

Australian Federal Police's Use of Statutory Powers

Australian Federal Police

© Commonwealth of Australia 2021

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-656-1 (Print)

ISBN 978-1-76033-657-8 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Senior Executive Director
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:

communication@anao.gov.au.



Canberra ACT

8 June 2021

Dear Mr President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Australian Federal Police. The report is titled *Australian Federal Police's Use of Statutory Powers*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — <http://www.anao.gov.au>.

Yours sincerely



Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
<http://www.anao.gov.au>

Audit team

Julian Mallett
Amanda Ronald
Zoe Pilipczyk
Anne Kent
Sam Jones
Lesla Craswell
Alex Wilkinson

Contents

Summary and recommendations.....	7
Background	7
Conclusion	7
Supporting findings	8
Recommendations	9
Australian Federal Police response.....	9
Key messages from this audit for all Australian Government entities	10
Audit findings.....	11
1. Background	12
Introduction	12
Structure and organisation	12
Rationale for undertaking the audit	14
Audit approach	15
2. Accountability and reporting	18
Does the AFP have an appropriate risk management framework in place in relation to the use of statutory powers?	18
Are instruments of delegation and authorisation accessible, complete and current?	20
Does the AFP maintain adequate records when powers have been exercised?	21
Does the AFP appropriately exercise statutory powers under warrant?	24
The AFP's record keeping practices and processes	46
3. Training and guidance	48
Does the AFP provide adequate training to all officers who will be exercising powers under applicable legislation?	48
Does the AFP undertake analysis of training needs and/or requirements to ensure the lawful exercise of powers by its officers?	54
Does the AFP obtain assurance that officers adequately understand their powers?	55
Are adequate records maintained in relation to the training of AFP officers?	56
Do officers have access to accurate and up-to-date guidance materials to assist with their exercise of powers?	58
Appendices	63
Appendix 1 Australian Federal Police's response	64
Appendix 2 Provisions of Acts that confer intrusive powers on Australian Federal Police Officers	66
Appendix 3 AFP record keeping processes and practices	72
Appendix 4 AFP recruitment programs: modules and subjects	83



Audit snapshot

Auditor-General Report No.43 2020–21

Australian Federal Police's Use of Statutory Powers



Why did we do this audit?

- ▶ The Australian Federal Police (AFP) is the national and principal federal law enforcement agency of the Australian Government.
- ▶ The exercise of statutory powers should occur within an effective accountability and reporting framework.
- ▶ This audit complements a similar audit that the ANAO undertook in 2016–17 of the Australian Border Force.



Key facts

- ▶ The AFP has 6834 staff of which more than 4000 are either police officers or protective service officers.
- ▶ The AFP's 2020–21 budget was \$1.57 billion.
- ▶ 86 Commonwealth Acts confer powers on AFP officers.



What did we find?

- ▶ The AFP's framework to ensure the lawful exercise of powers in accordance with applicable legislation is largely effective.
- ▶ There are serious deficiencies in the AFP's record keeping practices and processes.



What did we recommend?

- ▶ The Auditor-General made three recommendations to the AFP around warrant review processes, record keeping and quality assurance.
- ▶ The AFP agreed to all three recommendations.

4000

approximate number of warrants issued to AFP in 2019–20.

97.8%

of *Crimes Act 1914* search warrants complied with Crimes Act requirements

Summary and recommendations

Background

1. The Australian Federal Police (AFP) is the national and principal federal law enforcement agency of the Australian Government. Its role is to enforce Commonwealth criminal law; contribute to combating complex, transnational, serious and organised crime impacting Australia's national security; and to protect Commonwealth interests from criminal activity in Australia and overseas. It also has responsibility for providing policing services to the Australian Capital Territory and Australia's territories, including Christmas Island, Cocos (Keeling) Islands, Norfolk Island and Jervis Bay.

2. The AFP's 2020–21 budget was \$1.57 billion and at 30 June 2020, it had 6834 staff, of whom 3247 were sworn police officers and 829 were Protective Service Officers.¹

Rationale for undertaking the audit

3. AFP officers are able to exercise powers under more than 80 separate Commonwealth Acts, including a range of powers pursuant to warrant. It is important that the AFP has appropriate administrative frameworks to ensure that powers are exercised lawfully and in accordance with authorised procedures; and that officers are adequately trained to exercise powers that are conferred upon them.

Audit objective and criteria

4. The objective of the audit was to assess the effectiveness of the AFP's framework to ensure the lawful exercise of powers in accordance with applicable legislation.

5. The high-level criteria were:

- Is there an effective accountability and reporting framework for the AFP's lawful exercise of powers?
- Do AFP officers have adequate knowledge of their powers and how to use them?

Conclusion

6. The AFP's framework to ensure the lawful exercise of powers in accordance with applicable legislation is largely effective. There are serious deficiencies in the AFP's record keeping practices and processes.

7. The AFP has a largely effective accountability and reporting framework for the lawful exercise of its powers. The AFP met statutory reporting requirements under three key Acts examined. However, internal records relating to execution of section 3E Crimes Act warrants are stored in a way whereby retrieval is unable to be achieved efficiently or with an assurance of completeness.

1 Protective Service Officers (PSOs) — have more limited powers than fully sworn officers and protect Commonwealth interests in Australia and overseas, including counter-terrorism first response at Australia's major airports and at Parliament House in Canberra.

8. The AFP's framework relating to training and guidance is largely effective. However, it has not undertaken a training needs analysis at the whole-of-organisation level and there is limited quality assurance assessment of operational activity.

Supporting findings

Accountability and reporting

9. The AFP has an appropriate *Risk Management Policy* and *Risk Management Framework* as required by the *Commonwealth Risk Management Policy*. The potential risk presented by failure to meet statutory requirements is explicitly recognised in one of its eight enterprise risks. The AFP's approach to managing legislative compliance within the context of the risk management framework has been under consideration since August 2016.

10. The AFP Hub contains 54 instruments of delegation and authorisation which are accessible to all AFP staff and answers a number of Frequently Asked Questions. Instruments issued by the Commissioner conferring intrusive powers under the *Crimes Act 1914* were complete and current.

11. The AFP is statutorily required to submit a variety of reports about the use of certain powers to the Parliament through the relevant Minister/s (and to the Commonwealth Ombudsman). The AFP met its statutory reporting requirements under three key Acts. However, the AFP does not systematically record other uses of statutory powers and does not produce internal reports on their use.

12. The ANAO's review of a random selection of warrants under the *Crimes Act 1914*; *Telecommunications (Interception and Access) Act 1979*; and the *Surveillance Devices Act 2004* found:

- the AFP appropriately exercises TIA Act and SD Act warrants;
- six of 272 section 3E Crimes Act warrants did not meet the requirements of the Crimes Act; and
- 149 of 272 (54.8 per cent) section 3E Crimes Act warrants examined were not prepared consistently with AFP best practice.

13. The ANAO found that the AFP's compliance with internal administrative requirements was inconsistent, with weaknesses identified in:

- documentation of mandatory review of section 3E Crimes Act warrants; and
- warrants and their associated documentation being uploaded into PROMIS.

Training and guidance

14. The AFP provides appropriate training for external recruits and offers continuing training opportunities to its ongoing staff. The AFP is accredited as a Registered Training Organisation and is able to provide nationally-recognised qualifications.

15. The AFP has not undertaken a training needs analysis at the whole-of-organisation level, although there was evidence of limited analysis undertaken focussed on Operational Safety Assessment training and recruit induction training.

16. The AFP does not have an organisation-wide quality assurance framework. Although its Investigations Standards and Practices area has undertaken some operational review activity, this has been limited since its establishment in 2014.

17. The AFP maintains records of officers' completion of mandatory training requirements and monitors their completion. In terms of Operational Safety Assessment, the AFP's records demonstrate improvement since the ANAO's previous examination in Auditor-General Report No.30 2015–16 *Management of the Use of Force Regime*.

18. The AFP maintains a suite of guidance and directions for staff through its Governance Instrument Framework which is readily accessible through the Hub. Although approximately half the instruments were overdue (or possibly overdue) for review at the time of audit, the AFP is presently reviewing the framework.

Recommendations

Recommendation no. 1 Paragraph 2.63

The Australian Federal Police enforces its requirement that section 3E Crimes Act warrants be thoroughly reviewed by at least a supervisor and retain documentary evidence that the review has occurred.

Australian Federal Police response: *Agreed.*

Recommendation no. 2 Paragraph 2.92

As a matter of urgency, the Australian Federal Police should implement an Electronic Data and Records Management System (EDRMS) to allow it to store records so that they are secure and readily accessible. It should cease its reliance on network drives.

Australian Federal Police response: *Agreed.*

Recommendation no. 3 Paragraph 3.30

The Australian Federal Police implement a systematic quality assurance process for its section 3E Crimes Act warrant application, execution and documentation.

Australian Federal Police response: *Agreed.*

Australian Federal Police response

19. The Australian Federal Police's full response is at Appendix 1.

Key messages from this audit for all Australian Government entities

20. Below is a summary of key messages which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance

- Where highly operational entities have an extensive suite of guidance material for staff, a balance needs to be achieved between a centrally-managed regime to ensure consistency of messaging and a decentralised model which may be more responsive to individual work area needs but risks duplication and overlap.
- Entities should avoid proliferation of guidance material which may make it challenging for staff to find the 'right' guidance document — and also creates a downstream administrative burden because such material must be periodically reviewed.

Records management

- An effective Electronic Data and Records Management System is essential for the management of digital records. The National Archives of Australia does not consider that network drives are acceptable for the storage of official records.

Audit findings

1. Background

Introduction

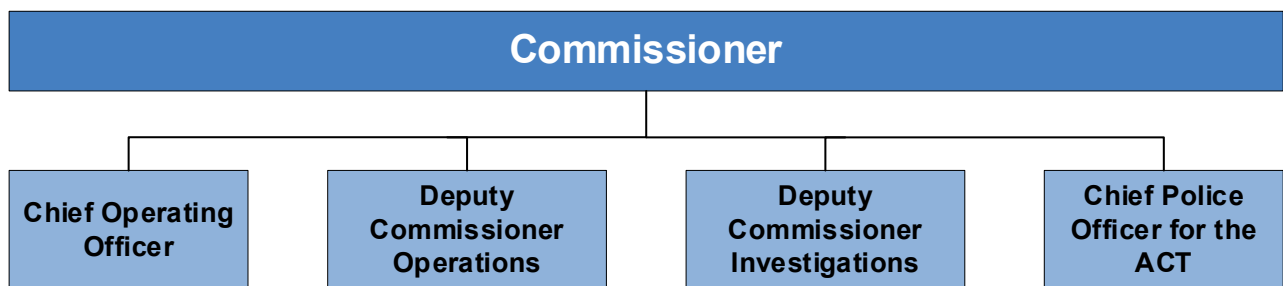
1.1 The Australian Federal Police (AFP) is the national and principal federal law enforcement agency of the Australian Government. Its role is to enforce Commonwealth criminal law; contribute to combating complex, transnational, serious and organised crime impacting Australia's national security; and to protect Commonwealth interests from criminal activity in Australia and overseas. It also has responsibility for providing policing services to the Australian Capital Territory (ACT) and Australia's territories, including Christmas Island, Cocos (Keeling) Islands, Norfolk Island and Jervis Bay.

1.2 The AFP's vision is 'Policing for a safer Australia' and its mission is 'As Australia's national policing agency we protect Australians and Australia's interests.'

Structure and organisation

1.3 The AFP is headed by a Commissioner, supported by four Deputies as shown in Figure 1.1.

Figure 1.1: AFP organisational structure at 16 April 2021



Source: AFP

1.4 The current AFP Commissioner was appointed in October 2019. Following his appointment, the Commissioner announced his 'Commissioner's Intent' which included:

- supporting the frontline;
- reducing red tape; and
- enhancing partnerships with state and territory police forces.

1.5 Following the Commissioner's appointment, the AFP commissioned a review of the AFP's structure and operating model. The review made seven recommendations, all of which were accepted.² Changes flowing from the review relevant to this audit were:

- a review of the governance framework;

2 The recommendations related to: a new organisational structure; standardising the delivery of strategic programs and performance measurement; revising and aligning purpose, strategy and organisational priorities to support the Commissioner's intent; growing and delivering leading capabilities by establishing capability delivery hubs; strengthening strategic workforce planning, supply/demand management and prioritisation modelling; developing a National Policing Operations/State Service Centre; and leveraging innovative technology and data to enhance operational delivery.

- a move to a geographic (as opposed to functional) structure; and
- the creation of a Learning Command headed by a Chief Learning Officer.

Staffing and budget

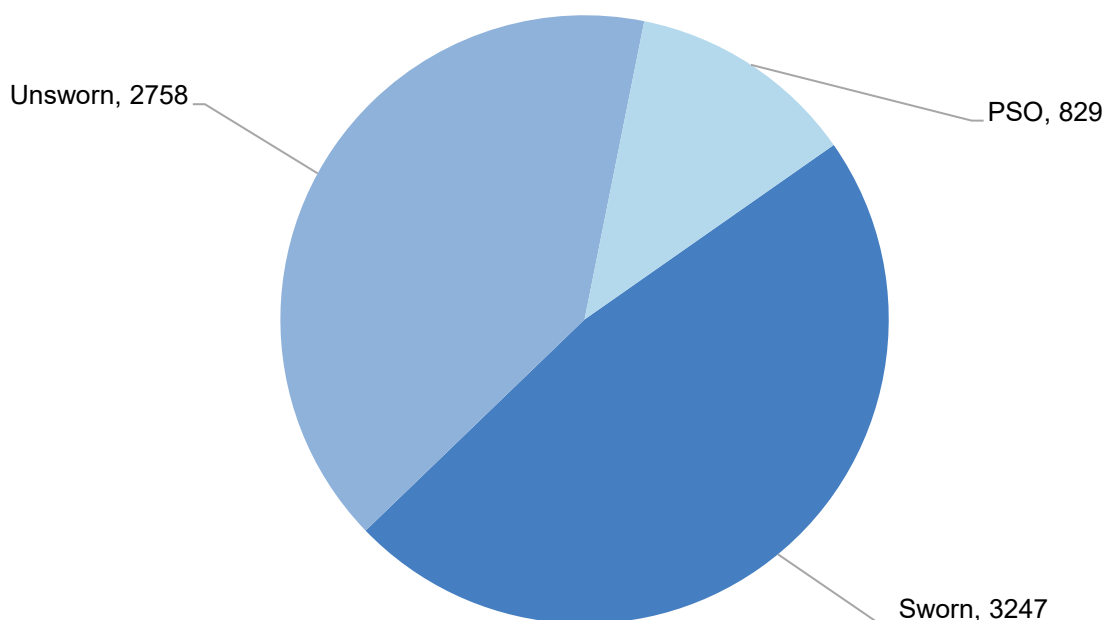
Staffing

1.6 At 30 June 2020, the AFP had a total of 6834 staff. AFP staff are classified into three categories:

- Members of the AFP (also known as sworn officers) — have full police powers and are able to enforce the law;
- Protective Service Officers (PSOs) — have more limited powers than fully sworn officers and protect Commonwealth interests in Australia and overseas, including counter-terrorism first response at Australia’s major airports and at Parliament House in the ACT; and
- AFP appointees (also known as unsworn officers) — non-policing or civilian roles including IT and business support, forensics, intelligence, investigative assistants, and human resource management roles.

1.7 Figure 1.2 details the number of AFP staff in each category.

Figure 1.2: AFP staffing at 30 June 2020



Source: Australian Federal Police, *Annual Report 2019–20*, AFP, 2020.

Budget

1.8 The AFP has two outcomes. These are shown in Table 1.1.

Table 1.1: AFP 2020–21 budget

Outcome	Detail	2020–21 budget (\$m)
1	Reduced criminal and security threats to Australia's collective economic and societal interests through cooperative policing services	1,390.0
2	A safe and secure environment through policing activities on behalf of the Australian Capital Territory Government	179.3
Total		1,569.3

Source: Australian Federal Police, *Agency Resourcing 2020–21, Budget Paper No.4*, AFP, 2020.

AFP powers

1.9 In planning this audit, the ANAO identified 86 Commonwealth Acts which potentially confer more than 800 separate powers upon AFP officers. The audit focusses on powers that would generally be regarded by the community as intrusive powers (such as arrest, search and seizure), as these powers have the greatest impact on individuals rather than less significant powers (such as the power to issue a speeding infringement). A list of the Commonwealth Acts and associated powers is at Appendix 2.

1.10 In addition, AFP employees can exercise certain powers under some state and territory legislation in those cases where state and territory legislation allows AFP officers to be recognised as 'special constables' (or similar terminology).³ The use by AFP officers of provisions under state and territory legislation was outside the scope of this audit.

Rationale for undertaking the audit

1.11 Powers such as searching premises and intercepting telecommunications are intrusive and can significantly impact members of the community. It is important that police officers be well trained and exercise their powers consistently with both applicable legislation, and with internal instructions and directions about the way in which powers are to be exercised. Accurate, accessible and complete record-keeping is fundamental to the effective administration of justice.

1.12 In February 2017, the ANAO tabled a performance audit: *The Australian Border Force's Use of Statutory Powers*⁴, and an examination of the Australian government's other key law enforcement agency, the AFP, complements that report.

3 These powers can be available where they are expressly stated to apply to AFP members, where AFP members are sworn in as special constables, or similar, in the jurisdiction in which they are performing functions, or by virtue of the *Australian Federal Police Act 1979* which confers on AFP members the powers of a constable in the state or territory in which the member is performing policing functions in certain circumstances.

4 Auditor-General Report No. 39 2016–17 [The Australian Border Force's Use of Statutory Powers](#).

Audit approach

Audit objective, criteria and scope

Objective

1.13 The objective of the audit was to assess the effectiveness of the AFP's framework to ensure the lawful exercise of powers in accordance with applicable legislation.

Criteria

1.14 The high-level criteria were:

- Is there an effective accountability and reporting framework for the AFP's lawful exercise of powers?
- Do AFP officers have adequate knowledge of their powers and how to use them?

Scope

1.15 The audit focusses on the AFP's federal policing functions as:

- ACT Policing was the subject of an ANAO audit in 2012–13⁵; and
- PSOs, while sworn officers, have more limited powers than fully sworn police officers. They are responsible for protective security at particular Commonwealth sites (such as Parliament House, international airports and official establishments).

1.16 During the audit, it became apparent that there are serious deficiencies in the AFP's record keeping processes and practices. The ANAO considered that these deficiencies pose a risk to the AFP's ability to achieve its core functions. Consequently, the ANAO broadened the scope of the audit to include record keeping (see Appendix 3).

1.17 As noted at paragraph 1.10, under certain circumstances, AFP officers may exercise powers under state or territory legislation. The ANAO did not examine the AFP's use of such powers.

Audit methodology

1.18 The audit team examined and analysed AFP records and consulted with various AFP staff. The team also met (virtually or in person) with:

- the Parliamentary Joint Committee on Law Enforcement;
- the Parliamentary Joint Committee on Intelligence and Security;
- the Office of the Commonwealth Ombudsman;
- the Office of the Commonwealth Director of Public Prosecutions; and
- the Office of the Australian Commission for Law Enforcement Integrity.

5 Auditor-General Report No. 13 2012–13 *The Provision of Policing Services to the Australian Capital Territory*. The AFP provides community policing services in the ACT under a contract with the ACT government. The audit was generally positive and concluded that 'The AFP is effectively managing the delivery of policing services to the ACT. The AFP is delivering the level and type of community policing services agreed with the ACT Government, and is consistently meeting the majority of its performance targets'.

1.19 In addition to assessing the adequacy of the AFP's framework supporting its use of statutory powers, the audit team undertook detailed testing and analysis of a random selection of warrants issued under selected Commonwealth legislation.

1.20 The audit was conducted in accordance with the ANAO Auditing Standards at a cost to the ANAO of approximately \$532,000.

1.21 The team members for this audit were Julian Mallett, Amanda Ronald, Zoe Pilipczyk, Anne Kent, Sam Jones, Lesa Craswell and Alex Wilkinson.

Relevant recent reports

Parliamentary Joint Committee on Intelligence and Security

1.22 The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is constituted under section 28 of the *Intelligence Services Act 2001*.⁶ At the time the ANAO conducted this audit, the PJCIS had five current inquiries relevant to the scope of this audit.⁷

1.23 Recent past inquiries conducted by the PJCIS that the ANAO examined as background to this audit included:

- Review of the mandatory data retention regime (October 2020)⁸;
- Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (August 2020)⁹;
- Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (April 2019)¹⁰;
- Review of police stop, search and seizure powers, the control order regime and the preventative detention order regime (February 2018)¹¹; and
- Advisory report on the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (February 2015).¹²

6 It has three main types of functions, including: providing oversight of Australian intelligence agencies by reviewing their administration and expenditure; building bipartisan support for national security legislation by reviewing national security bills introduced to Parliament; and ensuring national security legislation remains necessary, proportionate and effective by conducting statutory reviews.

