controlled operations are subject to a nominated Tribunal member's oversight and are they sufficient?	**1.1.4.** What are the agency's procedures for cancelling authorities and are they sufficient?

1.2. Were activities relating to a controlled operation covered by an authority?

1.2.1. What are the agency's procedures to ensure that activities engaged in during a controlled operation are covered by an authority and are they sufficient?	**1.2.2.** What are the agency's procedures to ensure the safety of participants of controlled operations?	**1.2.3.** What are the agency's procedures for ensuring that conditions of authorities are adhered to?

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

2.1. Were all records kept in accordance with Part IAB?

2.1.1. What are the agency's record keeping procedures and are they sufficient?	**2.1.2.** Does the agency keep an accurate general register?

2.2. Were reports properly made?

2.2.1. What are the agency's procedures for ensuring that it accurately reports to the Minister and Commonwealth Ombudsman and are they sufficient?	**2.2.2.** What are the agency's procedures for meeting its notification requirements and are they sufficient?

2.3. Was the agency cooperative and frank?

2.3.1. Does the agency have a culture of compliance?
Was the agency proactive in identifying compliance issues?
Did the agency self-disclose issues?
Were issues identified at previous inspections addressed?
Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

APPENDIX B – INSPECTION CRITERIA
DELAYED NOTIFICATION SEARCH WARRANTS

Objective: To determine the extent of compliance with Part IAAA of the *Crimes Act 1914* by the Australian Federal Police and its eligible officers (s 3ZZGB)
1. Was an appropriate authority in place to exercise the delayed notification search powers?
1.1 Were applications for delayed notification search warrants properly made?
Process checks – What are the agency's procedures, controls, guidance and training to ensure that delayed notification search warrants are properly applied for, and are they sufficient? – Does the agency have procedures in place to ensure that warrants meet the requirements set out in ss 3ZZBE and 3ZZBF(5)–(9)? **Records checks** We inspect applications, warrants and other agency records to assess whether: – internal authorisation to apply for warrants was sought and given in accordance with ss 3ZZBA and 3ZZBB – applications for warrants were made in accordance with Subdivisions A (normal process) and B (by electronic means) of Division 2 of Part IAAA – the agency gave the eligible issuing officer sufficient information in the form of an affidavit for the officer to determine whether to issue a delayed notification search warrant under s 3ZZBD – the agency complied with the requirements for applications by electronic means and associated record keeping obligations in s 3ZZBF
1.2 Were applications for extensions of time to re-enter premises properly made?
Process check – What are the agency's procedures, controls, guidance and training to ensure that extensions of time to re-enter premises are properly applied for, and are they sufficient? **Records checks** – We inspect applications, extensions and other agency records to assess whether applications were made in accordance with s 3ZZCC and contained sufficient information for the eligible issuing officer to determine whether to grant the extension

1.3 Were applications for extensions of time to examine or process things properly made?

Process check

- What are the agency's procedures, controls, guidance and training to ensure that extensions of time to examine or process things moved from a warrant premises are properly applied for, and are they sufficient?

Records checks

- We inspect applications, extensions and other agency records to assess whether applications were made in accordance with s 3ZZCE and contained sufficient information for the eligible issuing officer to determine whether to grant the extension

2. Were delayed notification search warrants properly executed?

Process checks

- What are the agency's procedures to lawfully exercise entry, search and related powers, and are they sufficient?
- What are the agency's systems and/or records for capturing the exercise of powers, and are they sufficient?

Records checks

We inspect records and reports relating to the exercise of warrant powers to assess whether:

- entry to premises was in accordance with section 3ZZCA and the warrant, including any conditions to which the warrant was subject
- the exercise of powers was in accordance with the warrant and ss 3ZZCA and 3ZZCB, and where applicable, extensions granted under s 3ZZCC (time to re-enter premises) and 3ZZCE (time to examine or process things moved from a warrant premises)
- assistance was provided and force was used in accordance with s 3ZZCD
- use and operation of equipment was in accordance with ss 3ZZCE, 3ZZCF, 3ZZCG and 3ZZCH
- compensation was paid for any damage to electronic equipment, data or programs in accordance with s 3ZZCI.

3. Were notices to occupiers properly given?

Process checks

- What are the agency's procedures, controls, guidance and training to ensure that warrant premises occupier's notices are properly given, and are they sufficient?
- What are the agency's procedures, controls, guidance and training to ensure that adjoining premises occupier's notices are properly given, and are they sufficient?

- What are the agency's procedures, controls, guidance and training to ensure that extensions of time to give a notice are properly applied for, and are they sufficient?

Records checks

We inspect notices, applications, extensions and other records to assess whether:

- warrant premises occupier's notices were given in accordance with s 3ZZDA
- adjoining premises occupier's notices were given in accordance with s 3ZZDB
- warrant premises and adjoining premises occupier's notices were given within the timeframes required under the warrant and section 3ZZDC
- applications for an extension of time to give notice were made in accordance with s 3ZZDC and contained sufficient information for the eligible issuing officer to determine whether to grant the extension

4. Did the agency properly manage things and data seized?

Process checks

- What are the agency's procedures for managing things seized under a delayed notification search warrant, and are they sufficient?
- What are the agency's procedures for recording use, sharing, return and retention of things seized, and are they sufficient?
- What are the agency's procedures, controls, guidance and training to ensure it meets its obligation to destroy copies and reproductions of data copied under a warrant, and are they sufficient?

Records checks

We inspect records relating to the seizure, use, sharing, return and retention of things and data seized under delayed notification search warrants to assess whether:

- things were used and shared in accordance with s 3ZZEA
- things were returned in accordance with s 3ZZEB
- data was removed and copies of data were destroyed in accordance with ss 3ZZCF and 3ZZCG
- applications for orders about retention, forfeiture, sale or disposal of things were made in accordance with s 3ZZEC and contained sufficient information for the eligible issuing officer to determine what order to make

5. Has the agency satisfied its reporting and record-keeping obligations?

5.1 Were reports to the Minister and the Ombudsman properly made?

Process check

- What are the agency's reporting procedures, and are they sufficient?

Records checks

- Have reports on each warrant been provided to the chief officer in accordance with s 3ZZFA?
- Did the chief officer report annually to the Minister in accordance with s 3ZZFB?
- Did the chief officer report six-monthly to the Ombudsman in accordance with s 3ZZFC?

5.2 Were records properly kept?

Process check

- What are the agency's record keeping procedures, and are they sufficient?

Records checks

- Did the agency keep documents connected with delayed notification search warrants in accordance with s 3ZZFD?
- Did the agency keep a register of delayed notification search warrants in accordance with s 3ZZFE?

6**.** 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 C – HEALTH CHECK CRITERIA[10] ACCOUNT TAKEOVER WARRANTS

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

d) 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?

[10] 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 account takeover warrants that are in the Act, while the results of our health check for data disruption warrants are included in our compliance with the *Surveillance Devices Act 2004* report.

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

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 s64B 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*[11]) 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?

[11] Under section 5(1) of Part 2-6 of the *Telecommunications (Interception and Access) Act 1979* data disruption intercept information means information obtained under a data disruption warrant by intercepting a communication passing over a telecommunications system.

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?