The Auditor-General
Auditor-General Report No.35 2025–26
Performance Audit

Administration of Investigations in Defence

Department of Defence

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76192-027-1 (Print)
ISBN 978-1-76192-028-8 (Online)

Chief Operating Officer
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:
communication@anao.gov.au.

Australian National Audit Office

Canberra ACT

29 May 2026

Dear 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 Department of Defence. The report is titled *Administration of Investigations in Defence*. 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

Dr Caralee McLiesh PSM
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 their 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

Contents

Summary and recommendations 7
Background 7
Conclusion 8
Supporting findings 8
Recommendations 9
Summary of entity response 11
Key messages from this audit for all Australian Government entities 12
Audit findings 13
1. Background 14
Introduction 14
Rationale for undertaking the audit 23
Audit approach 23
2. Arrangements for the conduct of investigations 25
Has Defence established an appropriate framework for managing investigations? 26
Has Defence developed training and guidance to support investigations? 35
3. Implementation of arrangements for investigations 51
Has Defence established monitoring and quality assurance arrangements for investigations? 51
Have selected investigations been conducted in accordance with the framework? 73
Appendices 87
Appendix 1 Entity responses 88
Appendix 2 Improvements observed by the ANAO 91
Appendix 3 Hierarchy of Defence documents 93
Appendix 4 Royal Commission recommendations 94

Audit snapshot

Auditor-General Report No.35 2025–26

Administration of Investigations in Defence

Why did we do this audit?

- An effective investigation function should support integrity, transparency and accountability, enable timely, proportionate and fair responses to potential non-compliance, and safeguard the wellbeing of impacted individuals.
- The 2022 Australian Government Investigations Standard (AGIS) sets the standard for Australian Government entities conducting investigations.
- The Senate Foreign Affairs, Defence and Trade Legislation Committee raised concerns regarding Defence investigations including timeliness, decision-making, and victim wellbeing.

Key facts

- The Department of Defence (Defence) has established four Defence Investigative Authorities for investigating matters referred under Defence's 'notifiable incidents' reporting pathways.
- The Inspector-General of the Australian Defence Force (IGADF) conducts independent investigations and inquiries into the military justice system.

What did we find?

- Defence has partly effective arrangements in place for the administration of investigations. Defence's investigations framework does not clearly align its different investigation functions or enable them to work together effectively, including referrals between Defence Investigative Authorities (DIA). Defence cannot assure that incidents are directed to the most appropriate DIA or that the same incident would receive the same outcome regardless of the reporting pathway.
- Investigations have not always been conducted in accordance with Defence policy or in a timely manner. Reported incidents have not always been handled in accordance with Defence policies and guidance, and Defence has not established enterprise-level reporting for incidents and investigations not related to fraud.

What did we recommend?

- There were nine recommendations to Defence relating to investigative jurisdictions, management of procurement related complaints, investigator qualifications, investigative guidance, monitoring and reporting, recovery of fraud-related debts, quality assurance, and the conduct of fact-finding and investigations.
- Defence agreed to all nine recommendations.

3,154

Closed investigations recorded by DIAs and IGADF between 1 January 2020 and 31 December 2025.

196 days

Average time between incidents being reported and investigations completed across the four DIAs.

269 days

Average time taken to finalise IGADF military police professional standards assessments, inquiries, and investigations.

Summary and recommendations

Background

1. An effective investigation function should support integrity, transparency and accountability, enable timely, proportionate and fair responses to identified incidents of potential non-compliance, and assist in safeguarding the wellbeing of impacted individuals. It should also support continuous improvement by providing assurance on the adequacy of existing practices.