7 Review of AFP Powers, Review of Part 14 of the *Telecommunications Act 1997* – Telecommunications Sector Security Reforms, Review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, Review of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* and *Telecommunications Legislation Amendment (International Production Orders) Bill 2020*.

8 Parliamentary Joint Committee on Intelligence and Security, *Review of the mandatory data retention regime*, October 2020.

9 Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*, August 2020.

10 Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, April 2019.

11 Parliamentary Joint Committee on Intelligence and Security, *Review of police stop, search and seizure powers, the control order regime and the preventative detention order regime*, February 2018.

12 Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.

1.24 Other relevant reviews included:

- A report concerning the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and related matters¹³ (June 2020);
- Review into the AFP's response to and management of sensitive investigations (Lawler Review) (January 2020)¹⁴;
- Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review) (December 2019)¹⁵;
- Committee of Privileges, *Parliamentary Privilege and the use of search warrants* (April 2019);
- Committee of Privileges, *Parliamentary privilege and the use of intrusive powers* (March 2018); and the
- Inquest into the deaths arising from the Lindt Café siege (May 2017).¹⁶

13 Independent National Security Monitor, *Trust but Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, June 2020.

14 John Lawler AM APM, *Review into the AFP's response to and management of sensitive investigations*, January 2020.

15 Dennis Richardson AC, *Comprehensive Review of the Legal Framework of the National Intelligence Community*, December 2019.

16 State Coroner of New South Wales, *Inquest into the deaths arising from the Lindt Café siege*, May 2017.

2. Accountability and reporting

Areas examined

The ANAO examined whether there was an effective accountability and reporting framework for the Australian Federal Police's (AFP's) lawful exercise of powers. The ANAO also reviewed a random selection of warrants under three key Acts.

Conclusion

The AFP has a largely effective accountability and reporting framework for the lawful exercise of its powers. The AFP met statutory reporting requirements under three key Acts examined. However, internal records relating to execution of section 3E Crimes Act warrants are stored in a way whereby retrieval is unable to be achieved efficiently or with an assurance of completeness.

Areas for improvement

The ANAO made two recommendations aimed at:

- the AFP enforcing its requirement that section 3E Crimes Act warrants be thoroughly reviewed by at least a supervisor and retain documentary evidence that the review has occurred; and
- the AFP implementing an Electronic Data and Records Management System as a matter of urgency.

Does the AFP have an appropriate risk management framework in place in relation to the use of statutory powers?

The AFP has an appropriate *Risk Management Policy* and *Risk Management Framework* as required by the *Commonwealth Risk Management Policy*. The potential risk presented by failure to meet statutory requirements is explicitly recognised in one of its eight enterprise risks. The AFP's approach to managing legislative compliance within the context of the risk management framework has been under consideration since August 2016.

2.1 Where Parliament confers statutory powers to enable officers to monitor and enforce compliance with regulation, there is an associated risk that those powers may be exercised unlawfully. Unlawful exercise of statutory powers may result in adverse impacts on individuals, such as deprivation of liberty as a result of the invasion of a person's privacy through the execution of a warrant. Other consequences include exclusion of evidence leading to failed prosecutions or overturned decisions, compensation claims against the Commonwealth, or reputational damage. In this section, the ANAO considered the appropriateness of AFP's enterprise risk management and operational risk management in relation to the use of its statutory powers.

Enterprise risk management

2.2 Section 16 of the *Public Governance, Performance and Accountability Act 2013* states 'The accountable authority of a Commonwealth entity must establish and maintain ... an appropriate system of risk oversight and management for the entity ...'

2.3 The *Commonwealth Risk Management Policy* creates a framework with which non-corporate Commonwealth entities must comply in order to establish an appropriate system of risk oversight and management.

2.4 The AFP's *Risk Management Policy* and *Risk Management Framework* was last reviewed and endorsed by the AFP Commissioner on 1 April 2019 and published on its intranet on 10 April 2019. In 2019, the AFP Risk Profile was also revised, reducing the AFP's previous 22 enterprise risks to eight, including the risk of the AFP not complying with professional standards, values, regulatory framework and statutory requirements, as shown in Table 2.1. The AFP advised that the AFP *Risk Management Framework* has been reviewed and is in the final stages of Accountable Authority endorsement.

Table 2.1: AFP enterprise risks at 18 March 2019

No.	Risk	Risk description	Risk rating
E1	Health, Safety and Wellbeing	Illness, injury or other health conditions which decrease the wellbeing and performance of the AFP workforce.	High
E2	Culture, Standards and Integrity	Systemic failure to comply with the AFP's professional standards, values, regulatory framework and statutory requirements.	High
E3	Operational Outcomes	Failure to achieve AFP's identified operational outcomes.	Significant
E4	Partnerships and Stakeholder Engagement	Failure to develop and coordinate effective relationships with domestic and international law enforcement, Government and non-government organisations, industry and academic partners.	Medium
E5	Effectiveness of AFP capabilities	The AFP's capabilities fail to adjust to a changing operating environment.	Significant
E6	Workforce	The AFP fails to attract, retain and maintain a workforce with the skills and capabilities aligned to the AFP's future organisational needs.	High
E7	Resourcing	Mismanagement or misuse of the resources the AFP needs to meet its operational objectives.	Significant
E8	Information	Systemic failure to effectively collect, use, manage or protect information.	High

Source: AFP.

2.5 The current *Risk Management Policy* and *Risk Management Framework* includes references to a number of supporting documents, including the National Guideline on Risk Management. These documents are available to all staff via the Hub, the AFP's intranet.

Operational risk management

2.6 In August 2016, the AFP's Audit and Risk Committee began discussions about the possible introduction of a Legislative Compliance Framework. In August 2017, the AFP's Chief Counsel provided the Audit and Risk Committee with the main legislation relevant to the operations of the AFP, including the key requirements of the legislation, the consequences of non-compliance and the attribution of risk to the relevant functional area. In November 2018, the Audit and Risk

Committee elected not to progress the development of the Framework.¹⁷ The proposed approach to legislative compliance was again considered at the February 2021 Audit and Risk Committee meeting. At that meeting, the National Manager Strategy and Performance briefed the Committee on a recent internal workshop with key functions related to legislative compliance, including risk, assurance, internal audit, legislation reform, and enterprise governance as well as the status of the review of the Governance Instrument Framework (see paragraphs 3.45 to 3.48). It was agreed that the matter would be further considered at the Committee's May 2021 meeting.

2.7 This audit's review of a random selection of warrants (see paragraphs 2.24 to 2.90) suggest that there are weaknesses in the AFP's processes to monitor the risk of legislative and administrative non-compliance in an operational context.

Are instruments of delegation and authorisation accessible, complete and current?

The AFP Hub contains 54 instruments of delegation and authorisation which are accessible to all AFP staff and answers a number of Frequently Asked Questions. Instruments issued by the Commissioner conferring intrusive powers under the *Crimes Act 1914* were complete and current.

2.8 When Parliament creates a statutory power it vests that power in an individual or body who is then able to exercise it. There are three ways in which a person can exercise powers under Commonwealth legislation:

- as of right — powers conferred directly upon officers. For example, in the *Crimes Act 1914*, many powers are given to 'constables' who are defined to mean members of the AFP (and also members of the police force of a state or territory);
- delegation — powers conferred on senior positions, such as a Minister, Secretary or Commissioner, that are delegated to other officers; and
- authorisation — powers conferred on officers who are authorised under a separate provision.

2.9 The key difference between a delegation and an authorisation is that a person exercising a delegation cannot be directed about how to exercise the power, whereas under an authorisation, a person can be required to follow particular 'rules' about how and when the power can be exercised.¹⁸ Delegations and authorisations must be in writing, and are known as instruments.

2.10 Since the exercise of a power by a person who does not have the legal power to do so may be unlawful, it is imperative that entities ensure that delegations and authorisations are up to date and complete.

17 The Audit and Risk Committee noted that 'while there is always room for improvement, and the AFP is currently undertaking a project to review the AFP Risk Profile, there have not been any obvious failings in the current systems to necessitate the introduction of the Framework at this time.'

18 Department of Finance, *Glossary* [Internet], available from <https://www.finance.gov.au/about-us/glossary> [accessed 12 May 2021].

2.11 The AFP has a specific webpage called the Delegations and Authorisations Collection (the Collection) within the Governance Framework section of the Hub. The webpage contains a number of useful and important Frequently Asked Questions such as:

- What is a delegation?
- What is an authorisation?
- What are your responsibilities and obligations as a delegate?

2.12 The Collection includes a total of 54 authorisations and delegations.¹⁹ The Collection webpage states that it ‘includes all statutory delegations and authorisations that apply to AFP appointees as at 8 July 2016, and will continue to capture all instruments as they are updated from that date.’

2.13 Although not all of the 54 instruments conferred powers which fell within the scope of this audit, for completeness the ANAO examined whether all of them were current at the time of audit and found that two had expired and were therefore no longer valid. The AFP advised that these would be removed from the Collection.

2.14 As noted in paragraph 1.9, the ANAO identified 86 Acts which confer statutory powers upon AFP officers. However, most of the commonly-used powers²⁰ are contained in the *Crimes Act 1914*. The ANAO examined the nine instruments issued by the Commissioner under this Act and found all nine were current, and had been reissued by the Commissioner shortly after his appointment (see paragraph 1.4).²¹

Does the AFP maintain adequate records when powers have been exercised?

The AFP is statutorily required to submit a variety of reports about the use of certain powers to the Parliament through the relevant Minister/s (and to the Commonwealth Ombudsman). The AFP met its statutory reporting requirements under three key Acts. However, the AFP does not systematically record other uses of statutory powers and does not produce internal reports on their use.

2.15 In a highly operational organisation such as the AFP, accurate and timely reporting is important. It assists with the planning and evaluation of operational activity; contributes to demonstrating accountability for actions and decisions; and supports analysis and comparison of operational effectiveness across Commands.

19 It also contains seven other legal instruments (such as instruments of appointment).

20 These include powers to execute warrants, search and arrest without warrant, question, require production of documents and seize goods.

21 There were six instruments which had been issued by previous AFP Commissioners. An instrument of delegation or authorisation issued by a holder of a position or office does not automatically become invalid if the holder of the position changes. However, it is considered good legal and administrative practice for a new holder of a position to review and reissue such instruments, particularly if they involve the use of intrusive powers. None of the six instruments issued by previous Commissioners related to such powers.

Internal reporting

2.16 The ANAO's initial audit approach was to review the AFP's internal reporting on all significant uses of statutory powers. However, the AFP does not systematically record or report internally on uses of statutory powers. Records are stored in a way which does not allow them to be retrieved efficiently, or with an assurance of completeness. Appendix 3 provides the ANAO's analysis of the AFP's records management processes and practices.

External reporting

2.17 The AFP is statutorily required to provide a variety of reports about the use of certain powers to Parliament and to relevant Minister/s and to the Commonwealth Ombudsman. In this section, the ANAO assessed whether the AFP met its statutory reporting requirements for the period 2019–20 under the:

- *Crimes Act 1914* (Crimes Act);
- *Telecommunications (Interception and Access) Act 1979* (TIA Act); and
- *Surveillance Devices Act 2004* (SD Act).²²

2.18 The ANAO observed that when there was a specific statutory external reporting requirement, the AFP provided the required reports.

Crimes Act 1914

2.19 Table 2.2 shows the AFP's statutory reporting requirements under the Crimes Act. In the period 2019–20, the AFP met these requirements.

Table 2.2: AFP statutory reporting requirements under the Crimes Act

Section	Subject	Recipient	Timing
3UJA	Terrorist acts and terrorism offences	Minister for Home Affairs, the Independent National Security Legislation Monitor and the Parliamentary Joint Committee on Intelligence and Security	As soon as practicable after the exercise of a power or powers
3ZZFB	Delayed notification search warrants	Minister for Home Affairs	Annual
15HM	Controlled operations	Minister for Home Affairs (and Commonwealth Ombudsman)	Biannual ^a
15HN ^b	Controlled operations	Minister for Home Affairs (and Commonwealth Ombudsman)	Annual ^c
15JS	Integrity testing	Attorney-General	Annual
15LD	Assumed identities	Attorney-General	Annual
15MU	Witness protection	Attorney-General	Annual

Note a: As part of the AFP's report on Controlled Operations between 1 January and 30 June 2020, the AFP reported on three controlled operations from the previous reporting period which had not been included in the previous

22 The ANAO limited its examination to reports that the AFP is required to submit to the Minister because the Ombudsman separately reports about information that the AFP is required to submit to it.

report, and revised the information provided for 27.7 per cent of the Controlled Operations previously reported on.

Note b: Part IAB Section I5HN of the Act requires the Minister for Home Affairs, to exclude from the Annual Report information that if made public, could reasonably be expected to: endanger a person's safety; identify or is likely to identify any person involved in the Controlled Operation; prejudice an investigation or prosecution; compromise any law enforcement agency's operational activities or methodologies; or making the information public would be contrary to the public interest for any other reason. Sixteen Controlled Operations were excluded either partially or fully in the 2019–20 Annual Report.

Note c: In 2019–20, 27.5 per cent of the AFP's reported Controlled Operations resulted in at least one arrest. In total, 28 persons of interest were arrested.

Source: *Crimes Act 1914* and ANAO analysis based on AFP data.

Telecommunications (Interception and Access) Act 1979

2.20 Table 2.3 shows the AFP's statutory reporting requirements under the TIA Act. For each TIA warrant issued, section 94 of the TIA Act requires the AFP to provide to the Minister a report containing information including:

- how the information obtained under the warrant was used;
- whether the information was conveyed to anyone outside the AFP;
- the number of arrests that have been (or are likely to be) made on the basis of the information obtained under the warrant; and
- the usefulness of the information obtained by interceptions under the warrant.

2.21 In practice, these reports are compiled and submitted to the Minister within three months after warrants cease to be in force.

2.22 As part of its assessment of a random selection of warrants, the ANAO found that all of the 24 warrants examined met the reporting requirement under section 94 of the TIA Act (see paragraph 2.82). In the period 2019–20, the AFP met all other reporting requirements detailed in Table 2.3.

Table 2.3: AFP statutory reporting requirements under the TIA Act

Section	Related power	Recipient	Timing
94	Telecommunications interception warrants	Minister for Home Affairs	Within 3 months after each warrant ceases to be in force
99	Telecommunications interception warrants	Minister for Home Affairs	Annual ^a
159	Stored communication warrants	Minister for Home Affairs	Annual ^b
186	Authorisations for access to existing information or documents	Minister for Home Affairs	Annual

Note a: In 2019–20, 137 arrests were made on the basis of information obtained through the use of intercepted telecommunications.

Note b: In 2019–20, 11 arrests were made on the basis of information obtained through the use of stored communications.

Source: *Telecommunications (Interception and Access) Act 1979* and ANAO's analysis based on AFP's data.

Surveillance Devices Act 2004

2.23 Similarly to the TIA Act, for each SD warrant issued, section 49 of the SD Act requires the AFP to provide the Minister with a report outlining a range of information about each warrant. The ANAO found that all SD Act warrants examined met this reporting requirement (see paragraph 2.90). In addition, section 50 of the SD Act requires the AFP to provide the Minister with an annual report which the Minister must table in Parliament. In the period 2019–20, the AFP met the reporting requirements under sections 49 and 50 of the SD Act.

Table 2.4: AFP statutory reporting requirements under the SD Act

Section	Related power	Recipient	Timing
49	Surveillance device warrants and control order (access) warrants	Minister for Home Affairs	As soon as practicable after a surveillance device warrant ceases to be in force and within six months after control order (access) warrant is issued.
50	Surveillance device warrants and computer access warrants	Minister for Home Affairs	Annual ^a

Note a: In 2019–20, 129 arrests and 112 prosecutions were made on the basis of information obtained by the use of a surveillance device under a warrant; access under a warrant to data held in a computer; an emergency authorisation for the use of a surveillance device; an emergency authorisation for access to data held in a computer; or a tracking device authorisation.

Source: *Surveillance Devices Act 2004* and ANAO analysis based on AFP data.

Does the AFP appropriately exercise statutory powers under warrant?

The ANAO's review of a random selection of warrants under the *Crimes Act 1914*; *Telecommunications (Interception and Access) Act 1979*; and the *Surveillance Devices Act 2004* found:

- the AFP appropriately exercises TIA Act and SD Act warrants;
- six of 272 section 3E Crimes Act warrants did not meet the requirements of the Crimes Act; and
- 149 of 272 (54.8 per cent) section 3E Crimes Act warrants examined were not prepared consistently with AFP best practice.

The ANAO found that the AFP's compliance with internal administrative requirements was inconsistent, with weaknesses identified in:

- documentation of mandatory review of section 3E Crimes Act warrants; and
- warrants and their associated documentation being uploaded into PROMIS.

2.24 The AFP can exercise a range of powers under warrants including search, arrest, surveillance and interception of telecommunications. It is important that these warrants are prepared and executed strictly in accordance with the legislation that governs them. In this section, the ANAO reviewed a random selection of warrants issued under three Acts:

- search warrants under section 3E of the Crimes Act;
- the TIA Act; and

- the SD Act.

2.25 These three Acts accounted for more than 90 per cent of warrants sought by the AFP in 2019–20.

2.26 Irrespective of under which Act the warrants are issued and for what purpose, the process for all warrants is broadly similar: an application is made to an issuing officer²³ who may then sign and issue a warrant, provided that he or she is satisfied that there are adequate grounds to justify its issue. Box 1 below explains some key terms relating to warrants.

Box 1: Warrants: key terms

Application

Accompanies an affidavit to the issuing officer and contains details about the warrant being sought. A formal application is not required for the Crimes Act but is required for the TIA and SD Acts.

Affidavit

A written statement submitted to the issuing officer. The author of an affidavit is required to swear by oath or make an affirmation that the contents are true. An affidavit is required for every warrant application.

Search warrant

‘A search warrant is a document issued under authority of law which authorises the holder to enter and search private premises, or sometimes to search a person, and to seize evidential material. It authorises what would otherwise be a trespass and would be an actionable tort.’^a

Issuing officer

An independent person with the power to issue a warrant. For section 3E Crimes Act warrants, this may be a magistrate, a justice of the peace or a ‘person employed in a court of a state or territory who is authorised to issue search warrants or warrants for arrest’. For the TIA and SD Acts, the power to issue warrants is limited to an ‘eligible Judge or nominated AAT member.’^{b c}

Executing Officer

Section 3E Crimes Act warrants are issued to a named executing officer who will be the officer in charge of the execution of the warrant. The executing officer must be present when the warrant is executed (see paragraph 2.47).

Note a: Source: Commonwealth Director of Public Prosecutions’ *Search Warrant Manual*, April 2018.

Note b: ‘Eligible’ means a judge who has consented to be an issuing officer and has been declared by the Minister to be so. A nominated Administrative Appeals Tribunal (AAT) member must have legal qualifications.

Note c: In August 2020, the Parliamentary Joint Committee on Intelligence and Security recommended that for journalist information warrants, only Supreme or Federal Court judges should be able to issue section 3E Crimes Act search warrants. The government accepted this recommendation, but the necessary legislative amendments have not yet occurred.

Source: ANAO.

23 The Crimes Act uses the term ‘issuing officer’ while the TIA and SD Acts do not. For convenience, the term ‘issuing officer’ is used in this report to refer to a person who is authorised to issue a warrant.