Rationale for undertaking the audit

2. The Senate Foreign Affairs, Defence and Trade Legislation Committee[1] has raised concerns regarding Department of Defence (Defence) investigations, inquiries and fact-finding activities at previous hearings, including:

- timeliness and robustness of investigative processes;
- decisions to prosecute personnel and contracted companies for fraudulent conduct;
- potential repercussions against people reporting incidents within Defence;
- conduct and recording of fact-finding;
- wellbeing of victims involved in investigations; and
- extent to which the Inspector-General of the Australian Defence Force (IGADF) has been subject to previous Australian National Audit Office (ANAO) scrutiny.[2]

3. Previous ANAO audits have identified deficiencies in the way Defence handles procurement and contractor integrity issues, including not identifying and reporting notifiable incidents.[3]

Audit objective and criteria

4. The audit objective was to assess the effectiveness of Defence's administration of investigations and inquiries. This included investigations and inquiries conducted into Australian Public Service (APS) personnel, Australian Defence Force (ADF) members, and Defence contractors, consultants and outsourced service providers, which are subject to different legislative frameworks and employment conditions (see paragraphs 1.3–1.4).

1 Parliament of Australia, *Senate Standing Committees on Foreign Affairs Defence and Trade*, Australian Government, Canberra, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade [accessed 25 March 2026].

2 In June 2023, Senator Jacqui Lambie wrote to the Auditor-General requesting a performance audit be conducted into the effectiveness and efficiency of the IGADF. Further correspondence from Senator Lambie was received in October 2023, November 2023 and October 2024. Senator Lambie's correspondence, and the Auditor-General's responses are available at: https://www.anao.gov.au/work/request/audit-of-the-inspector-general-of-the-australian-defence-force.

3 Auditor-General Report No.50 2024–25, *Department of Defence's Sustainment of Canberra Class Amphibious Assault Ships (Landing Helicopter Dock),* ANAO, Canberra, 27 June 2025, paragraphs 3.55–3.68, available from https://www.anao.gov.au/work/performance-audit/department-of-defence-sustainment-of-canberra-class-amphibious-assault-ships-landing-helicopter-dock [accessed 24 May 2026].

5. To form a conclusion against this objective, the following high-level criteria were adopted:

- Has Defence established fit-for-purpose arrangements for the conduct of investigations?
- Has Defence effectively implemented its arrangements for investigations?

Conclusion

6. Defence has partly effective arrangements in place for the administration of investigations. Defence's investigations framework does not clearly align its different investigation functions or enable them to work together effectively, including referrals between Defence Investigative Authorities (DIA). As a result, investigations may not be managed in a consistent or coordinated way, creating a risk that responses are not timely, fair, or proportionate.

7. Defence has not established an enterprise-wide approach to investigative jurisdictions, including clear referral pathways between investigative authorities and safeguards for the management of incidents by Defence investigative functions. Defence cannot assure that incidents are directed to the most appropriate DIA or that the same incident would receive the same outcome regardless of the reporting pathway. Defence has not complied with Australian Government Investigations Standard (AGIS) requirements for investigators to hold qualifications.

8. Investigations have not always been conducted in accordance with Defence policy. Between January 2020 and December 2025, the average time to finalise investigations after an incident was reported was 196 days for DIAs and 269 days for IGADF military police professional standards assessments, inquiries and investigations. These protracted timeframes may present risks to the wellbeing of affected personnel if not appropriately managed. Fact-finding activities have been conducted into notifiable incidents without proper referral to DIAs, as required by Defence policy. Defence has not established enterprise-level reporting for incident and investigation trends, timeliness and outcomes that are not related to fraud, limiting Defence's assurance that similar matters are dealt with equitably, proportionately and in alignment with Defence policies.

Supporting findings

Arrangements for the conduct of investigations

9. Defence has established requirements for notifiable incidents to be reported to a DIA. There is overlap between the roles of DIAs and the conduct of fact-findings and inquiries. Reporting pathways for notifiable incidents are not always aligned with Defence policies and rely on judgement. This creates a risk that reported incidents are not managed equitably and proportionately, or with the appropriate level of DIA oversight. (See paragraphs 2.3–2.36)

10. DIAs and the IGADF have established guidance to support investigations. Recognising the complexity of Defence's investigations system, DIA-level guidance does not always establish clear jurisdictions or referral processes between DIAs, or for deciding whether an investigation or inquiry is warranted. This impacts the alignment and interoperability of Defence's investigative functions. Defence has not established enterprise-level arrangements to ensure that investigative and inquiry processes achieve outcomes that are equitable and proportionate to the conduct. Defence guidance has not been regularly reviewed, and Defence does not hold qualification records for all investigators or supervisors involved in investigations. These deficiencies increase

the risk that Defence and Commonwealth investigation policies are not consistently applied or complied with. (See paragraphs 2.37–2.97)

Implementation of arrangements for investigations

11. Defence has implemented quarterly reporting to governance committees on fraud-related incidents and investigations. There is no enterprise-level reporting on the trends, timeliness and outcomes of incidents and investigations across DIAs and the IGADF that are not related to fraud. Defence has not established enterprise-level performance measures or AGIS aligned quality assurance arrangements for investigations, presenting a risk that investigations are not handled equitably and proportionately. Investigations and inquiries are not always conducted in a timely manner or in accordance with targets for investigation timeliness, where they have been set by investigative functions. Fraud recoveries have not been undertaken in a timely manner and unrecovered fraud debts have not been managed in accordance with the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). (See paragraphs 3.3–3.87)

12. Investigations and inquiries have not always been conducted in accordance with Defence policy. Deficiencies were identified in: record keeping; investigation and inquiry planning; documentation of key decisions and evidence; the provision of updates to stakeholders; and consultation with relevant authorities. Decisions to investigate or refer matters have been applied inconsistently by Defence, and fact-finding activities have been conducted for notifiable incidents without referral to DIAs, as required by Defence policy. (See paragraphs 3.88–3.117)

Recommendations

Recommendation no. 1
Paragraph 2.36

The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, strengthen enterprise-level guidance to clearly outline the jurisdiction of each Defence Investigative Authority and the IGADF and provide for the effective management of reported incidents and investigations.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 2.50

The Department of Defence, in preparation for the establishment of the Defence Delivery Agency from 1 July 2027, establish clear and consistent arrangements for managing procurement-related complaints that are currently handled by the Capability Acquisition and Sustainment Group.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 2.85

The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force:

(a) update Defence Investigative Authority and IGADF guidance to align with Commonwealth and Defence policies and provide clear direction on the triaging and referral of incidents between investigative functions;

(b) implement enterprise-level policy to mandate regular review of investigation guidance and process documents; and

(c) establish enterprise-level requirements to support the equitable management and proportionate outcomes of investigations, such as for the referral of matters to the Australian Government Security Vetting Agency.

Department of Defence response: *Agreed.*

Recommendation no. 4
Paragraph 2.97

The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, ensure that AGIS required investigator qualifications, including accepted equivalencies, are in place and recorded for all investigators involved in investigations.

Department of Defence response: *Agreed.*

Recommendation no. 5
Paragraph 3.47

The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, implement enterprise-level oversight mechanisms to support an end-to-end investigative framework and monitor:

(a) DIA and IGADF performance relating to investigation outcomes and timeliness; and

(b) actions taken by business areas and units in response to investigation findings and recommendations.

Department of Defence response: *Agreed.*

Recommendation no. 6
Paragraph 3.59

The Department of Defence ensure that Commonwealth and Defence policy requirements for the recovery and write off of fraud-related debts are enforced and that the value of write offs are reported appropriately within the department.

Department of Defence response: *Agreed.*

Recommendation no. 7
Paragraph 3.84

The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, establish quality assurance arrangements for Defence Investigative Authorities and the IGADF that align with AGIS requirements, including requirements for regular independent external review.

Department of Defence response: *Agreed.*

Recommendation no. 8
Paragraph 3.96

The Department of Defence implement measures to improve awareness and educate units when fact-finding is appropriate and the approvals requirement for fact-finding into notifiable incidents.