2.27 Courts have been strict in their interpretation of the law in both the issue of warrants and their execution by police, and have excluded evidence on the basis of technical or procedural deficiencies. In this respect, the High Court has stated²⁴:

in construing and applying such statutes, it needs to be kept in mind that they authorise the invasion of interests which the common law has always valued highly and which, through the writ of trespass, it went to great lengths to protect. Against that background the enactment of conditions which must be fulfilled before a search warrant can be lawfully issued and executed is to be seen as a reflection of the legislature's concern to give a measure of protection to those interests. To insist on strict compliance with the statutory conditions governing the issue of search warrant is simply to give effect to the purpose of the legislation.²⁵

2.28 Evidence obtained as a result of a warrant may be determined by a court as inadmissible for two possible reasons. The first is as a result of a technical deficiency in the warrant itself, such as the issuing officer not signing the warrant or not including the date of its expiry (see paragraphs 2.52 to 2.54). The second possible reason is where the warrant itself was valid but there was a deficiency in the way that it was executed. Examples include if the warrant was executed after it had expired, or the executing officer was not present at the search (in the case of section 3E Crimes Act warrants).²⁶

The AFP's use of warrants

2.29 Table 2.5 below identifies the number and types of warrants issued to the AFP in the last three financial years.²⁷ The data in Table 2.5, supplied by the AFP, carried a number of caveats as to its accuracy. Numbers of warrant types shown with an asterisk were compiled by the AFP from warrant registers that are required to be kept by the legislation governing them, and are regarded by the AFP as accurate. The number of warrant types without an asterisk were obtained by using a keyword search for the word 'warrant' in PROMIS.²⁸ The AFP advised:

24 *George v Rockett* [1990] 170 CLR 104 (High Court of Australia).

25 In a speech to the House of Commons in March 1763, Pitt the Elder said:

'The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail - its roof may shake - the wind may blow through it - the storm may enter - the rain may enter - but the King of England cannot enter - all his forces dare not cross the threshold of the ruined tenement.'

26 Where evidence has been obtained in such circumstances, it is not automatically invalid: section 138 of the *Evidence Act 1995* provides that such evidence 'is not to be admitted unless the desirability of admitting the evidence outweighs the undesirability of admitting evidence that has been obtained in the way in which the evidence was obtained.'

27 The Acts under which these warrants were issued were: the *Crimes Act 1914* (search, control order monitoring); the *Extradition Act 1988* (surrender, extradition); the *Mutual Assistance in Criminal Matters Act 1987* (mutual assistance); the *Proceeds of Crime Act 2002* (proceeds of crime); the *Surveillance Devices Act 2004* (surveillance device, retrieval, computer access); and the *Telecommunications (Interception and Access) Act 1979* (telecommunications intercept, stored communication and journalist information). Arrest warrants may be issued under the *Crimes Act 1914* and a number of other Commonwealth and state and territory Acts. In December 2020, the government introduced the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 which proposes the creation of three new types of warrant: data disruption warrants, network activity warrants and account takeover warrants.

28 PROMIS (Police Real-time Online Management Information System) is the AFP's case management system.

These figures are indicative only and do not capture all warrants issued to the AFP that are not saved into PROMIS, nor those warrants saved by members as other types of documents (including correspondence and planning for example).

2.30 The AFP advised that 'operationally there has been no need to capture all warrant statistics in a form that is centrally extractable.' The ANAO's examination of a random selection of warrants as described below showed that 26.3 per cent of issued warrants were not saved into PROMIS and that assigned keywords were often incorrect or misleading. Table 2.5 is therefore limited by these caveats. It is of concern to the ANAO that the AFP does not accurately record the number of section 3E Crimes Act warrants it has been issued, or that it has executed.

Table 2.5: Warrants issued to AFP 2017–18 to 2019–20 (indicative only)

Type	Number of warrants issued			
	2017–18	2018–19	2019–20	Total
Search	2125	2065	2483	6673
Telecommunications intercept ^a	724	634	636	1994
Surveillance device ^a	596	555	620	1771
Arrest	143	135	105	383
Stored Communication ^a	61	100	72	233
Retrieval ^a	16	23	16	55
Computer Access ^a	0	7	16	23
Mutual Assistance	13	11	15	39
Surrender	2	9	12	23
Proceeds of Crime	8	1	10	19
Extradition	8	7	8	23
Control Order Monitoring ^a	0	0	8	8
Journalist Information ^a	2	6	0	8
Total	3698	3553	4001	11,252

Note a: See paragraph 2.29.

Source: AFP unaudited advice.

ANAO assessment of warrants

2.31 When a decision is made to seek a warrant in the course of an AFP investigation, there are two sets of requirements that officers must observe:

- the first is that the requirements of the applicable legislation must be met, which is referred to below as statutory compliance; and
- the second set of requirements is the suite of directions, instructions and guidance contained in various documents which make up the AFP's Governance Instrument Framework (GIF).²⁹ This is referred to below as administrative compliance.³⁰ Some of these 'instruments' contain mandatory requirements: others encourage 'better practice.'

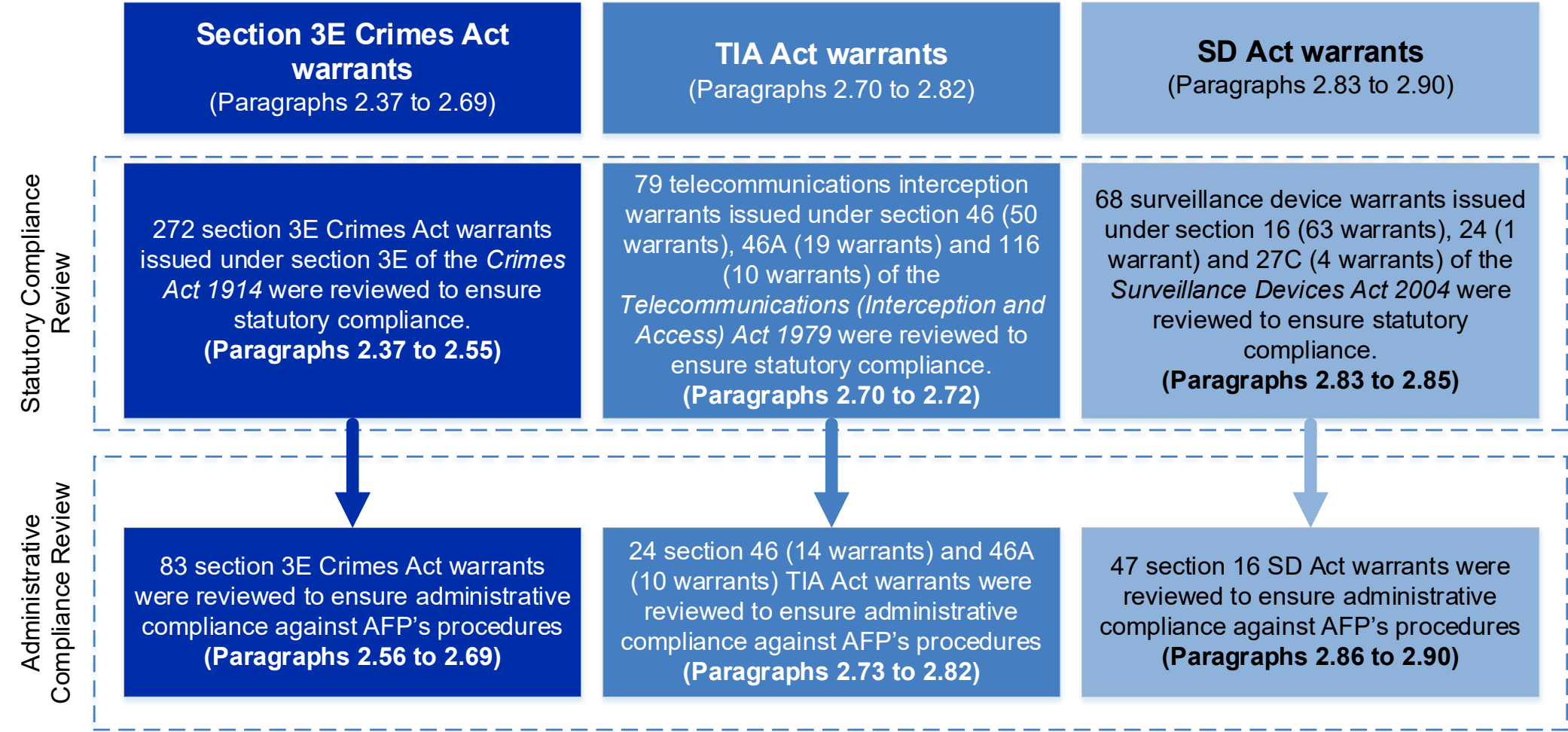
2.32 In the following paragraphs, the two sets of requirements are distinguished as 'statutory compliance' for compliance with relevant legislation and 'administrative compliance' for compliance with the AFP's internal governance instruments.

2.33 Figure 2.1 outlines how the analysis that follows is laid out.

29 The GIF is discussed in Chapter 3.

30 The GIF instruments relevant to this analysis are: Better Practice Guide: *Crimes Act 1914* Search Warrants (2018); Investigation Practice Standard — Search Warrants (2015); Better Practice Guide: *Telecommunications Interception and Access Act 1979* (2017); National Guideline on telecommunications interception and accessing stored communication (2006); Better Practice Guide: Surveillance Devices (2017) and National Guideline on surveillance device warrants, computer access warrants and tracking device authorisations under the *Surveillance Devices Act 2004*.

Figure 2.1: Outline of ANAO’s warrant assessment for statutory and administrative compliance



Source: ANAO.

Selection of warrants for examination

2.34 The ANAO randomly selected 50 PROMIS³¹ case numbers which had at least one warrant issued in 2019–20³², and extracted all of the uploaded section 3E Crimes Act, TIA Act and SD Act warrants attached to these case numbers. As a single PROMIS case may contain more than one warrant, the ANAO's selection of 50 PROMIS cases across the three Acts resulted in a total of 419 warrants as shown in Table 2.6.³³

2.35 The ANAO undertook a statutory compliance review of all 419 warrants selected. However, it became apparent that locating all relevant records in order to conduct an administrative compliance review of all 419 warrants in many cases required the AFP to contact individual case officers across Australia. Consequently, the administrative compliance review in this audit is limited to 154 of the 419 warrants selected.³⁴ Further ANAO comment on the appropriateness of the AFP's record keeping practices can be found in Appendix 3 of this report.

2.36 Administrative procedures for the drafting of warrants are set out in the AFP's *Better Practice Guides* applicable to each warrant type.³⁵

Table 2.6: Warrants reviewed as part of ANAO legislative and administrative compliance review

	3E Crimes Act	TIA Act	SD Act	Total
Legislative compliance review	272	79	68	419
Administrative compliance review	83	24	47	154

Note: All administrative compliance review warrants also underwent a statutory compliance review.

Source: ANAO analysis based on AFP data.

Section 3E Crimes Act warrants

Statutory compliance of section 3E Crimes Act warrants

2.37 The ANAO assessed whether 272 section 3E Crimes Act warrants were obtained and executed in accordance with the legislation. The warrants were assessed regardless of whether or

31 The smallest number of warrants for any one PROMIS case in the ANAO's sample was one; the largest was 54.

32 The earliest issued warrant was a section 3E Crimes Act warrant issued on 11 October 2007, with the latest being 30 October 2020.

33 The ANAO had originally intended to review the processes around 50 randomly chosen warrants. However, this was not possible as individual warrants are not assigned any form of unique identifier. Matters being investigated are assigned PROMIS case numbers and some (but not all) documents relating to that case are filed in PROMIS.

34 The ANAO took a convenience sample of 50 affidavits drawn from the 50 PROMIS cases originally randomly selected.

35 The AFP maintains a GIF which is intended not only to provide guidance but also directions and instructions. These instruments include *Better Practice Guides*. A further examination of the AFP's governance instruments is contained in paragraphs 3.40–3.48 of this report.

not the search warrant was executed³⁶ (207 or 76.1 per cent of the warrants examined were executed).

2.38 Box 2 shows the six statutory requirements from the Crimes Act which must be stated in all section 3E Crimes Act warrants.

Box 2: *Crimes Act 1914* Subsection 3E(5)

3E(5) If an issuing officer issues a warrant, the officer is to state in the warrant:

- (a) the offence to which the warrant relates; and
- (b) a description of the premises to which the warrant relates or the name or description of the person to whom it relates; and
- (c) the kinds of evidential material that are to be searched for under the warrant; and
- (d) the name of the constable who, unless he or she inserts the name of another constable in the warrant, is to be responsible for executing the warrant; and
- (e) the time at which the warrant expires (see subsection (5A))^a; and
- (f) whether the warrant may be executed at any time or only during particular hours.

Note a: Subsection 3E(5A) states 'The time stated in the warrant under paragraph 3E(5)(e) as the time at which the warrant expires must be a time that is not later than the end of the seventh day after the day on which the warrant is issued.' Put simply, warrants last seven days.

Source: *Crimes Act 1914* Subsection 3E(5).

2.39 The ANAO identified 12 of 272 (4.4 per cent) section 3E Crimes Act warrants which it considered to contain deficiencies or potential non-compliance with legislative requirements. In response to the ANAO's findings, the AFP:

- agreed that two warrants were not executed correctly (see paragraphs 2.49 and 2.54);
- agreed that there was a risk that four warrants could be 'contested at Court'³⁷;
- stated that in its opinion, two warrants only contained administrative errors, which were unintentional and 'that a court may find the warrants to be invalid'; and
- provided additional evidence³⁸ for four warrants to demonstrate compliance with the Crimes Act.

36 Not all warrants that are issued need to be executed. For example, if the AFP is investigating a particular person of interest, three warrants might be obtained: one for the person of interest, one for his or her car and one for his or her place of residence. However, if the AFP arrives at the person's residence and finds that the person of interest and his or her car are located on the premises, the warrant obtained for the residence would cover all three searches. The separate search warrants for the person and car would not be needed.

37 These four warrants did not contain an expiration date. The AFP advised that 'it is likely that a court may find the warrants to be invalid given the failure to comply with legislative requirements. But, there would be reasonable arguments to support the admission of the material under s138 Evidence Act.'

38 These four warrants were signed over to another officer to execute (see paragraph 2.47). On face value, the ANAO considered these sign overs to be inappropriate. However, the AFP provided the police statements for the two officers involved, which confirmed that the sign over was appropriate.

3E(5)(a) The offence to which the warrant relates was stated in the warrant

2.40 Paragraph 3E(5)(a) requires that the offence to which the warrant relates must be stated in the warrant. All 272 Crimes Act warrants assessed by the ANAO included, at a minimum, the section and Act for the offence to which the warrant related.

2.41 Case law states that there is no 'verbal formula' for satisfying paragraph 3E(5)(a) and courts have declined to elaborate on whether certain elements are required under paragraph 3E(5)(a). For example, in *Australian Broadcasting Corporation v Kane (No 2)*, Abraham J stated:

First, the statement of the offence in a search warrant need not be made with the precision of an indictment. The purpose of the statement of the offence is not to define the issues for trial, rather it is to set boundaries to the area of search... Second, the line as to what may, or may not be seized, cannot be precisely drawn as a search warrant is not concerned with what is known, but with what there is reasonable grounds for suspecting... Third, the particularity in an offence description is directed to ensuring that the occupier knows the object of the search and can therefore make an assessment of the material likely to be relevant... Fourth, at the stage a search warrant is granted, it may not be known what particular offences may have been committed and therefore it is sufficient that the warrant specifies the suspected offences in a way so as to enable the executing officer and those assisting to decide if the things seized come within the terms of the warrant... Fifth, the issue of the sufficiency of an offence description should be viewed broadly, having regard to the terms of the warrant in the circumstances of each case. It should be answered in accordance with the principle that a search warrant should disclose the nature of the offence so as to indicate the area of search, with the precision required varying from case to case. It should not be answered by the application of a verbal formula...³⁹

2.42 The AFP Better Practice Guide: *Crimes Act 1914* Search Warrants (BPG on Search Warrants) states:

There should be sufficient detail to show: the date range of offending, identify any victim⁴⁰, identify the offender (or contain a statement to indicate the offender is yet to be identified), identify the section number of the offence and the Act within which the offence is listed.

2.43 The ANAO found that:

- 103 warrants (37.9 per cent) did not list the offender who committed the offence, or the date range to which the offence was committed; and
- 46 warrants (16.9 per cent) did not include the date range to which the offence was committed.

39 *Australian Broadcasting Corporation v Kane (No 2)* [2020] FCA 133 (Federal Court of Australia) paragraph 79.

40 This is where the victim is a natural person. Where the 'victim' is the Commonwealth (such as fraud against the Australian Taxation Office), this is inferred and a victim need not be specified.

2.44 In total, 149 warrants (54.8 per cent) were not prepared consistently with AFP best practice.^{41, 42}

3E(5)(b) A description of the premises to which the warrant relates or the name or description of the person to whom it relates was stated in the warrant

2.45 The AFP must describe the premises, person or conveyance to which the warrant relates. For example, if a car was to be searched, a description and registration number should be provided in the warrant. Ninety-nine per cent of warrants examined by the ANAO had the premises, person or conveyance described appropriately. For the two warrants which did not meet this requirement, the AFP did not consider that this invalidated the warrant, but acknowledged that ‘the lack of descriptors used on the warrant could present a risk to the warrant being challenged at the time of execution or in the future during Court proceedings.’

3E(5)(c) The kinds of evidential material that are to be searched for under the warrant was stated in the warrant

2.46 The nature of the evidential material (drug paraphernalia, for example) that is to be searched for under the warrant must be stated on the warrant. All warrants examined by the ANAO clearly stated the evidentiary material.

3E(5)(d) The name of the constable who is stated on the warrant to be responsible for executing the warrant

2.47 All warrants must nominate a particular constable as the executing officer for the warrant (so that the owner or occupier is aware of who is responsible for the execution of the warrant). If that constable does not intend, or is not able, to be present at the execution of the warrant, he or she may ‘sign over’ the warrant to another constable in a way that makes it very clear that a different officer is to be the executing officer.

2.48 The fact that courts have taken a strict approach to this particular requirement is demonstrated by the case of *R v Alqudsi*⁴³ where the warrant was ruled invalid due to an inadequate sign-over process.⁴⁴

41 In 2020, the AFP conducted an internal audit looking at section 3E Crimes Act warrant compliance with the BPG on Search Warrants. In a sample of 80 warrants, the audit found that 21.3 per cent of warrants did not include the date range to which the offence was committed and 22.3 per cent did not list the offender who committed the offence.

42 The AFP stated that ‘Of the 149 3E Crimes Act warrants cited as not complying with the Better Practice Guide (BPG), 64 warrants were drafted prior to development of the BPG and as such should not be assessed against the BPG’.

43 *R v Alqudsi* [2015] NSWSC 1615.

44 In that case, the officer to whom the warrant was issued passed the warrant to another officer to execute it. The second officer struck out the first officer’s name and added his own as executing officer. The judge held that the warrant was invalid because the first officer did not personally make the amendment.

2.49 In the ANAO's review, there was one clear instance where the warrant was executed by a constable not named on the warrant.⁴⁵ The AFP agreed that the executed warrant 'constitutes a failure to comply with the legislative requirements in s 3E(5)(d).'⁴⁶

2.50 The BPG on Search Warrants states 'the executing officer must 'sign over' the original search warrant by drawing a line through their name and substituting it with the name of the new executing officer.' As discussed in paragraph 3.42 below, when a governance instrument uses the word 'must', compliance is mandatory in the absence of reasonable departure and failure to comply may result in professional standards action. Thirty-seven of the 272 warrants the ANAO reviewed (13.6 per cent) did not meet this requirement.

2.51 During the conduct of this audit, the AFP issued a reminder to officers of the correct sign over practice.

3E(5)(e) The time at which the warrant expires was stated in the warrant

2.52 A section 3E Crimes Act warrant expires no later than the end of the seventh day after the day on which the warrant was issued. All of AFP's section 3E Crimes Act warrants are required to contain the clause:

The time at which this warrant expires is midnight at the end of the seventh day after the day on which the warrant is issued (or lesser period).

2.53 The ANAO found four warrants did not have a completed date of issue — only the day and month were listed, but not the year. Therefore, these four warrants did not have a valid expiry date stated on the warrant. In response to the ANAO's findings, the AFP stated 'that this is an oversight and clerical error, but one that could potentially result in the validity of this warrant to be contested at Court.'

2.54 One of the 207 executed warrants examined by the ANAO (see paragraph 2.37) was executed three days after its expiry and was therefore invalidly executed.⁴⁷ The AFP advised that this failure had been detected by the AFP within a month of the warrant being executed. The AFP provided evidence that showed that the seized property had been returned, a new warrant obtained and executed, and the property lawfully re-seized.

3E(5)(f) Whether the warrant may be executed at any time or only during particular hours was stated in the warrant

2.55 All section 3E Crime Act warrants must state whether the warrant can be executed at any time or only during particular hours. For example, if the warrant is being executed at a place of business, it may state that the warrant can only be executed between 9am and 5pm. All warrants examined met this requirement and were executed within the time stipulated on the warrant.

45 The ANAO referred 19 warrants to the AFP, where it was not clear on face value, who signed the warrant over. The AFP stated that the warrants 'satisfied the legislated requirements of section 3E 5(d) of the *Crimes Act 1914*'.

46 The AFP noted that 'the case officer plans to return the documents and re-seize them' and is currently in 'consultation with CDPP on this matter.'

47 This warrant was executed by another Australian police force.

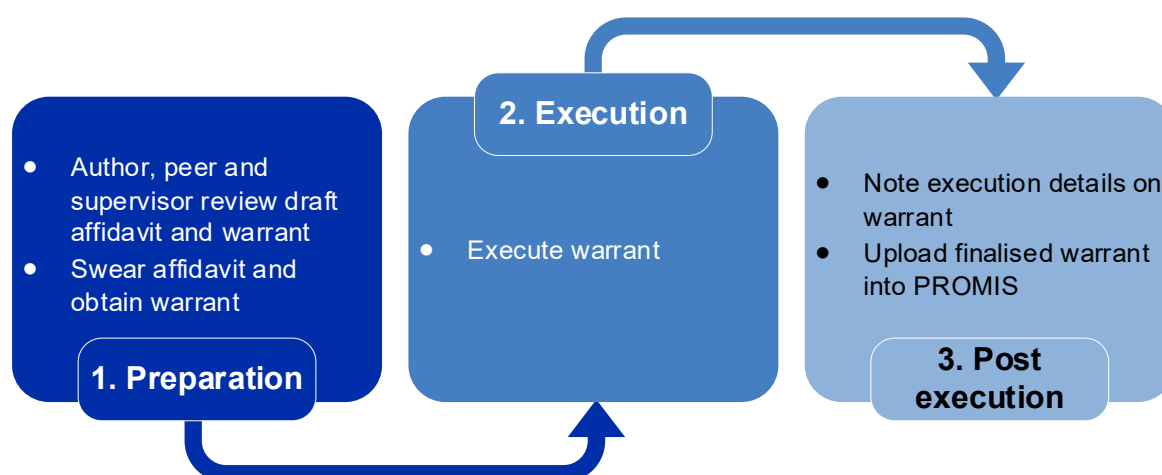
Administrative compliance of search warrants

2.56 In addition to the statutory compliance review, the ANAO assessed the administrative compliance for 83 section 3E Crimes Act warrants (associated with 30 search warrant affidavits).⁴⁸

2.57 Figure 2.2 provides a high level workflow of the administrative processes to prepare and execute a section 3E Crimes Act warrant. For convenience, these have been divided into three distinct phases:

- preparation;
- execution; and
- post execution.

Figure 2.2: AFP's high level process for section 3E Crimes Act warrants



Note: As part of the preparation phase, the AFP is required to complete a tactical planning assessment for any search warrant where there are targets or suspects likely to be present, or where there is a risk to the safety of the police members and community. For example, possible drug labs or where there is a possibility that suspects possess weapons. Due to the relatively small number, the ANAO did not examine this part of the administrative process.

Source: ANAO.

48 Similarly to the statutory compliance review, the ANAO assessed all warrants against AFP internal processes regardless of whether the warrant was executed or not.

Table 2.7: Section 3E Crimes Act warrants which were compliant/consistent with AFP's administrative processes

Phase	Action	Mandatory or non-mandatory	Number compliant/consistent ^a	Per cent compliant/consistent ^c
1. Preparation	Author, peer and supervisor review draft affidavit and warrant	Mandatory	19 (n = 83)	22.9
	Swear affidavit	Mandatory	29 (n = 30) ^b	97.6
	Obtain warrant	Mandatory	81 (n = 83)	96.7
2. Execution	Execute warrant	Non-mandatory	53 (n = 81)	65.4
3. Post execution	Note execution details on warrant	Non-mandatory	69 (n = 81)	85.2
	Upload finalised warrant into PROMIS	Non-mandatory	56 (n = 81)	69.1

Note a: Eighty-three warrants were reviewed. Two applications were refused by the issuing officer (because the issuing officer was not satisfied that there were adequate grounds) and 53 were executed.

Note b: The ANAO selected 30 affidavits to review as part of the administrative compliance. Each warrant must have its own affidavit. However, each affidavit can have multiple warrants.

Note c: 'Compliant' relates to meeting mandatory requirements; 'consistent' relates to meeting non-mandatory requirements.

Source: ANAO analysis based on AFP data.

Preparation

2.58 Once a need for a warrant is identified, the affidavit and warrant/s are drafted. Any officer (including the most junior and inexperienced officers) can prepare an affidavit and draft a section 3E Crimes Act warrant. It is therefore important that such documents be reviewed by a more senior or experienced officer. To this end, the BPG on Search Warrants states that section 3E Crimes Act warrants and affidavits 'must be thoroughly reviewed by the author, peer and supervisor.'⁴⁹

2.59 In 2014, the AFP developed a section 3E Crimes Act warrant checklist⁵⁰ for this purpose, which is available to all officers. The checklist allows officers to demonstrate compliance with the Crimes Act, and that a review has been undertaken. This checklist is not mandatory to use⁵¹ but is a simple way to demonstrate compliance with AFP requirements.

2.60 As shown in Table 2.7, the ANAO reviewed 83 section 3E Crimes Act warrants for compliance with the AFP's administrative processes and sought evidence that the mandatory review had occurred. The ANAO found that:

49 There is no requirement that a review be conducted by the AFP's legal area or that the supervisor have legal qualifications.

50 The AFP refers to this as an adjudication cover sheet.

51 In 2019, the AFP conducted an audit on section 3E search warrants, comparing AFP's practice against its internal guidance. In the ten PROMIS cases reviewed there were two adjudication cover sheets saved on file.

- nineteen warrants had some evidence of review:
 - two warrants had been reviewed by both a peer and supervisor;
 - twelve warrants were reviewed by a supervisor only; and
 - for five warrants, it was unclear whether a peer or supervisor was the reviewer.
- for the remaining 64 warrants, the AFP officers claimed that a review was done but were not able to provide any evidence of this.⁵²

2.61 Two recent High Court cases have underlined the importance of precision when preparing section 3E Crimes Act warrants:

- In *Smethurst & Anor v Commissioner of Police & Anor* [2020], the High Court:

unanimously held that the warrant relied upon by the AFP was invalid on the ground that it misstated the substance of s 79(3) of the Crimes Act, as it stood on 29 April 2018, and failed to state the offence to which the warrant related with sufficient precision. The entry, search and seizure which occurred on 4 June 2019 were therefore unlawful.⁵³
- In *Zhang v The Commissioner of Police & Ors* [2021], the Chief Justice observed:

But one might expect that police, like a prosecuting authority, would take steps, in view of what was said in *Smethurst*, to ensure so far as possible, but in particular in relation to serious matters which are likely to come before this Court, to ensure that warrants are drawn by persons who have legal qualifications, and preferably some prosecutorial background.⁵⁴

2.62 While there may be practical difficulties for the AFP if it were to require that affidavits and warrants be drafted by ‘persons who have legal qualifications, and preferably some prosecutorial background’, the ANAO considers that the present arrangements — where the AFP was unable to provide evidence of mandatory review of warrants in more than three quarters of the warrants examined by the ANAO (see paragraph 2.60) — impose significant risks on the AFP.

52 For example, one supervisor wrote to the ANAO ‘I have always been and remain a very strong advocate of the concept that ‘a man’s home is his castle’ and as a consequence it has been my practice since 1989, when I was promoted, to review/adjudicate all search warrant affidavits and search warrants prepared by members who report to me.’ The same supervisor then went on to say ‘There is no requirement to retain the draft affidavits containing my feedback.’

53 *Smethurst & Anor v Commissioner of Police & Anor* [2020] HCA 14 (High Court of Australia).

54 *Zhang v The Commissioner of Police & Ors* [2021] HCA 16 (High Court of Australia).

Recommendation no. 1

2.63 The Australian Federal Police enforces its requirement that section 3E Crimes Act warrants be thoroughly reviewed by at least a supervisor and retain documentary evidence that the review has occurred.

Australian Federal Police response: *Agreed.*

2.64 *The AFP understands the benefits of an accountable and formal document review process for search warrants. Whilst comfortable that the search warrant review process is being performed operationally and is effective, the value of formal documentation of review and associated accountability is acknowledged. The AFP further notes the corporate systems are being updated to include search warrant work flows including a mandatory review process.*

2.65 Once reviewed, the affidavit is sworn⁵⁵ and if the issuing officer is satisfied, he or she issues the warrant.⁵⁶ All 81 warrants were issued, although the AFP was only able to provide ANAO evidence of 29 of 30 sworn affidavits (see Table 2.7).

2.66 The remaining affidavit was retained by the issuing officer (see definition in Box 1) and not accessible to the AFP at the time of the audit. The affidavit not provided was associated with six warrants in the ANAO's administrative compliance review. The AFP advised that the issuing officer had retained the affidavit and had refused to return it (or a copy of it) without 'an official request ... including official letter head, be sent to him detailing reasons as to why it is being sought.' Consequently, the only copy of the affidavit that the AFP has in its possession is both unsigned and unsworn and there is nothing to demonstrate that it was the same document as was presented to the issuing officer (as opposed to, for example, a draft which was later changed). The ANAO asked the AFP how often this situation arose. The AFP advised that it does not keep such records but provided details of the inconsistent practices of issuing officers around Australia as detailed in Table 2.8.

Table 2.8: AFP commands where affidavits are retained by issuing officers

State (AFP Command)	Is original affidavit retained by issuing officers?
NSW (eastern)	Yes in 90 per cent of cases
VIC (southern)	Yes, but provides a copy when warrant is authorised
QLD (northern)	Yes in 90 per cent of cases
SA (western and central)	Rarely
WA (western and central)	Rarely
Tas (southern)	Not advised by AFP

55 An affidavit is made by oath (sworn) before a Magistrate (or other authorised person) on the Bible — or other religious document — or by affirmation. The investigator places his or her hand on the Bible (or similar) and reads out a statement (which is the oath or pledge).

56 Analysis of the 272 section 3E search warrants reviewed as part of the audit found: 162 were issued by magistrates; 16 by registrars; 13 were issued by justices of the peace (one in NSW and 12 in Queensland); and 29 were issued by 'other persons employed by the court.'

State (AFP Command)	Is original affidavit retained by issuing officers?
NT (northern and western and central)	No
ACT	No

Source: AFP unaudited advice.

2.67 It should be noted that issuing officers are generally not Commonwealth officials and the AFP did not consider that it had the power to require that the signed affidavit (or a copy) be returned to the AFP. While the ANAO acknowledges this difficulty, since affidavits may be required for court proceedings or as supporting evidence for future warrant applications, the ANAO considers that the AFP should have (at the least) a copy of the original sworn document.

Execution

2.68 Fifty-three of the assessed warrants were executed (see Table 2.7). Any property identified as relating to the conditions of the warrant is seized from the premises, person or conveyance.⁵⁷ If the occupier of the premises is present⁵⁸, the executing officer must provide a copy of the search warrant to the occupier at the commencement of the execution of the warrant.⁵⁹

Post execution

2.69 Once a warrant has been executed, the BPG on Search Warrants states that investigators should endorse the front page of the warrant as to whether it was executed or not, and then upload the warrant to PROMIS.⁶⁰ Sixty-nine of 81 warrants (85.1 per cent) had their execution details marked on the front of the warrant. Of these, 56 finalised warrants were uploaded into PROMIS (see Table 2.7).

TIA Act warrants

Statutory compliance of TIA Act warrants

2.70 The ANAO assessed 79 TIA Act warrants for compliance with the TIA Act. The AFP primarily uses sections 46, 46A and 116 of the TIA Act to exercise warrants.⁶¹ As part of the statutory compliance review, the ANAO considered the statutory compliance of 50 warrants issued under section 46, 19 warrants under section 46A, and 10 warrants under section 116 of the TIA Act.

2.71 Compared to section 3E Crimes Act warrants (see paragraph 2.38), there are more statutory requirements for a TIA Act warrant. However, many of these requirements rely on the issuing officer

57 Various circumstances surrounding the execution of a section 3E Crimes Act warrant may result in the AFP exercising additional powers. For example, the person of interest may be arrested. The ANAO did not review any additional powers exercised in concert with the section 3E Crimes Act warrant.

58 When a person is not present, the AFP may undertake a planned or unplanned forced entry. A copy of the warrant is then left within the house for when the occupier returns.

59 This is also a requirement if it is a person or a conveyance being searched.

60 In an audit conducted by the AFP in 2019 on section 3E Crimes Act warrants, the AFP found that information was stored outside of PROMIS, including shared drives. Some of the risks identified with inconsistent PROMIS use included 'loss of productivity and inefficiencies,' 'time delays in progressing investigations' and 'judicial scrutiny over a lack of records.'

61 Section 46 relates to interception of communication to or from a particular service, while section 46A relates to any or all services used by a person named in the warrant. Section 116 of the TIA Act relates to stored communication warrants.

(an eligible Judge or nominated Administrative Appeals Tribunal member) being satisfied that the TIA Act warrant is the appropriate course of action.⁶² As a result, the ANAO assessed only those aspects of the TIA Act which could be assessed objectively, and did not examine the individual issuing officer's assessment. Table 2.9 outlines the tests the ANAO applied in this analysis, and for which warrant type each test was applicable.

Table 2.9: ANAO tests for TIA Act warrant statutory compliance review

Test	Applicable warrant type
Was the warrant valid for greater than 90 days?	section 46, section 46A
Was a particular person specified on the warrant?	section 46, section 46A
Was a telecommunications number identified?	section 46
Was the issuing officer eligible to issue warrant?	section 46, section 46A, section 116
Was the (short) offence detailed in the warrant?	section 46, section 46A, section 116
Was the warrant in the prescribed form?	section 46, section 46A, section 116
Were there any obvious errors on the warrant?	section 46, section 46A, section 116
Was the warrant valid?	section 46, section 46A, section 116

Source: ANAO based on TIA Act.

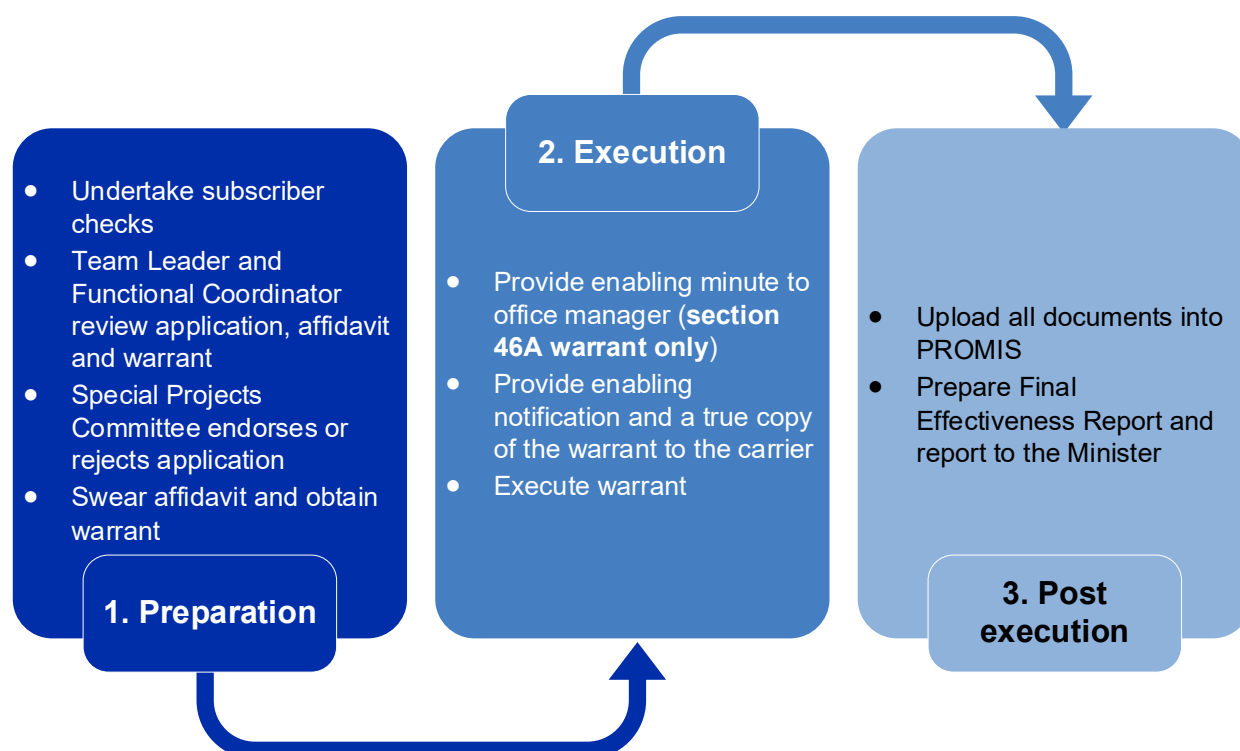
2.72 The ANAO found that all 79 TIA Act warrants reviewed were compliant with the statutory requirements listed above.

Administrative compliance of TIA Act warrants

2.73 Figure 2.3 provides a high level workflow diagram for the preparation and execution of sections 46 and 46A warrants. For convenience, these have been divided into three distinct phases:

- preparation;
- execution; and
- post execution.

62 For example, the eligible judge or nominated Administrative Appeals Tribunal member needs to be satisfied that 'there are reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service' and 'information that would be likely to be obtained by intercepting under a warrant ... would be likely to assist in connection with the investigation by the agency of a serious offence, or serious offences, in which the person is involved.'

Figure 2.3: AFP's high level process for sections 46 and 46A TIA Act warrants

Source: ANAO from AFP *Better Practice Guide: Telecommunications Interception and Access Act 1979*.

Table 2.10: Sections 46 and 46A TIA Act warrants which were compliant/consistent with AFP's administrative processes

Phase	Action	Mandatory or non-mandatory	Number compliant/consistent	Per cent compliant/consistent ^b
1. Preparation	Undertake subscriber checks	Non-mandatory	12 (n = 24)	50.0
	Team Leader and Functional Coordinator review application, affidavit and warrant	Non-mandatory	24 (n = 24)	100.0
	Special Projects Committee endorses or rejects application	Mandatory	24 (n = 24)	100.0
	Swear affidavit	Mandatory	11 ^a (n = 11)	100.0
	Obtain warrant	Mandatory	24 (n = 24)	100.0
2. Execution	Provide enabling minute to office manager (section 46A warrant only)	Mandatory	10 (n = 10)	100.0
	Provide enabling notification and a true copy of the warrant to the carrier	Mandatory	24 (n = 24)	100.0

Phase	Action	Mandatory or non-mandatory	Number compliant/consistent	Per cent compliant/consistent ^b
	Execute warrant	Non-mandatory	24 (n = 24)	100.0
3. Post execution	Upload all documents into PROMIS	Mandatory	0 (n = 24)	0.0
	Prepare Final Effectiveness Report and report to the Minister	Mandatory	24 (n = 24)	100.0

Note a: An affidavit can contain both TIA Act and SD Act warrants. The ANAO selected 20 affidavits for its administrative review, which contained at least one TIA Act or SD Act warrant.

Note b: 'Compliant' relates to meeting mandatory requirements; 'consistent' relates to meeting non-mandatory requirements.

Source: ANAO's analysis based on AFP data.

Preparation

2.74 Once a need for a TIA Act warrant has been identified, the Better Practice Guide: *Telecommunications Interception and Access Act 1979* (BPG on TIA Act warrants) outlines that subscriber checks⁶³ should be undertaken on the person of interest to identify any service/s subject to the warrant application. Twelve of the 24 warrants had their associated subscriber checks on file (see Table 2.10).

2.75 The BPG on TIA Act warrants states that all documentation should be reviewed by an appropriate Team Leader and Functional Coordinator. This review is not compulsory and its outcome is not retained on the hard copy file. However, when the Special Projects Committee (SPC)⁶⁴ convenes to endorse the warrant, the documentation is reviewed. The ANAO considered this to be an appropriate review point. All warrants were reviewed by the SPC (see Table 2.10).

2.76 The SPC convenes to reject or endorse the application for a TIA Act warrant. The approval decision was clearly documented for all warrants (see Table 2.10). If the warrant is rejected, the reason should be provided.⁶⁵

2.77 Once a TIA Act warrant is endorsed, the affidavit is submitted to the issuing officer (see Box 1) who issues the warrant if he or she is satisfied that a warrant is the appropriate course of action. All 11 affidavits examined were sworn, and all warrants issued (see Table 2.10).

63 A subscriber check is not required if the telecommunications details have been already obtained by the AFP as part of an investigation.

64 The SPC is comprised of the relevant Special Projects Registrar, two Coordinators or a Manager. The Investigator may also be required to attend.

65 In 2019–20, 636 of 638 (99.7 per cent) TIA Act warrants applied for were issued.

Execution

2.78 For section 46A TIA Act warrants, the BPG on TIA Act warrants requires AFP officers to prepare and provide an enabling minute to the relevant AFP office manager. This process was completed for all 10 section 46A TIA Act warrants.⁶⁶

2.79 The AFP is required to provide an enabling notification and a true copy of the TIA Act warrant to the carrier. This was undertaken for all 24 warrants reviewed (see Table 2.10).⁶⁷

2.80 The telecommunications interception commences once the carrier is notified of the warrant. Sections 46 and 46A TIA Act warrants have a maximum duration of 90 days. When the carrier sets up the collection profile, the expiry date is entered into the carrier's system which will automatically cut off at 23:59 on the date of expiry. All 24 warrants were executed (see Table 2.10).

Post execution

2.81 The BPG on TIA Act warrants states that the investigator 'must immediately upload all⁶⁸ documents, including affidavit and warrant' into PROMIS when all associated documents are finalised. It is unclear what 'all documents' refers to, but the ANAO reviewed documents referenced in the BPG on TIA Act warrants, including, for example, the capacity request form⁶⁹ and notification to the carrier. The ANAO found:

- none of the warrants reviewed had all of the relevant documentation uploaded into PROMIS (see Table 2.10);
- nine of the 24 (37.5 per cent) TIA Act warrants had both the warrant and affidavit uploaded into PROMIS⁷⁰; and
- four TIA Act warrants had the warrant uploaded onto PROMIS, but not the affidavit.

2.82 Once the warrant expires, a Final Effectiveness Report must be prepared. Where a warrant was not executed, a reason as to why must be included. The AFP must report the information captured in the Final Effectiveness Report⁷¹ to the responsible Minister within three months of the TIA Act warrant ceasing to be in force. This was completed for all 24 warrants (see Table 2.10 and paragraph 2.22).

66 Due to a named person warrant possibly involving the interception of multiple communication devices, across multiple carriers, the ANAO considered compliance when at least one notification to the carrier was completed.

67 A carrier is an Australian telecommunications carriage service provider and internet service provider as defined in the *Telecommunications Act 1997*.

68 While the BPG on TIA Act warrants does not define 'all relevant documents', on 24 March 2021, the AFP advised that it intended to include 'all documents required by the relevant legislation such as the warrant/s, affidavits and applications only. The case officer or responsible investigator is responsible for loading the documents onto PROMIS.' The AFP advised it will update guidance material appropriately.

69 The capacity request form is an internal document AFP officers are required to submit prior to obtaining a TIA Act warrant.

70 The ANAO only looked at the PROMIS cases provided by the AFP for each of these warrants. The ANAO did not review whether the warrant and/or affidavit were uploaded onto a different PROMIS case.

71 The Final Effectiveness Report includes information such as the services that were intercepted, who the information captured through the warrant was communicated to, and whether any arrests were made.

SD Act warrants

Statutory compliance of SD Act warrants

2.83 The ANAO assessed 68 SD Act warrants for compliance with the SD Act. The AFP primarily uses section 16 of the SD Act to execute warrants.⁷² However, as part of the statutory compliance review the ANAO considered the statutory compliance of warrants exercised under sections 16, 24⁷³ and 27C⁷⁴ of the SD Act.

2.84 As for TIA Act warrants, SD Act warrants rely on the issuing officer being satisfied that an SD Act warrant is appropriate (see paragraph 2.71). As a result, the ANAO assessed each SD Act warrant only against those aspects of the SD Act which could be assessed objectively, and did not examine the appropriateness of the issuing officer's decision. Table 2.11 lists the tests the ANAO applied in this analysis for each warrant assessed.

Table 2.11: ANAO tests for SD warrant statutory compliance review

Test
Was a particular person specified on the warrant?
Were the surveillance device/s intended to be used listed on the warrant?
Was the issuing officer eligible to issue the warrant?
Does the warrant state that the issuing officer is satisfied and had grounds to issue the warrant?
Is the applicant named on the warrant?
Was the offence detailed on the warrant?
Was a premises, vehicle type or object subject to surveillance listed on the warrant?
Was the warrant too general?
Were there any obvious errors on the warrant?
Was the warrant valid?

Source: ANAO's analysis based on AFP data.

2.85 The ANAO found that all 68 SD Act warrants reviewed were compliant with the statutory requirements listed above.

Administrative compliance of SD warrants

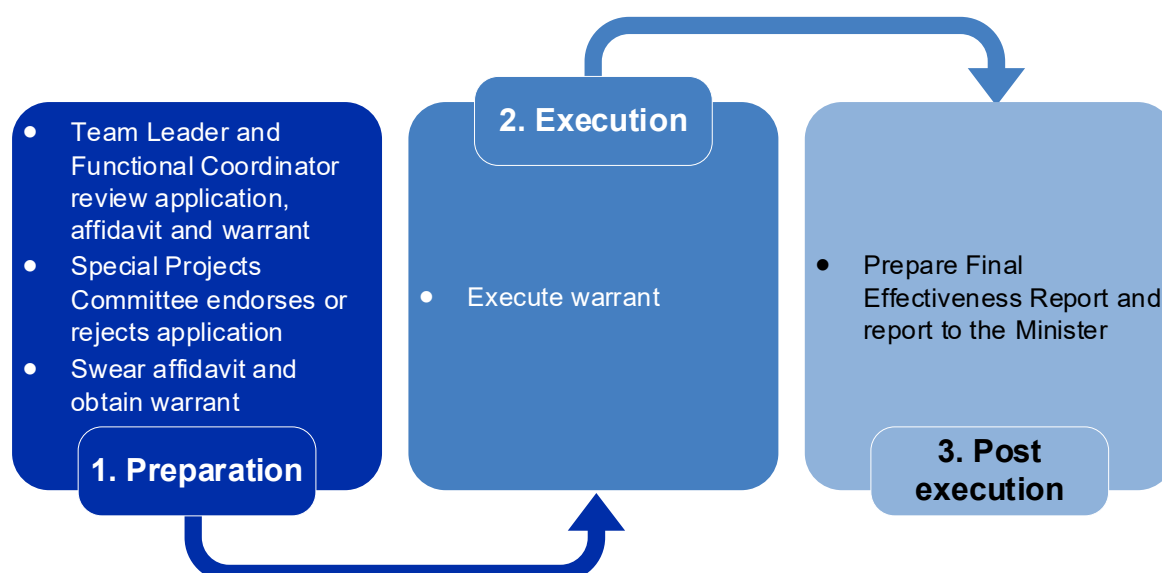
2.86 Figure 2.4 provides a high level workflow diagram to prepare and execute section 16 SD Act warrants. For convenience, these have been divided into three distinct phases:

- preparation;
- execution; and
- post execution.

72 A surveillance device means a data surveillance device, a listening device, an optical surveillance device or a tracking device, or a device that is a combination of any two or more of the devices.

73 Section 24 of the SD Act is for a Retrieval Warrant.

74 Section 27C of the SD Act is for a Computer Access Warrant.

Figure 2.4: AFP's high level process for section 16 SD Act warrants

Note: The SD Act warrant administrative process is broadly similar to the TIA Act warrant administrative process (see Figure 2.3). The main difference between the two is that the AFP is dealing with a third party as part of the TIA Act warrant process — the carrier — who activates the intercept. By comparison, for SD Act warrants, it is the AFP who installs the surveillance device(s) as part of the execution phase of the SD Act warrant process.

Source: ANAO from AFP *Better Practice Guide: Surveillance Devices*.

Table 2.12: Section 16 SD Act warrants which were compliant/consistent with AFP's administrative processes

Phase	Action	Mandatory or non-mandatory	Number compliant/consistent	Per cent compliant/consistent ^b
1. Preparation	Team Leader and Functional Coordinator review application, affidavit and warrant	Non-mandatory	47 (n = 47)	100.0
	Special Projects Committee endorses or rejects application	Mandatory	47 (n = 47)	100.0
	Swear affidavit	Mandatory	13 ^a (n = 13)	100.0
	Obtain warrant	Mandatory	47 (n = 47)	100.0
2. Execution	Execute warrant	Non-mandatory	21 (n = 47)	44.7
3. Post execution	Prepare Final Effectiveness Report and report to the Minister	Mandatory	47 (n = 47)	100.0

Note a: An affidavit can contain both TIA Act and SD Act warrants. The ANAO selected 20 affidavits for its administrative review, which contained at least one TIA Act or SD Act warrant.

Note b: 'Compliant' relates to meeting mandatory requirements; 'consistent' relates to meeting non-mandatory requirements.

Source: ANAO's analysis based on AFP data.

Preparation

2.87 With the exception of subscriber checks, SD Act warrants follow the same administrative process as TIA Act warrants in the preparation phase (see paragraphs 2.74 to 2.77). Table 2.12 shows the number of SD Act warrants which met each of these steps.⁷⁵

Execution

2.88 The surveillance associated with an SD Act warrant commences when the surveillance device/s is installed and activated. SD Act warrants have a maximum duration of 90 days but can be extended.⁷⁶ Nineteen of 47 (40.4 per cent) SD Act warrants examined by the ANAO were extended.⁷⁷ Devices installed should be removed prior to the expiration of the warrant.⁷⁸

2.89 When an SD Act warrant is issued for a person (rather than a specific location), devices can be installed across multiple locations. The ANAO's analysis considered a hard copy file was compliant when there was a record of at least one device used. Twenty one SD Act warrants were executed (see Table 2.12).

Post execution

2.90 Once the warrant expires, a Final Effectiveness Report must be prepared. Where a warrant was not executed, a reason must be included. The SD Act requires the AFP to report the information captured in the Final Effectiveness Report to the responsible Minister as soon as practicable after the warrant ceases to be in force for SD warrants. This was completed for all SD Act warrants (see Table 2.12).

The AFP's record keeping practices and processes

2.91 As noted at paragraph 1.16 and throughout this chapter, deficiencies in the AFP's record keeping processes and practices became apparent during the fieldwork phase. Key documents (such as applications, affidavits and warrants) are kept by the AFP in a variety of locations. More significantly, the ANAO considers that the AFP's poor record keeping practices and processes are a risk to the integrity of the AFP's operations. Consequently, the ANAO broadened the scope of the audit to include record keeping (see Appendix 3).

75 In 2019–20, 620 of 628 (98.7 per cent) SD Act warrants applied for were issued.

76 Unlike TIA Act warrants, SD Act warrants may be extended (more than once if necessary) but the extension must be approved by the issuing officer before the original warrant expires.

77 All extension applications were made prior to the warrant expiring.

78 The ANAO did not review whether surveillance devices were removed, because the Commonwealth Ombudsman examines this as part of his inspection regime.

Recommendation no. 2

2.92 As a matter of urgency, the Australian Federal Police should implement an Electronic Data and Records Management System (EDRMS) to allow it to store records so that they are secure and readily accessible. It should cease its reliance on network drives.

Australian Federal Police response: *Agreed.*

2.93 *The AFP is developing a digital transition roadmap which includes an initiative to market-test suitable digital records management capabilities that will inlay with our operating and technology environment. This work will identify potential solutions and enable the AFP to modernise, strengthen and streamline records management.*

3. Training and guidance

Area examined

The ANAO examined whether Australian Federal Police (AFP) officers have adequate knowledge of their powers and how to use them.

Conclusion

The AFP's framework relating to training and guidance is largely effective. However, it has not undertaken a training needs analysis at the whole-of-organisation level and there is limited quality assurance assessment of operational activity.

Area for improvement

The ANAO has recommended that the AFP develop a quality assurance framework.

Does the AFP provide adequate training to all officers who will be exercising powers under applicable legislation?

The AFP provides appropriate training for external recruits and offers continuing training opportunities to its ongoing staff. The AFP is accredited as a Registered Training Organisation and is able to provide nationally-recognised qualifications.

3.1 As noted in paragraph 1.9, the ANAO identified 86 Commonwealth Acts which potentially confer more than 800 separate powers upon AFP officers. It is important that officials who may exercise intrusive powers have been properly trained in their use. In this section, the ANAO considered whether the AFP provides adequate training to all officers who may exercise powers under applicable legislation.

3.2 Learning Command, which is headed by the Chief Learning Officer (CLO) (an SES Band 2 officer) is split across two SES Band 1 officers as shown in Figure 3.1.⁷⁹ The Learning Command's 2020–21 budget is \$48.7 million which represents about 3.1 per cent of the AFP's total budget.

⁷⁹ The Learning Command was created in 2020 as part of the new Commissioner's organisational reforms. It was previously known as Learning and Development and was headed by one SES Band 1 officer.

Figure 3.1: Enterprise Learning and Performance

Source: AFP.

3.3 The AFP has a Learning Strategy which articulates seven 'learning principles' as shown in Figure 3.2.

Figure 3.2: The AFP's Learning Principles

Source: AFP.

3.4 To embed these learning principles, the AFP uses a '70:20:10' model in which:

- 70 per cent of learning is informal 'on the job' and experience based;
- 20 per cent is coaching, mentoring, developing through others; and
- 10 per cent is formal learning interventions and structured courses.

Registered Training Organisation certification

3.5 The AFP College is a Registered Training Organisation (RTO) and attained its RTO status in 1994, which enables it to offer nationally-recognised qualifications.⁸⁰ Currently, these qualifications are:

- Certificate IV in Protective Services;
- Certificate IV in Government Investigations;
- Diploma of Police Intelligence Practice;
- Diploma of Policing;
- Diploma of Police Search and Rescue Coordination (Marine/Land);
- Advanced Diploma of Surveillance;
- Advanced Diploma of Police Close Personal Protection; and
- Advanced Diploma of Police Investigation.

3.6 RTO certification is provided by the Australian Skills Quality Authority (ASQA), the Australian Government regulator for Australia's vocational education and training (VET) sector. In 2016, the AFP engaged a consultant to conduct an audit of two qualifications⁸¹ to ensure compliance with the *Standards for Registered Training Organisations 2015*. The audit report found that the AFP did not meet six of the eight RTO standards assessed and identified 19 'rectifications' required. In relation to the report, the AFP advised:

The implementation of recommended corrective actions produced by the independent consultant is not a mandatory requirement for the AFP, however out of the recommendations 78% were addressed. Of the remaining 22%, 12% were deemed not applicable and 10% were not agreed to.⁸²

3.7 More recently, an RTO assurance and validation plan for 2020–21 has been implemented to ensure that the RTO qualifications provided by the AFP comply and meet the needs of the recruits and other members undertaking training. The audit and validation schedule was scheduled to begin in March 2021, with targeted desktop reviews.⁸³

80 Training is provided by instructors comprising of sworn, unsworn and specialist members who hold a Certificate IV in Training and Assessment.

81 The Diploma of Public Safety (Police Search and Rescue – Coordination) and the Advanced Diploma of Police Close Personal Protection.

82 The AFP also advised 'The AFP have not had an audit undertaken by ASQA on our Registered Training Organisation. ASQA have implemented a risk-based approach to regulation in order to reduce the burden for high-performing providers and focus regulatory attention on those providers considered higher risk. AFP has been considered low risk by ASQA and as such the approach has been to focus on self-assurance and excellence in training outcomes. A component of this is regular internal reviews and the rectification of any identified compliance issues. It has been confirmed that ASQA have not conducted any further assessments for any of the AFP qualifications since 2016'.

83 The AFP advised that the schedule informally commenced in November 2020 with the POL58115 Diploma of Police Search and Rescue Coordination (Marine/Land) and formal validation of this qualification commenced in March 2021. Validation of POL62415 Advanced Diploma of Surveillance commenced in April 2021.

Recruit training

3.8 The AFP has provided training at the AFP College to recruits since its inception in 1979. The AFP College is located in Canberra and recruits reside at the AFP College during the training phase.

3.9 There are three avenues by which external applicants can enter the AFP as a sworn officer or Protective Service Officer (PSO) (see paragraph 1.6):

- the Federal Police Development Program;
- the Federal Police Lateral Program (for existing state and territory police officers seeking to join the AFP); and
- the Protective Service Officer Program.⁸⁴

3.10 Details of each of recruitment program are shown in Table 3.1.

Table 3.1: AFP recruitment programs for external applicants

Name	Open to	Details
Federal Police Development Program	External applicants	A 24 week live-in course comprising law; evidence; procedure; investigations techniques; police powers; the intelligence process; defensive skills; firearms; and driver training.
Federal Police Lateral Program	External applicants with minimum three years' state or territory policing experience	A six to seven week course specifically designed for people with current policing experience from state or territory jurisdictions. The course focus is to assist recruits to adapt existing knowledge of state/territory legislation to the legislative framework used by the AFP.
Protective Service Officer Program	External applicants	A 14 week course comprising theoretical (the law and role of a PSO) and practical components (firearms training, defensive tactics (batons/handcuffs), crowd control (batons/shields), and team building exercises). All components are assessable and essential qualifications maintained.

Note: All external applicants must: be Australian citizens; be over 18; hold a valid driver's licence; have minimum Year 10 certificate; complete an Employment Suitability Questionnaire; meet minimum health and medical standards; undergo illicit drug testing and be able to obtain a security clearance.

Source: AFP.

3.11 The curriculum for the programs above is designed on a modular basis, with the number of modules (and subjects within them and lessons within subjects) required dependent on the program. The current modules are shown in Table 3.2. More detail is provided at Appendix 4.

⁸⁴ There is also a Federal Police Transition Program for existing PSOs wishing to transition to a full policing role. This course aligns with the Federal Police Development Program, with candidates having to successfully complete the workbook to attain the Diploma of Policing (as outlined in paragraph 3.13).

Table 3.2: AFP programs — modules

Module	Name	Number of subjects	Number of lessons
1	Pre-Residential	2	2
2	Organisational Policy, Culture & Ethics	8	34
3	Police Practice & Procedures	9	60
4	Initial Investigations	7	39
5	Judicial Process	3	5
6	Health & Operational Safety	12	65
7	Workplace Training Phase	8	8
Total		49	213

Source: AFP.

3.12 Of the 213 lessons referred to in Table 3.2, the ANAO identified 24 that are relevant to officers' understanding of the principles and practice of the exercise of AFP statutory powers. These are listed in Table 3.3.

Table 3.3: Examples of training subjects relevant to use of statutory powers

Subject examples		
Human rights	Burden & Standard of Proof	Entry powers
Cultural Awareness	Suspicion vs Belief	Police Powers and Part 1C of the <i>Crimes Act 1914</i>
Criminal law in Australia	Court Procedures	Briefs of Evidence
Evidence Law	Statement of Facts	Search warrants and affidavits
Jurisdiction	Arrest & Caution	Search warrant application
Proving an offence	Search (Arrested Person)	Search Warrant Execution
Court proceedings	Hearsay	Controlled operations
Categories of offences	Fairness	Introduction to legal research

Source: AFP.

3.13 Following successful completion of the Federal Police Development Program, graduates are declared as sworn members of the AFP and enter the AFP workforce.⁸⁵ To attain the Diploma of Policing, sworn members maintain and complete a workbook and collect workplace evidence to satisfy that assessment requirements have been met. Workbooks (along with workplace evidence) are assessed and submitted to the Team Leader and saved into PROMIS.

3.14 Upon being assessed as competent, the sworn member is awarded a Diploma of Policing, which is a nationally recognised qualification.

⁸⁵ Successful graduates are known as probationary Constables of Police, have police powers and may be deployed to locations in ACT policing or around Australia.

Continuing training

3.15 The AFP is presently developing an AFP Career Framework aimed at highlighting the various career opportunities available to both sworn and unsworn staff. The Framework consists of 17 job ‘families’, each with a number of occupational groups and job roles. The 17 job ‘families’ are shown in Table 3.4.

Table 3.4: AFP job families

Job families	
Administrative & Operations Support	Human Resources
Communications	Information & Communications Technology
Community Policing	Intelligence
Covert Services	Planning, projects and improvements
Compliance, Regulation & Legal	Technical & Surveillance Capability
Education, Training & Development	Investigations
Finance & Commercial	Protective Security
Forensic	Specialist Response
Health	

Source: AFP.

3.16 In total, the Career Framework contains 47 occupational groups and 180 job roles. The AFP advised that the overall anticipated benefits of the Career Framework are:

- employees can clearly see the expectations around the skills required and the potential development path within that role, as well as enabling them to better plan out and own their own career; and
- supervisors can use the profiles to better attract and select the right people, support performance management and development discussions and provide insight into the competency requirements of a team, now and into the future.

3.17 The AFP expects that the Career Framework will be fully implemented by October 2021.

Online training

3.18 The AFP also uses electronic learning (eLearning) as part of its delivery of training programs.⁸⁶ There are three main platforms which are shown at Table 3.5.

⁸⁶ Design, development, implementation and maintenance of eLearning is managed by Command Technology Enhanced Learning Team in partnership with various subject matter experts and business areas.

Table 3.5: eLearning platforms

Online platform	Description
iAspire — online learning environment	Online training accessible to all AFP staff for a diverse range of training packages. This platform is used for both mandatory and non-mandatory training.
Moodle — virtual learning environment	An eLearning platform that is used by a range of course participants, including AFP Recruits at the AFP College.
Avalanche — immersive simulated environment	This platform is an Immersive Simulation Environment (real life scenarios) system that allows participants to experience real-world scenarios and demonstrate/practice the decision making process. Instructors are able to observe and assess participants in real time. Avalanche has six scenarios with more in development.

Source: ANAO analysis of AFP documentation.

Does the AFP undertake analysis of training needs and/or requirements to ensure the lawful exercise of powers by its officers?

The AFP has not undertaken a training needs analysis at the whole-of-organisation level, although there was evidence of limited analysis undertaken focussed on Operational Safety Assessment training and recruit induction training.

3.19 The purpose of an analysis of training needs is to identify whether there is a gap between the training that an entity delivers and the skills and knowledge that staff need to do their jobs. In this section, the ANAO identified two examples of training needs analyses relevant to the lawful exercise of powers by its officers, although they were both somewhat dated.

Operational Safety Assessment

3.20 As noted at paragraph 3.34 below, operational safety training (OST) (including the use of force) is a key part of recruit training and sworn officers are required to undergo operational safety assessment (OSA) every year thereafter.

3.21 In October 2016, an internal training needs analysis of OSA was conducted which made six recommendations around: inclusion of additional skills⁸⁷; restructuring of OSA; and training staffing and resourcing. In March 2021, the AFP advised that the recommendations from the original report were accepted and work was undertaken to implement the changes but commented that ‘as this report is five years old now much of the initial work has changed due to ongoing review and continuous improvement.’

Recruit Transformation Taskforce

3.22 In October 2017, a Recruit Transformation Taskforce (RTT) was created with the intent to ‘Design a contemporary law enforcement recruit and induction training framework incorporating flexibility, innovation and content that supports the evolving and emerging needs of law enforcement’. The RTT’s draft report made 11 recommendations aimed at addressing ‘the

87 These were Cover and movement; Moving as an operational pair; Crossing open ground; Situational firearm capability; Post incident management; Situational awareness and critical incident response.

requirement to adopt a new approach and enhanced structure, as well as gaining a thorough understanding of the necessary competencies to inform curriculum requirements.’ A March 2019 Executive Board paper noted that the project had been completed and that ‘recommendations are currently being costed’ but that ‘Implementation is dependent upon a major commitment from People Strategies (Recruitment) and the workplace in changing how we recruit and integrate recruits pre and post foundation training.’ The AFP advised in March 2021 that the draft report was not finalised and ‘the recommendations were never formally endorsed by the Senior Executive’.

Does the AFP obtain assurance that officers adequately understand their powers?

The AFP does not have an organisation-wide quality assurance framework. Although the Investigations Standards and Practices area has undertaken some operational review activity, this has been limited since its establishment in 2014.

3.23 AFP sworn officers are able to exercise a wide range of powers, many of them intrusive in character, under 86 Commonwealth Acts. In such a complex operational environment, it is important that the AFP obtains assurance that the officers exercising these powers understand them.

3.24 The main recruitment programs referred to in Table 3.1 include a variety of assessment methods including: questioning, observation, third party reports, interviews, simulations, written tests and portfolios of evidence. Recruits are required to demonstrate that they meet the assessment standards before being formally sworn in. The AFP is therefore able to demonstrate reasonable assurance that recruits have an adequate understanding of their statutory powers at the time that they graduate.

3.25 The ANAO examined the adequacy of routine review processes in the context of its assessment of a sample of warrants (see paragraphs 2.24 to 2.90).

3.26 The AFP does not have a documented quality assurance framework. In April 2014, the AFP established Investigations Standards and Practices (ISP) which is described as follows:

Investigations Standards and Practices (ISP) is a professional practice body promoting consistency, standards and quality in a support of investigations across the organisation. ISP is owned and led by investigators for investigators and drives the development and implementation of best practice through the frontline delivery of Regional Investigations Advisers (RIAs).

3.27 In 2018, an audit function⁸⁸ was established within ISP. It has conducted four audits:

- Search Warrant audit (November 2019);
- Covert and Capability resource allocation (November 2019);
- Senior Investigating Officer (April 2020); and
- Search Warrant (Third Condition) Audit (December 2020).

88 These reports did not refer to any standards to which the audit was conducted.

3.28 The first of these (Search Warrant) exhibited some quality assurance characteristics in that it was sample-based, compared selected warrants against statutory and AFP internal administrative requirements and made recommendations for improvement.

3.29 In the light of the ANAO's findings in its examination of warrants (including failures to follow procedures contained in internal guidance material and inconsistent filing of key warrant documentation), the ANAO considers that the AFP should consider establishing a routine and systematic quality assurance process over warrant application processes, warrant execution and documentation. Such a process could be based on a random selection of warrants sought and executed.

Recommendation no. 3

3.30 The Australian Federal Police implement a systematic quality assurance process for its section 3E Crimes Act warrant application, execution and documentation.

Australian Federal Police response: *Agreed.*

3.31 *The AFP acknowledges the need for a more robust and consistent quality assurance process for investigations. Drawing upon existing mechanisms including investigative standards and practice oversight, the AFP will review training, governance and corporate systems to reinforce accountability mechanisms and ensure ongoing statutory compliance.*

Are adequate records maintained in relation to the training of AFP officers?

The AFP maintains records of officers' completion of mandatory training requirements and monitors their completion. In terms of Operational Safety Assessment, the AFP's records demonstrate improvement since the ANAO's previous examination in Auditor-General Report No. 30 2015–16 *Management of the Use of Force Regime*.

3.32 As noted below, an integral part of recruit training is OST and OSA (see paragraph 3.34) which includes use of force and weapons training. Sworn officers are required to be assessed and recertified annually. In addition to OSA, there are a number of other mandatory courses which both sworn and unsworn staff are required to complete as shown in Table 3.6.

Table 3.6: Mandatory courses

Course	Audience	Requirement
Armed Intruder Emergency Procedures	All staff	Every two years
AFP Security Awareness	All staff	Yearly
AFP Work Health and Safety	All staff	Every two years
Australian Privacy Principles	All staff	Yearly
Controlled Operations	Sworn staff	Once only
CRM: Introduction to <i>Public Governance Performance and Accountability Act 2014</i>	All staff	Once only

Course	Audience	Requirement
Fraud Control and Anti-Corruption Awareness	All staff	Every three years
Human Source Awareness	Sworn staff	Yearly
Information Management Level 1	All staff	Every two years
Introduction to Professional Standards	All new staff	Once only
Official Online Activities (Tectus)	All staff	Once only
Operational Safety Training and Assessment	Sworn staff	Required for recertification
Performance Development Agreement	All new staff	Once only
Workplace Bullying	All staff	Once only

Source: AFP.

3.33 Both mandatory courses and OSA require a process in order to monitor compliance and ensure that requirements have been met. The AFP uses SAS Firefly (a proprietary visual analytics tool) to capture data from SAP⁸⁹ to monitor individuals' status for mandatory courses (including OSA). Notifications are able to be sent from SAP as an automated email notification at nominated durations before the expiry of mandatory qualifications and it is incumbent on officers to complete the necessary action to maintain qualification. For example, for OSA recertification, officers are required to complete an online test and then book themselves in for a three day assessment process (including a practical test of marksmanship at a shooting range). Supervisors also receive copies of email notifications and are expected to monitor the compliance of their staff.

Operational safety training recording

3.34 Police officers can be exposed to dangerous situations, requiring them to have the necessary training to deal with a wide variety of situations and people. For this reason, the AFP places particular emphasis on OST as part of initial recruit training. OST includes an emphasis on negotiation and de-escalation techniques, with non-lethal or lethal force to be used as a last resort.⁹⁰

3.35 Under the Commissioner's Order on Operational Safety (CO3), sworn officers are required to complete an OSA every year throughout their career. There are two components to the OSA:

- knowledge assessment, which is completed via the AFP's online learning management system, iAspire (this component must be successfully completed first); and
- a practical assessment, which includes firearms, defensive tactics, holsters, light sources, holistic scenarios and skills maintenance.

89 SAP is the AFP's Human Resource Management Information System.

90 Standard operational equipment issued to operational officers includes a Glock 19 19mm 15 round pistol, an expandable baton, a conducted energy weapon (Taser) and oleoresin capsicum (OC) spray. Officers also carry handcuffs and a radio.

3.36 Officers who do not complete the OSA within 60 days of it falling due or who do not pass are required to surrender all 'controlled'⁹¹ items.⁹²

3.37 The ANAO examined the AFP's use of force management in Auditor-General Report No.30 2015–16 *Management of the Use of Force Regime*.⁹³ That report found that 'AFP records indicated that of 3502 sworn officers, 250 (7.1 per cent) had been issued or retained firearms without holding a current OSA'. This audit reviewed and re-audited the AFP's records to assess whether there had been an improvement in compliance with the Commissioner's Order on Operational Safety.

3.38 Based on the AFP's data, the ANAO's review found that at 3 March 2021:

- the AFP had 4043 firearms⁹⁴; and
- 36 of 3356 sworn officers (1.1 per cent) had been issued a firearm, but did not have a current OSA qualification.⁹⁵

3.39 This is a significant improvement from the ANAO's findings in 2015–16.

Do officers have access to accurate and up-to-date guidance materials to assist with their exercise of powers?

The AFP maintains a suite of guidance and directions for staff through its Governance Instrument Framework which is readily accessible through the Hub. Although approximately half the instruments were overdue (or possibly overdue) for review at the time of audit, the AFP is presently reviewing the framework.

3.40 As Appendix 2 demonstrates, AFP officers are able to exercise powers under a wide range of Commonwealth Acts. As noted above, officers are provided with training when they are recruited, and ongoing training during their careers. A necessary part of the statutory powers framework is the provision of a suite of guidance material that officers may consult when necessary. The AFP maintains an extensive Governance Instrument Framework (GIF) which is intended not only to provide guidance but also directions and instructions. Details of the GIF are shown in Table 3.7.

91 Controlled items includes firearms (including ammunition and accessories), conducted energy weapons, operational accoutrements (ballistic vests, helmets, shields, batons, handcuffs), oleoresin capsicum (OC) spray and radios.

92 Officers who have their OSA qualification revoked for health or management reasons are also required to surrender all controlled items.

93 Auditor-General Report No.30 2015–16 [*Management of the Use of Force Regime*](#).

94 Grenade launchers (38), handguns (3717), rifles (207), shotguns (63) and sub-machine guns (18). Some officers (such as trainers) have multiple firearms on issue to them.

95 The AFP followed up on this data and identified a number of discrepancies in the data. On 31 March 2021, the AFP advised that all identified officers had either completed OSA or did not have a firearm on issue.

Table 3.7: Key elements of the Governance Instrument Framework

	Type	Detail
Primary	Commissioner's Orders (CO)	Issued by the Commissioner under section 38 of the AFP Act with respect to the general administration of, and the control of, the operations of the AFP.
	Commissioner's Financial Instructions (CFI)	Issued by the Commissioner under section 37(1) of the AFP Act and section 20A of the PGPA Act ^a CFIs set out the financial, legislative and regulatory requirements for the financial management and accountability of public resources by the AFP.
	National Guidelines (NG)	Typically establish mandatory compliance obligations in respect of higher-risk matters relevant to the whole of the AFP or a specific function.
Functional	Better Practice Guides (BPG)	Identify, assess and articulate good practice across the AFP.
	Handbook	Provide specific guidance and information relating to a particular subject matter, area of business or operation within the AFP.
	Standard Operating Procedures (SOP)	Detail and establish processes to be followed by AFP appointees for the performance of designated operations or functions in designated situations.

Note a: *Public Governance, Performance and Accountability Act 2013*. Known in other entities as Accountable Authority Instructions (AAls).

Source: AFP.

3.41 The documents within the GIF comprise primary governance instruments which are issued by the Commissioner pursuant to legislation, and functional governance documents which may be issued by Senior Executive Service level officers. In December 2020, the AFP advised that:

Under our Governance Framework, BPG's are among the lowest rung and are intended to articulate good practice. Similarly, Handbooks are intended to provide specific guidance. Neither are intended to be vehicles for promulgating rules, orders, instructions, practices and procedures across the whole AFP, that is the role of a Primary Governance Instrument.

3.42 However, when any instrument in the GIF uses the word 'must', compliance is mandatory and failure to comply may result in disciplinary action.⁹⁶ In a dynamic environment such as the AFP where new legislation may be introduced or existing legislation amended with potential impacts on operational policing, it is important that all governance instruments are accurate and up to date. The *AFP Commissioner's Order on Governance* (CO1) requires that:

AFP SES managers must have processes in place to regularly review AFP governance instruments to ensure currency and relevance — and this must take place at least every three years from their date of issue or last review. However, AFP governance instruments which treat high or critical risk must be monitored carefully and formally reviewed at least every two years.

3.43 Individual instruments do not indicate whether they 'treat high or critical risk' and it is therefore not possible to determine whether they are required to be reviewed every two years (rather than every three). In any event, however, all instruments should have been reviewed within

96 Under paragraph 4.1.1 of the *Commissioner's Order on Governance*, officers are required to comply with requirements 'which are denoted by the word 'must'' in an AFP governance instrument.

the last three years. The ANAO reviewed all instruments within the GIF as at 14 December 2020. In the following table, instruments which had been reviewed within the last two years are highlighted green, instruments which have been reviewed within the last two to three years (and therefore are possibly overdue for review) are coloured orange and those which had not been reviewed for more than three years are coloured red.

Table 3.8: Governance Instrument Framework instruments — last review as at 14 December 2020

	Period since last review							
	Less than two years		Two to three years		More than three years		Total	
	No.	Per cent	No.	Per cent	No.	Per cent	No.	Per cent
CO	1	20.0	2	40.0	2	40.0	5	100.0
CFI	1	100.0	0	0.0	0	0.0	1	100.0
NG	39	55.7	13	18.6	18	25.7	70	100.0
BPG	99	45.2	45	20.5	75	34.2	219	100.0
Handbooks	10	58.8	2	11.8	5	29.4	17	100.0
SOP	58	60.4	21	21.9	17	17.7	96	100.0
Total	208	51.0	83	20.3	117	28.7	408	100.0

Source: ANAO's analysis based on AFP data.

3.44 Table 3.8 shows that at the time of the ANAO's assessment, about half of all GIF instruments were overdue for review (or possibly so). This was consistent with one of the findings of the *Review into the AFP's response to and management of sensitive investigations* (the Lawler Review) which observed:

Examination by the review of 16 key and many other relevant governance documents identified that some: were out of date; did not include a review schedule; had no owner; had been overtaken by organisational changes; or referenced other documents that had been archived. Upon bringing this to the attention of the Commissioner, he directed senior managers to review their governance documents immediately to ensure they were updated.

3.45 The Lawler Review also recommended that the previous decentralised management of the GIF be recentralised to 'ensure the governance framework is current, maintained and fit-for-purpose.'

3.46 In July 2020, a formal review was established to give effect to the Commissioner's direction. The review's Terms of Reference are shown in Table 3.9.

Table 3.9: Review of Governance Instrument Framework: Terms of Reference

No.	Detail
1	Propose options for ongoing oversight and assurance of the GIF, consistent with broader options to enhance the effectiveness of governance instruments, including but not limited to: <ul style="list-style-type: none"> a) accountability of risk owners; b) active validation of governance instruments rather than passive timeframes for review; c) integration of governance instruments with enterprise risk management and business risk controls; and d) development of principles giving effect to a risk-based approach for development of governance instruments as a risk control.
2	Map and propose options for the integration of the body of primary and functional governance with enterprise governance, including risk, audit and assurance.
3	Review existing primary and functional governance instruments for critical gaps for urgent remediation to ensure consistency with Lawler review outcomes.
4	Propose a timeline for the review and revalidation of all primary and functional governance instruments.
5	Propose options for ongoing oversight and assurance of the GIF, consistent with broader organisational governance.

Source: AFP.

3.47 The review was completed in May 2021. Among its 12 recommendations were:

- that the AFP retain, manage and continuously improve a Governance Instruments Collection (GIC);
- transition to a principles-based AFP Orders and Instructions Framework rather than primary governance instruments and certain functional governance instruments;
- closer integration with other enterprise governance frameworks (in particular risk);
- stronger SES leadership and accountability;
- increased resourcing to support administration; and
- the AFP's Audit and Risk Committee to have primary responsibility for overseeing the quality and management of the GIC.

3.48 Implementation of the review's recommendations was commencing at the time of the conclusion of this audit.



Grant Hehir
Auditor-General

Canberra ACT
8 June 2021

Appendices

Appendix 1 Australian Federal Police's response



COMMISSIONER
GPO Box 401,
Canberra ACT 2601 Australia
Telephone +61 2 5127 4100
www.afp.gov.au

Our Reference: EC21-000751

20 May 2020

Mr Grant Hehir
Auditor-General
Australian National Audit Office

Via email: Grant.Hehir@anao.gov.au

Dear Mr Hehir

AFP Comments on proposed report under s.19 of the Auditor-General Act 1997

Thank you for the proposed audit report (Report) on the Australian Federal Police (AFP) use of statutory powers received on 21 April 2021 and the opportunity to respond.

The AFP is pleased the Report found the AFP's framework to ensure the lawful exercise of statutory powers is largely effective, that all statutory reporting requirements were met and that the warrants reviewed overwhelmingly complied with legislative requirements. This was heartening to me as a Commissioner focussed on accountability and continuous improvement.

As Australia's national policing agency, the AFP's mission is to protect Australians and Australia's interests. To achieve this mission the AFP has been entrusted with powers under various Commonwealth, State and Territory Legislation. These powers represent critical law enforcement tools which are accompanied by government and community expectations that they be used appropriately.

The Report identifies three recommendations around documentary evidence of review, implementation of an Electronic Data and Records Management System and implementation of a quality assurance process for section 3E Crimes Act warrants. These recommendations address findings in the report relating to record keeping and adherence to better practice.

The AFP accepts all recommendations. We note the commentary regarding non-compliance with better practice may be potentially misleading. Under AFP Governance, Better Practice Guides (BPG's) form part of AFP functional governance that exists to identify, assess and articulate good practice. As such BPG's are not intended to generate mandatory compliance obligations categorised by AFP primary governance instruments.

POLICING FOR A SAFER AUSTRALIA

Nevertheless, the AFP accepts that improvements can be made, including strengthening guidance around review requirements and considering when management or legal review may be required (for example, in the case of higher risk investigations). The AFP takes seriously its legislative and governance obligations and strives for continuous improvement in terms of its systems, processes, training and culture. For example, as a result of the Lawler Review, significant improvements were implemented in 2020 to ensure additional oversight of AFP sensitive investigations, including closer consultation with AFP Legal. A significant body of work is also underway to automate applications for warrants and authorities to exercise powers. This will promote compliance by building it into our automated systems and also stream-line record keeping.

In line with the AFP's commitment to accountability we have reviewed the six search warrants identified as containing deficiencies within the Report. Of these, one instance pertained to the execution of a warrant by the AFP. The remainder involved technical deficiencies, such as a partially completed date on behalf of the issuing officer, potentially inadequate descriptions used to describe the target, and a warrant executed by another agency.


In respect of record keeping, the AFP accepts that the distributed nature of information holdings within the AFP posed challenges for the ANAO's independent verification of material. Pleasingly, the AFP is unaware of any instance where it could not produce a document requested by the ANAO with the exception of one original affidavit retained by the issuing officer. Further, when drawing conclusions on record keeping, it should be acknowledged that policing and court processes remain heavily dependent on paper based records. For example, paper based warrants, briefs of evidence and official police diaries remain a necessary feature of policing.

Importantly, given the ever increasing volume of material that must be processed by modern police forces, information management remains an area of focus for the AFP and risks are assessed and mitigated on an on-going basis. Mitigation practices include the provision of enterprise wide unified search functionality and mandatory information management training. The development of an Investigative Management Solution to better integrate existing systems will also offer further mitigation of these risks.

Finally, strengthening guidance and compliance around record keeping obligations to ensure records pertaining to the use of statutory powers are appropriately captured on the AFP's investigative case management systems will continue to be an area of focus for the AFP. A dedicated implementation team will also be established in response to the findings of the Report, which will be overseen by the Deputy Commissioner Investigations.

On behalf of the AFP I would like to thank the ANAO for their work in ensuring the AFP remains accountable in its use of statutory powers and continues our learning as an organisation. I look forward to the tabling of the Final Report.

Yours sincerely



Reece P Kershaw APM
Commissioner

Appendix 2 Provisions of Acts that confer intrusive powers on Australian Federal Police Officers

Act	No.	Question, demand or gather information	Stop, enter, board, search, seize (person or place)	Arrest, detain, restrain, remove, recover
<i>A New Tax System (Family Assistance) (Administration) Act 1999</i>	3	102S(2), 102U(1)	–	102S(2)
<i>A New Tax System (Tax Administration) Act 1999</i>	2	–	260-150(1)	260-150(1)
<i>Antarctic Treaty (Environment Protection) Act 1980</i>	6	17(4)	17(1), 18(1), 18(2)	16(1), 17(1)
<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>	25	199(1), 199(2), 200(1), 200(2), 200(3)	199(2A), 199(3), 199(4), 199(5), 199(7), 199(8), 199(9), 199(10), 200(4), 200(5), 200(6), 200(7), 200(8), 200(9), 200(11), 200(12), 200(13), 200(13A),	201(1), 201(2)
<i>Australian Crime Commission Act 2002</i>	4	–	13(2), 31(2)	31(2), 34D(1)
<i>Australian Federal Police Act 1979</i>	15	14I(1), 14I(2)	14D(1), 14D(4), 14D(5), 14J(2), 14J(6), 14J(8), 14J(9), 14K(1), 14K(2)	14A, 14J(2), 14J(6), 14J(9)
<i>Australian Passports Act 2005</i>	6	23(1), 24(1), 24A(1), 25(1)	26(1), 26(2)	–
<i>Australian Security Intelligence Organisation Act 1979</i>	14	34W(1), 34W(5), 34ZD(2)	34ZB(1), 34ZB(3), 34ZB(5), 34ZB(8), 34ZB(9), 34ZC, 34U(1)	34G(3), 34K(7), 34U(1), 34ZD(2)
<i>Aviation Transport Security Act 2004</i>	7	–	83, 84(1), 85(1)	86(1), 87(1), 87(2), 88(1)
<i>Bankruptcy Act 1966</i>	5	–	130(2), 264B(4), 267E(3), 267E(4)	130(2)
<i>Biosecurity Act 2015</i>	2	–	–	103(1), 104(1)
<i>Budget Savings (Omnibus) Act 2016</i>	12	43Y(2), 43ZA(1), 102S(2), 102U(1), 200S(2), 200U, 1256(2), 1258(1)	–	43Y(2), 102S(2), 200S(2), 1256(2)
<i>Chemical Weapons (Prohibition) Act 1994</i>	2	–	14(2)	14(2)
<i>Child Support (Registration and Collection) Act 1988</i>	3	72U(2)	72U(2)	72U(2)
<i>Federal Circuit Court of Australia Act 1999</i>	2	–	113A(2)	113A(2)
<i>Classification (Publications, Films and Computer Games) Act 1995</i>	1	–	106	–

Act	No.	Question, demand or gather information	Stop, enter, board, search, seize (person or place)	Arrest, detain, restrain, remove, recover
<i>Cocos (Keeling) Islands Act 1955</i>	1	–	–	15AF
<i>Commonwealth Electoral Act 1918</i>	8	316(8)	316(8), 346(3)	200DB(6), 218(3), 346(3), 347(3), 348(5)
<i>Commonwealth Inscribed Stock Act 1911</i>	1	–	51	–
<i>Competition and Consumer Act 2010</i>	8	154G(1), 154H, 154R	154G(1), 154G(2), 154GA, 154H	154H
<i>Corporations Act 2001</i>	7	154E(b), 154R	154E, 154R, 154S	154E(e), 489A
<i>Court Security Act 2013</i>	9	15(1)	16(3), 17(6), 19(1), 28(2)	15(2), 16(1), 16(2), 28
<i>Crimes (Aviation) Act 1991</i>	8	–	49(1), 49(2)	30(1), 30(2), 32(1) 33(1), 33(2), 33(2A)
<i>Crimes (Biological Weapons) Act 1976</i>	1	–	9(2)	–
<i>Crimes (Currency) Act 1981</i>	1	–	29(2)	–
<i>Crimes (Internationally Protected Persons) Act 1976</i>	1	–	–	11(2)
<i>Crimes (Overseas) Act 1964</i>	2	–	–	6(1), 6(2)
<i>Crimes Act 1914</i>	59	3F(1), 3F(2B), 3J(1), 3L, 3UC(1), 3UP(1), 3V(1), 3ZJ(3), 3ZZKE, 3ZZLB	3E, 3F(1), 3F(2), 3L(2), 3T(2), 3UD(1), 3UE, 3UEA(1), 3UEA(2), 3UEA(5), 3UEA(6), 3US(2), 3ZB, 3ZE, 3ZF, 3ZG, 3ZH, 3ZZJA, 3ZZKA, 3ZZKB, 3ZZKD, 3ZZKF, 3ZZKG(2), 3ZZKG(4), 3ZZLB, 3ZZLC, 3ZZOA(1), 3ZZOB(2), 23WJ(3), 23WM(1), 23WN, 54(1)	3L(5), 3UD(1), 3UE, 3UEA(2), 3UEA(3), 3UEA(5), 3UEA(6), 3UQ, 3W(1), 3WA(1), 3X, 3Y, 3ZZKD, 19AV(1), 20BM(3), 23XF(1), 54(1)
<i>Crimes at Sea Act 2000</i>	2	–	6(1), 6(2)	–
<i>Criminal Code Act 1995</i>	13	105.21(2), 105.43(2), 105.43(3)	105.22(1), 105.23, 105.24	72.27, 105.19(1), 105.3, 105.4(1), 105.4(4), 105A.18(3), 105A.18(4)
<i>Customs Act 1901</i>	32	199(1), 199(4A), 199B(1), 203K(1), 213(1), 219R(12), 219RAA(5), 219W(4), 240AA, 240AC	187, 199(1), 199(2), 199A, 199B, 203(1), 203A(1), 203B(1), 203C(2), 203C(2A), 203CB(3), 203DA(4), 203DB(1), 211, 211A, 219R	203C(2), 210, 219Q(1), 219R(8), 219S(1), 219W(3)
<i>Cybercrime Act 2001</i>	6	3L(1), 3L(1A), 3LA(1), 201(1), 201(1A)	–	201(1A)

Act	No.	Question, demand or gather information	Stop, enter, board, search, seize (person or place)	Arrest, detain, restrain, remove, recover
<i>Defence Force Discipline Act 1982</i>	28	101B(1), 101C(1), 101C(2B), 101D(1), 101D(3), 101L(1), 101L(6), 101T(1), 101T(2)	91(2), 101P(1), 101P(3), 101W(1), 101W(2), 101W(3), 101X(1), 101X(2), 101Y(5), 101Z(1), 101Z(2), 101Z(3)	89(2), 89(5), 91(1), 94(1), 94(2), 170(4), 194(5)
<i>Defence Force Discipline Appeals Act 1955</i>	2	—	32(3)	32(3)
<i>Defence (Special Undertakings) Act 1952</i>	8	23(2)	20(1), 20(2), 21	20(1), 21, 22, 23(1)
<i>Defence Act 1903</i>	8	—	79(3), 116W(1), 116W(3)	72P(2), 82(4), 116F, 116G(1), 116V
<i>Environment Protection (Sea Dumping) Act 1981</i>	11	29(3), 29(5), 31(1)	29(2), 30(1), 30(2), 30(3)	29(2), 29(3), 29(4), 32(1)
<i>Environment Protection and Biodiversity Conservation Act 1999</i>	33	403(2A), 406(1), 443(2), 443(3), 443A(1), 444(1)	22(1), 403(2), 405(1), 406(1), 406A(2), 406AA(2), 407A(4), 408(1), 408(4), 431, 432, 433, 444A(1), 445(1), 456AA(2), 447(1)	8(1), 12(1), 13(2), 403(2), 403(3), 406AA(2), 406AA(3), 406AA(4), 406AA(5), 407A(6), 430(1)
<i>Excise Act 1901</i>	9	107BB(1)	104(1), 104(2), 107BA(3), 107BB(1), 107BB(6)	100(1), 100(2), 104(1)
<i>Extradition Act 1988</i>	13	—	13(1), 13(2), 14(1), 30(1), 30(2), 31(1)	13(5), 26(1), 30(1), 30(5), 38(1), 49(1), 49A(1)
<i>Fair Work (Registered Organisations) Act 2009</i>	1	—	335L(2)	—
<i>Family Law Act 1975</i>	4	—	122AA(1), 122AA(3)	68C(1), 114AA(1)
<i>Family Law Reform Act 1995</i>	2	—	67Q	68C(1)
<i>Federal Circuit Court of Australia Act 1999</i>	2	—	113A(2)	113A(1)
<i>Federal Court of Australia Act 1976</i>	2	—	55A(2)	55A(1)
<i>Financial Transaction Reports Act 1988</i>	6	—	33(3A), 33(4), 33(6), 33(7), 33(8)	33A
<i>Fisheries Management Act 1991</i>	26	84(1), 85A(1), 85E(1), 85F(2), 92(1)	Sch1A CI1(3), Sch1A CI15(1), Sch1A CI15(3), 84(1), 84(1AA), 84(1AB), 85(1), 85(2), 85(4), 85A(1), 85F(2), 85F(3), 106C(1), 106C(1A)	Sch1A CI1(1), Sch1A CI8(1), Sch1A CI12(1), 11(1), 12(1), 12(2), 84(1)
<i>Foreign Passports (Law Enforcement and Security) Act 2005</i>	6	16(2), 16A(2), 17(1)	16(2), 16A(3), 17(1)	—

Act	No.	Question, demand or gather information	Stop, enter, board, search, seize (person or place)	Arrest, detain, restrain, remove, recover
<i>Human Services (Medicare) Act 1973</i>	11	8ZE(1), 8ZG(2), 8ZGA(2)	8ZC(b), 8ZD, 8ZF(9), 8ZG(4), 8ZGA(4), 8ZI	8ZF(2), 8ZG(6)
<i>International Criminal Court Act 2002</i>	22	70(4), 78A, 88(1) 114(1), 120(1)	27(1), 27(2), 78(1), 78(2), 114(1), 127(2), 128, 129(1), 132, 133, 134, 135(1), 137(1)	43(1), 129(1), 182(1), 182(2)
<i>International Transfer of Prisoners Act 1997</i>	2	–	–	22(3), 56(1)
<i>International War Crimes Tribunals Act 1995</i>	17	40AH(1), 50(1)	15(1), 15(2), 34(1), 34(2), 50(1), 63(2), 65(1), 68, 69, 70, 71(1),	21(1), 65(1), 78(1), 79(1)
<i>Law Enforcement Integrity Commissioner Act 2006</i>	7	121(1), 123(2)	117(3), 123(5)	96D(1), 100(2), 139
<i>Life Insurance Act 1995</i>	2	–	144(2), 144(3)	–
<i>Marine Safety (Domestic Commercial Vessel) National Law Act 2012</i>	25	98(1), 99(2), 100(2), 104(2), 105(1), 106(1)	95(1), 96(1), 96(3), 97(1), 99(2), 99(3), 100(5), 103(1), 103(2), 104(2), 105(1), 105(5)	99(3), 99(5), 100(3), 101(1), 104(4), 104(6), 105(3)
<i>Maritime Powers Act 2013</i>	37	55(1), 57(1), 58, 63(2), 65, 115	32(1), 52(1), 54(1), 54(3), 56(1), 59(1), 61(1), 61(2), 61(3), 61(4), 888iiii 63(2), 67(1), 69(2), 70	32(1), 54(1), 54(3), 55(7), 60, 64(1), 66(1), 66(2), 68(1), 69(1), 71, 73(1), 78, 79(1), 83(1), 84, 116(1)
<i>Maritime Transport and Offshore Facilities Security Act 2003</i>	10	–	152(1), 152A(1), 153(1), 154(1), 155(1)	156(1), 156(2), 157(1), 158(1), 159(1)
<i>Migration Act 1958</i>	85	91W(1), 188(1), 192(3), 225(3), 225(4), 226(4), 227(4), 231(1), 245(3), 245F(3), 245F(10), 257(1), 257A(1), 261AE(1), 261AK(1), 268BA(2), 268BL, 268BM(1), 268CI(1), 268CJ, 268CK, 487K(1), 487K(2)	223(16), 223(18), 245F(3), 245F(10), 245FA(1), 251(1), 251(6), 251(8), 252(1), 252(2), 252(3), 252(4), 252A(1), 252G(1), 252AA(1), 268(2), 268CA(1), 268CB(1), 268CD(1), 268CE, 268CI(1), 268CR(2), 268CT(2), 487D(1), 487D(2), 487E, 487F(2), 487F(4), 487G(2), 487Z, 487ZC(1), 487ZH, 487ZJ	180(1), 180(3), 189(2), 189(3), 189(4), 192(1), 198B(1), 198AD(3), 199(1), 199(2), 199(3), 245F(3), 245F(3), 245F(8), 245F(9A), 245F(10), 245FA(3), 249(1), 249(1AA), 251(6), 251(7), 251(8), 252(3), 252(4), 252C(1), 253(1), 253(10), 261G(1), 268CT
<i>Mutual Assistance in Criminal Matters Act 1987</i>	10	–	38B(2), 38B(3), 38F(1), 38S(1), 38V(1), 38W(1)	25(1), 31(1), 38S(1), 38ZB(1)
<i>Norfolk Island Act 1979</i>	3	–	–	60F(1), 60G(2), 60H(1)
<i>Offshore Petroleum and Greenhouse Gas Storage Act 2006</i>	3	621(1)	621(1)	620(1)

Act	No.	Question, demand or gather information	Stop, enter, board, search, seize (person or place)	Arrest, detain, restrain, remove, recover
<i>Paid Parental Leave Act 2010</i>	2	200S(2)	–	200S(2)
<i>Petroleum (Australia-Indonesia Zone of Cooperation) (Consequential Provisions) Act 1990</i>	2	–	–	17A(1), 17A(2)
<i>Proceeds of Crime Act 1987</i>	20	66(4), 66(9), 66(10)	35(1) 35(2), 35(3), 36(1), 36(2), 36(4), 36(9), 36(10), 38(1), 38(2B), 42(2), 70(1), 71(4), 71(8), 72(2)	66(9), 69(2)
<i>Proceeds of Crime Act 2002</i>	20	202(1), 202(3), 204, 213(1), 219(4), 242(1)	205(1), 225(3), 227(1), 237(3), 245(4), 249(1), 251(2), 252(3), 257(1)	15C, 17(1), 18(1), 19(1), 20A(1)
<i>Protection of Cultural Objects on Loan Act 2013</i>	1	–	11(2)	–
<i>Protection of Movable Cultural Heritage Act 1986</i>	1	–	30(1)	–
<i>Protection of the Sea (Civil Liability) Act 1981</i>	3	15(4), 19C(2)	–	19(3)
<i>Protection of the Sea (Harmful Anti-fouling Systems) Act 2006</i>	2	17(2)	17(2)	–
<i>Public Order (Protection of Persons and Property) Act 1971</i>	11	13C(1)	13D(1), 13D(5), 13E(3)	12(2), 13D(1), 13E(1), 13E(3), 17(1), 17D(4), 22
<i>Referendum (Machinery Provisions) Act 1984</i>	4	–	–	28(3), 73CB(5), 134(3), 135(5)
<i>Removal of Prisoners (Australian Capital Territory) Act 1968</i>	2	–	–	5(1), 6(1)
<i>Removal of Prisoners (Territories) Act 1923</i>	3	–	–	7B(1), 8A(7), 10A(3)
<i>Retirement Savings Accounts Act 1997</i>	1	–	103(3)	–
<i>Royal Commissions Act 1902</i>	4	–	4(1), 4(3), 4(5)	6B(3)
<i>Service and Execution of Process Act 1992</i>	2	–	–	82(3), 94D
<i>Student Assistance Act 1973</i>	1	43ZA(1)	–	–
<i>Surveillance Devices Act 2004</i>	4	28(1), 28(1A), 37(1), 38(1),	–	–
<i>Taxation Administration Act 1953</i>	2	–	Sch1 Ch4 260E-150(2)	Sch1 Ch4 260E-150(2)

Act	No.	Question, demand or gather information	Stop, enter, board, search, seize (person or place)	Arrest, detain, restrain, remove, recover
<i>Telecommunications Act 1997</i>	19	547(1), 547B(1), 548(1), 549(1)	535(1), 542(2), 542(3), 544(1), 544(1A), 545(1), 545(2), 545(3), 547(1), 547A(1), 547B(1)	542(3), 545(3), 547B(1), 550
<i>Telecommunications (Interception and Access) Act 1979</i>	4	–	39(1), 139C, 180T	107P(1)
<i>Therapeutic Goods Act 1989</i>	23	28(5), 32EA(1), 40(4), 41EJ(1), 41EWA(6), 46A(1), 48(1)	28(5), 32EA(1), 37(2), 40(4), 41EJ, 41EWA(6), 41FN(1), 46(1), 46A(1), 46B(1), 47(1), 47(4), 48(1)	48BA(4), 48C(4), 48H(2)
<i>Timor Gap Treaty (Transitional Arrangements) Act 2000</i>	2	–	–	6B(1), 6B(2)
<i>Torres Strait Fisheries Act 1984</i>	4	42(1)	42(1)	42(1), 11
<i>Underwater Cultural Heritage Act 2018</i>	1	37(2)	–	–
<i>Weapons of Mass Destruction (Prevention of Proliferation) Act 1995</i>	1	–	17(2)	–

Source: ANAO's analysis based on publicly available data.

Appendix 3 AFP record keeping processes and practices

Summary of findings

1. This appendix examines the AFP's digital record keeping processes and practices. It also includes a limited examination of the AFP IT security framework.
2. The AFP's poor digital record keeping is a risk to the integrity of its operations.
 - The AFP does not have an Electronic Data and Records Management System (EDRMS) and keeps more than 90 per cent of its digital operational records in network drives which are not considered by the National Archives of Australia (NAA) to be appropriate for that purpose.⁹⁷
 - Records in network drives are not secure from unauthorised access, alteration or deletion.
 - The AFP does not have the capacity to identify all digital records that it holds on any individual or entity.
 - On its own assessment, in 2019, the AFP ranked 156th of 166 Australian government entities in its information management maturity.⁹⁸
 - Many officers choose not to use PROMIS, the AFP's current case management system and are not obliged to do so.
 - Based on a limited examination⁹⁹, the ANAO has identified gaps in the AFP's management of IT security.

Findings

3. As noted at paragraph 1.16, the ANAO considers that there are serious deficiencies in the AFP's digital record keeping.¹⁰⁰ Although record keeping was not originally included in the scope of the audit, the ANAO considers that the issues identified are sufficiently important to be reported upon in this appendix.
4. The conduct of this audit was complicated by the AFP's generally poor digital record keeping. In large part, this is due to the fact that the AFP does not have an EDRMS¹⁰¹ and by its own reckoning, 'has digital records in approximately 700 business systems'. However, it is also partly due to poor digital record keeping practices. This appendix examines the adequacy of the AFP's digital record keeping both as it relates to the exercise of statutory powers and more broadly.

97 The National Archives of Australia, *Network drives* [Internet], available from: <https://www.naa.gov.au/information-management/types-information-and-systems/systems-manage-information/network-drives> [accessed 12 May 2021].

98 The NAA provided the ANAO with the 2019 Agency Performance Index League Table which listed the index scores for all 166 entities.

99 The ANAO met with the AFP, and requested and reviewed documentation related to the AFP's management of the network and internal audits undertaken by AFP.

100 The AFP also has extensive paper-based records but this examination focussed on digital records.

101 Also known as an Electronic Content Management (ECM) system.

5. Auditor-General Report No.6 of 2006–07 *Recordkeeping including the Management of Electronic Records*¹⁰² observed that ‘Recordkeeping is a fundamental function of all Australian government entities’ and quoted the Australian Public Service Commissioner’s 2004–05 *State of the Service Report*:

The values set out in the [Public Service] Act provide that the APS is openly accountable for its actions within the ministerial responsibility to the Government, the Parliament and the Australian public. The maintenance of effective recordkeeping systems allows agencies to demonstrate that due process has been followed in actions and decisions. It also helps agencies to achieve business goals by ensuring that necessary corporate information is available and accessible as required. Furthermore, effective recordkeeping assists employees to meet their specific obligations to Ministers, the Government and the Parliament.

Importance of good record keeping in law enforcement

6. The ANAO has previously commented on the issue of record keeping in law enforcement entities. In a number of reports over several years, the ANAO identified deficiencies in both the Department of Immigration and Border Protection’s (DIBP’s) and the Australian Customs and Border Protection Service’s (ACBPS’) record keeping. Following the integration of DIBP and the ACBPS in July 2015, the new entity endorsed a *Records and Information Management Action Plan 2016–20* which succinctly outlined the risks of poor record keeping in the following terms:

- Poor decision making and advice to key stakeholders or for individuals;
- Poor intelligence to support operational requirements;
- Inability to accurately and comprehensively locate information on demand;
- Ongoing resource and productivity impacts as staff are redirected from core duties to manually locate or manipulate records and information;
- Rapidly escalating storage costs for both physical and digital material;
- Rapidly increasing resource costs and demands to manage records and information;
- Failure to comply with legislative requirements due to poor and inconsistent records and information management policies, systems, strategies and practices;
- Failure to deliver on strategic objectives and priorities (risk and crisis management);
- Increasing costs to defend the Department’s reputation; and
- Excess exposure to litigation, FOI, investigations, audits and government accountability.¹⁰³

102 Auditor-General Report No.6 2006–07 [Recordkeeping including the Management of Electronic Records](#).

103 Since the reports referred to in this paragraph, the ANAO has observed improvements in the Department of Home Affairs’ record keeping. In a recent audit in the Department of Home Affairs (which includes the former DIBP and ACBPS), [Procurement of Garrison Support and Welfare Services](#) (Auditor-General Report No.37 2019–20), the ANAO referred to its earlier findings and commented ‘Evidence identified throughout this audit indicates an improvement in record keeping: the majority of documents collected as evidence were filed in TRIM [an EDRMS], and contained a TRIM reference, improving the ability to identify related records, and that staff recognise their obligation under the department’s Records Management policy that ‘... evidence of the Department’s business activities and decision-making processes must be captured within approved records management systems.’’

7. In this audit, the ANAO saw evidence that many, if not all, of the same risks apply to the AFP. For example, in August 2018, a paper presented to the AFP's Information and Data Governance Committee reported on the status of the AFP's Strategic Risk 4.3 'We don't adequately manage or protect our information' in the following terms (emphasis in original):

However, the risk will remain at CRITICAL for the foreseeable future due to two key treatments not being supported and/or funded by the various strategic and finance committees. These are:

- Establishing a new Electronic Content Management (ECM) capability; and
- Establishing strong Information & Data Management section within the IDMA Branch.

8. The paper further noted that the likelihood of this risk occurring was 'almost certain' and that the consequence would be 'severe.'¹⁰⁴

9. The Australian Federal Police's *Investigations Doctrine* also underlines the importance of good record keeping in a law enforcement environment:

The maintenance and management of complete and accurate investigative records is of fundamental importance. Decisions made, actions taken and information uncovered should be recorded in detail while the information is still contemporary.

Accurate and well-managed records can directly facilitate the conduct and outcome of the investigation. This is particularly important in a complex, large or long-term investigation. During the conduct of an investigation, the ability to store, analyse and retrieve collected information in a timely fashion can help track progress toward objectives and identify new avenues of inquiry. At the outcome stage, this will facilitate the compilation of a brief of evidence which may be necessary for a prosecution or inquiry or to obtain any warrants necessary for certain prevention or disruption activities. Investigators should use the most effective and efficient information management system or tools consistent with dimensions of the investigation. Any information management system used needs to be able to record information and identify sources, credibility and any assessment of its truth and relevance.

Current AFP record keeping arrangements

10. Despite the reference at paragraph 4 above to the AFP having 'approximately 700 business systems', the AFP principally uses three different systems to store digital records and data which are described below.

Network drives

11. Network (or shared) drives are storage devices (such as hard disk drives) connected to an entity's computer system. Most computer systems are sold with some limited network drive storage capacity which can be added to later. The AFP has a number of network drives but the

104 As noted at paragraph 2.4, the number of enterprise risks was reduced to eight in April 2019. The relevant risk in the revised framework — systemic failure to effectively collect, use, manage or protect information — is rated as high.

main drive is known as the S drive. The AFP advised in October 2020 that the S drive contained approximately 680 TB¹⁰⁵ of data.¹⁰⁶

SPOKES

12. SPOKES is a web-based collaboration tool using Microsoft SharePoint through Internet Explorer. At October 2020, the AFP advised that it contains approximately 20 TB of data.

PROMIS

13. As noted at paragraph 2.29, PROMIS is the AFP's case management system. At the time of audit, the AFP advised that PROMIS held about 5 TB of data.

14. The total volume of the three systems described above is 705 TB (of which network drives account for 96.4 per cent). However, this amount is significantly different — by a factor of four — from the advice that the AFP has provided to the NAA¹⁰⁷ in 2019 that the total volume of its digital records were 3,000,000 GB (which is 3000 TB). The ANAO asked the AFP to explain the difference between the two figures (which is 2,295TB). The AFP advised that 'Share Drives, PROMIS and SPOKES are a fraction of our digital information holdings. The NAA response figure includes ALL Digital holdings' and that 'the majority of the remaining digital information is stored in digital forensics (evidence store of lawfully seized data) and is managed according to post court outcomes, which includes destruction or returning to owner'.

15. At the time of audit, the AFP was in the process of implementing an Investigations Management Solution (IMS) which is 'a software solution being developed to provide a single platform for operational members to manage investigations throughout their lifecycle'. It is not intended to replace PROMIS but to 'supersede the investigations management functionality' of it. A decision was made not to migrate the records currently in PROMIS into the IMS and 'only new investigations will be managed using the IMS.' As with PROMIS, its use will not be mandatory. To that extent, the IMS will become a fourth record keeping system.

EDRMS vs network drives

16. The NAA recommends that entities use an EDRMS rather than managing their information with a network drive. The NAA has identified the benefits of an EDRMS as including:

- greater security and access control over sensitive information;

105 The University of Oregon has calculated that one terabyte is the equivalent of 85.9 million pages of Microsoft Word documents. On that basis, the volume of records contained on the S drive is the equivalent of approximately 58.4 billion pages. In practice, the S drive would also contain data in other formats such as photographs and PDF documents which take up more space.

106 There are no mandated naming conventions for the S drive and officers are free to create folders as and when they choose. There are a total of 137,111 folders in the S drive. Some of these folders bear simply a Christian name or surname, and others had names such as Ideas 'n stuff, Old stuff, Misc, Junk, My music and Footy tips 2002.

107 The functions of the NAA as set out in the *Archives Act 1983* include 'overseeing Commonwealth record-keeping, by determining standards and providing advice to Commonwealth institutions' and 'to impose record-keeping obligations in respect of Commonwealth records'.

- guaranteed authenticity and integrity of information by ‘locking down’ the final authoritative version of a record;
 - reduced risk of loss or inappropriate destruction of important information;
 - more accurate and faster retrieval of information;
 - enhanced ability to locate and retrieve information;
 - comprehensive audit trails; and
 - reduced duplication.
17. In contrast, the NAA describes¹⁰⁸ the risks of network drives in the following terms:
- anyone who has access can alter or delete records;
 - it is difficult to demonstrate the authenticity, integrity and trustworthiness of uncontrolled records;
 - it can be difficult to identify the record’s status or version;
 - metadata is often missing and there are no links between documents and their business context;
 - poor management can result in large volumes of uncontrolled information, which is difficult to manage and takes up network space; and
 - difficulty finding relevant records poses a reputational risk to the agency.

Reports on AFP record keeping

18. Evidence in a number of both external and internal reports show that the AFP has long been aware of the need to improve its digital record keeping. Extracts from these reports are quoted below. These reports have been quoted at some length in order to demonstrate that there are a variety of issues in relation to the AFP’s record keeping and that they are longstanding.

External reports

Information Governance Assessment (Deloitte, August 2009)

There is no whole-of-AFP vision and approach to information ... Individual business areas are developing separate ways and means to manage information;

Our information governance assessment has found a number of key issues faced by the AFP as it relates to Information Governance. Specifically:

- Lack of an enterprise vision for information governance and management
- A lack of structure for consistently categorising information regarding how and when information should be shared and/or disseminated
- There is no definitive list of where information is available across the organisation, which has resulted in the recreation of existing documentation as opposed to reuse

108 The National Archives of Australia, *Network drives* [Internet], available from: <https://www.naa.gov.au/information-management/types-information-and-systems/systems-manage-information/network-drives> [accessed 12 May 2021].

More than half of AFP's information is not maintained in structured "systems", but is contained in files of various kinds that are created, structured, organised and stored on the basis of operational contexts in which they arise. These files are created and managed in the absence of any organising framework...

Operational resources spend a disproportionate amount of their time in searching for operational and corporate information to support their core responsibilities and activities.

There is no definitive list of where information is available across the organisation, which has resulted in the recreation of existing documentation as opposed to reuse.

Our assessment has indicated that sharing and dissemination of information is limited due to... a lack of structure for consistently categorising information regarding how and when information should be shared and/or disseminated. This has resulted in AFP members not understanding the information held by the AFP and the value to investigations and intelligence.

National Security Hotline (Auditor-General Report No.4 2010–11)¹⁰⁹

The AFP advised the ANAO in May 2010 that it had corporately 'already recognised opportunities for enhancement' in relation to administrative record keeping and provided a draft Plan for Implementation of an AFP Information Management Strategy which sets out to address these known shortcomings.

On 29 October 2009, the AFP provided approximately 100 loose papers that were said to have been left by the previous manager of the relevant work area. A further request for administrative records was made on the same day. On 25 November 2009, the AFP advised the ANAO that it could locate no further documentation. After intervention at a more senior level in the AFP, a small number of additional records were provided, as well as four hard-copy files, one of which was empty.

Administration of Project Wickenby (Auditor-General Report No.25 2011–12)¹¹⁰

The AFP's use of PROMIS and local network drives to electronically manage and store case documentation was not consistent across Project Wickenby investigations. For example, not all investigation management plans were uploaded into PROMIS. The AFP advised that it is in the process of procuring a commercial investigation, intelligence and incident management system that would replace PROMIS and better manage case documentation.

Management of the Use of Force Regime (Auditor-General Report No.30 2015–16)¹¹¹

The AFP informed the ANAO that there are acknowledged integrity issues with its equipment issuance records, and that some of the equipment items identified above may be of a specialist nature, and that teams trained in the use of these weapons often maintained their own training records independently of the centralised qualification database.

Managing Mental Health (Auditor-General Report No.31 2017–18)¹¹²

Information on employee mental health is held across a range of disconnected information systems and multiple hardcopy records which make it difficult for the AFP to monitor and respond to emerging issues.

109 Auditor-General Report No.4 2010–11 [National Security Hotline](#).

110 Auditor-General Report No.25 2011–12 [Administration of Project Wickenby](#).

111 Auditor-General Report No.30 2015–16 [Management of the Use of Force Regime](#).

112 Auditor-General Report No.31 2017–18 [Managing Mental Health](#).

The AFP Organisational Health function has six bespoke Microsoft Access databases to hold relevant information on AFP employees. These databases were designed and developed in-house by AFP staff to assist in managing information that had previously been held in hardcopy files. The databases are not supported by AFP ICT, have functionality limitations and do not integrate with the AFP's corporate records management system.

...case notes are not filed in a consistent manner and may be located on the AFP's H-drive, attached to individual AFP employees' psychological hard copy file or added to the PLANES access database.

Internal reports and other documents

AFP Information Management Strategy and Roadmap 2015–18 (May 2015)

A large barrier to timely delivery of FOI information to members of the public, journalists and others is sourcing information. Members spend a considerable amount of time searching PROMIS and other information systems.

The AFP is immature in its information management. There is no consistent approach to information management and as a result:

- there is inability to easily search, access and share information;
- there is limited confidence in the integrity of information;
- existing information systems are not addressing current and evolving information management needs;
- the AFP is poorly positioned to exploit the value of its digital holdings. In May 2012, an AFP staff survey was conducted and 76% of the respondents said they spend an average of 90 minutes a day searching for information¹¹³;
- we do not know what information we have, where it is stored, how to find it and how to analyse it and use it in the most effective way.

The first phase of an AFP EDRMS project commenced in 2014–15. The second phase did not receive SIC funding for 2015–16.

Digital Investment Moratorium (METIS Committee¹¹⁴ paper, December 2017)

Currently the AFP has no digital system that is compliant with the National Archives Act.

We have no definitive way of knowing we have disclosed all the information we are holding on a person / event and this opens the AFP up to adverse criticism and increases risk of legal action.

Update on Strategic Risk 4.3.a (METIS Committee paper, August 2018)

However, the risk¹¹⁵ will remain at CRITICAL for the foreseeable future due to two key treatments not being supported and/or funded by the various strategic and finance committees. These are:

- establishing a new Electronic Content Management (ECM) capability; and

113 The ANAO did not seek to verify this estimate. However, if the estimate was correct, it is the equivalent of more than 1000 staff per year or \$143.4 million (based on 2019–20 staffing numbers and staff costs).

114 The METIS committee is the AFP's Information and Data Governance committee. Its terms of reference state that its primary objectives are to: strategically position the AFP to be a good manager of its data and information; maximize the value of its data and information by balancing information related benefits and opportunities with their associated costs and risks; and meet its legislative, legal, policing and administrative information obligations and requirements.

115 The risk referred to was the then enterprise risk 'We don't adequately manage or protect our information'.

- establishing strong Information & Data Management section within the IDMA Branch.

Data management maturity in the AFP (AFP Audit and Risk Committee paper, March 2019)

The AFP remains in the bottom 10% of agencies that have still not progressed a pathway for moving away from paper-based processes. This is a direct consequence of funding for an Electronic Document Records Management System (EDRMS) being consistently re-directed towards other priorities. Overall the AFP scores 140th out of 146 Agencies.

Summary of AFP Enterprise Capability Priorities (October 2019)

Collected information are recorded and stored inconsistently across systems, email and personal folders, where information holdings are kept in disparate format and inaccessible.

Inquest into the deaths arising from the Lindt Café Siege¹¹⁶ highlighted criticality of collection and record management for police. The inquest concluded that deficiencies identified in record and information management had the potential to degrade operational effectiveness.

Inability to access information as a result of recording investigation materials in disparate format (e.g. diary, PROMIS, personal drive) leads to missing information and difficulty in conducting post-operational analysis.

Background information on Enterprise Capability Priorities — eDRMS (September 2020)¹¹⁷

AFP collected information is currently recorded and stored inconsistently across systems, email and folders and information holdings are kept in disparate format and is inaccessible in some cases. This lack of information management is complex and multi-faceted which is largely due to current technology limitations.

Check-up and Check-up plus

19. In 2010, the NAA introduced Check-up 2.0. As part of this program, all Australian Government entities are requested to complete self-assessment questionnaires 'to assess their information and records management practices'. In 2018, Check-up 2.0 was replaced with Check-up Plus (also a self-assessment questionnaire) to assess entities' 'maturity and performance in information management.'

20. The 2019 survey asked entities to respond to 19 multi-part questions addressing the areas of:

- information governance;
- creation and generation of information;
- interoperability of information, systems and processes;
- storing and preserving information digitally;
- disposing of information (by destruction and transfer); and
- digital operations.

116 The Lindt Café siege occurred in Sydney on 15 December 2014 when a lone gunman took 18 people hostage in the café. The gunman executed one hostage and one hostage was killed when the NSW police raided the café.

117 This document was prepared for the ANAO audit team in response to its queries. The paper estimated the cost of implementing an EDRMS as \$4 million over seven years.

21. The NAA compiles entities' responses and provides each entity with analysis which allows it to compare its performance with other entities. Table A.1 shows the AFP's information management maturity index scores for 2019 which shows that the AFP was ranked 156th of 166 entities.

Table A.1: Check-up Plus: AFP index scores

Index	Score (out of 5)	Rank (of 166 entities)
Governance	2.86	123
Information Creation/Generation	1.95	165
Interoperability	2.12	138
Storing Information Digitally	2.00	152
Disposing	1.29	149
Digital Operations	2.00	160
Overall	2.22	156

Source: National Archives of Australia.

Record keeping guidance and instructions

22. As discussed in Chapter 3, the AFP maintains a Governance Instrument Framework (GIF) to provide officers with guidance and direction. A number of GIF instruments deal with information creation, management and storage.

23. The *Information Management Handbook* (published in June 2019) reminds officers that 'in accordance with the Archives Act, the AFP must create and manage records which document AFP business activities and processes', but does not provide information or instructions on where officers should store documents. The Handbook states:

Electronic systems for storing information (including e-mail, text messages, network drives, SPOKES or any other electronic information systems) are not record-keeping systems formally managed by the AFP.

Current Electronic systems for storing information lack key record-keeping functionality and cannot ensure the integrity, security and defensible destruction of records. For example records in these repositories or systems can be:

- Inappropriately Deleted;
- Inappropriately Altered;
- Inappropriately Accessed;
- Inaccessible when needed;
- Kept for longer than required.

24. Similarly, a document entitled *Record-keeping framework and responsibilities* (issued in July 2019) states (emphasis in original):

Where not to keep records.

Records should not be kept in:

- Outlook folders
- personal drives
- temporary drives
- shared areas on the network.

These electronic repositories and systems are not record-keeping systems. AFP personnel must not use them as a records management system because they lack key record-keeping functionality and cannot ensure the integrity and security of the record over time.

25. The *Better Practice Guide on Conducting Information Audits* (issued in May 2018) states:

Information is a critical strategic asset for the AFP and must be treated and accounted for accordingly. The mismanagement of information has been identified as a strategic critical risk... To identify information assets, the business area needs to perform an Information Audit.

An Information Audit is the process for identifying and evaluating your business area's information and identifying Information Assets. The audit identifies what information is held, who holds it, how it is managed, how it flows through the organisation and what is the value of the information, whether it should be retained and who should access it.

The Report that contains your findings and any action you have completed will now become an official AFP record and becomes a high-value information asset.

26. In November 2020, the ANAO asked the AFP how many business areas have undertaken audits since the BPG was issued in 2018 and where the audit team could find them. The answer the AFP provided was 'the answer to your questions is likely to be unknown and nowhere'. No further response was received.

AFP record keeping practices

27. In March 2021, the AFP advised that some officers 'do not like PROMIS' and 'do not use it to its full extent' although 'all investigations must have a PROMIS case which is created when the complaints or allegations are accepted.' The ANAO's fieldwork found that many officers preferred to use network drives to store digital records relating to warrants (such as applications, affidavits and warrants themselves). As a result, obtaining relevant documents to support the ANAO's assessment of a selection of warrants was time consuming, even with the AFP's assistance, leading to the ANAO having to revise its selection of warrants. For example, the ANAO's selection of warrants for assessment was based on PROMIS case numbers. It became apparent that for a given case number, while some affidavits and warrants were stored in PROMIS, others were in the network drive. In one instance, 10 warrants were in PROMIS but a further 12 were in the network drive.

28. As noted above, there is an absence of clear, mandatory and unequivocal direction to officers as to where they must store this type of information which could potentially be required either as reference for future operational activity or required to be produced in court (or for an inquest such as the Lindt café inquiry).

AFP IT security

29. During the audit, it became apparent that there may be weaknesses in the AFP's IT security framework. For example, the audit team was advised that individuals' access to folders in the

network drive is not managed, with officers able to continue using and accessing folders 'belonging' to work areas that they left some years ago.

30. At the ANAO's request, the AFP provided key system and network documentation and internal audit reports. While the scope of this audit did not permit a full examination or audit, on the basis of a review of the documents provided and discussions with the AFP, the ANAO considers that:

- all system and network documentation provided is significantly out of date: the Australian Government Information Security Manual¹¹⁸ requires that entities' security documentation should be kept up to date and reviewed at least annually;
- many of the risk mitigations in place and assessments documented are no longer relevant because they were based on an operating system that the AFP no longer uses; and
- no current documentation was provided by the AFP to indicate that its security configurations are appropriate.

31. On the basis of the ANAO's limited review and discussions:

- the AFP's security management of its network and systems has gaps; and
- the AFP is not meeting the mandatory requirements of the Australian Government's Protective Security Policy Framework.

118 The Information Security Manual is published by the Australian Cyber Security Centre to 'outline a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats'.

Appendix 4 AFP recruitment programs: modules and subjects