Department of Defence response: *Agreed.*

Recommendation no. 9
Paragraph 3.117

The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, ensure:

(a) key investigation and inquiry decisions and documents are recorded for all investigations and inquiries; and

(b) regular updates are provided on investigation and inquiry progress to relevant stakeholders as required under Defence policies and guidance.

Department of Defence response: *Agreed.*

Summary of entity response

13. The proposed final report was provided to the Department of Defence. The summary response is provided below with a full response at Appendix 1.

> Defence and the Inspector-General of the Australian Defence Force (IGADF) acknowledge the findings of the Auditor-General's Performance Audit report: *Administration of Investigations in Defence* and accepts the key findings and recommendations laid out in the report. The Defence Investigative Authorities will implement the recommendations to further strengthen and enhance the effectiveness of the investigative function.
>
> Defence and the IGADF are committed to safeguarding the integrity of government resources and to upholding the highest standards of conduct and accountability across the organisation. This commitment includes ensuring incidents and investigations are managed in a consistent, fair and proportionate manner, reflecting the nature and seriousness of the conduct involved and the diversity of the workforce.
>
> Defence and the IGADF operate within a complex environment involving both the Australian Defence Force members and Australian Public Service employees, shaped by multiple legislative, regulatory and policy frameworks. The circumstances in which incidents arise vary significantly in terms of context, with differing operational settings, impacts and consequences.
>
> Defence and the IGADF continue to strengthen governance, assurance and oversight to improve transparency, data quality and monitoring of system impacts. These measures have included reviews of Defence Investigative Authority artefacts and technical instructions. In light of the ANAO recommendations, Defence will also review its enterprise level policies to ensure jurisdictional clarity and management of incidents. Defence has also harmonised 16 legacy

systems with the introduction of the Defence Enterprise Resource Planning Case Management Solution system.

Measures have been taken to mitigate the impacts of investigations, inquiries and military justice processes on personnel by improving procedural clarity, strengthening workplace protections, and embedding trauma-informed practices. This includes implementation activities underway for the 30 Defence-led and 13 IGADF-led recommendations in Volume 3 of the Royal Commission into Defence and Veteran Suicide Final Report, which focuses on military sexual violence, unacceptable behaviour and military justice.

Key messages from this audit for all Australian Government entities

14. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance and risk management

- Well-designed incident reporting and investigation arrangements support confidence in the integrity of the system, encourage individuals to report concerns, and help ensure reported matters are addressed appropriately and in a timely manner.
- Clear enterprise-level arrangements for investigative functions, including defined processes for triaging and assessment of incidents, supports consistent decision-making, reduces duplication, and promotes consistency in investigation responses.
- Active monitoring of investigative timeframes, caseloads and delays supports timely resolution and helps mitigate risks to the wellbeing of affected individuals and to the entity.
- Timely fraud recovery and debt management practices support compliance with the *Public Governance, Performance and Accountability Act 2013* and reinforce an organisational culture of integrity and accountability in the use of public resources.
- Persistent non-compliance with legislative frameworks, policies and probity requirements can escalate into more serious misconduct risks. Entities with mechanisms in place to identify and report these matters are better positioned to detect systemic issues and strengthen preventative controls.

Records management

- Good record keeping underpins the integrity and defensibility of investigations and inquiries, particularly where activities may result in adverse outcomes for individuals.
- Documenting key decisions, the rationale for those decisions, and the extent to which relevant evidence is considered supports integrity, transparency and defensibility of investigative processes.

Audit findings

1. Background

Introduction

1.1 The Department of Defence's (Defence) mission and purpose is to defend Australia and its national interests in order to advance Australia's security and prosperity. As at 30 June 2025, Defence was resourced to deliver against this through 20,545 Australian Public Service (APS) personnel and 92,178 Australian Defence Force (ADF) members, including 33,269 ADF reservists.[4]

1.2 Defence conducts a wide range of investigative and inquiry activities in relation to incidents involving ADF members and APS personnel, including matters in relation to: misconduct; public interest disclosures; policing; procurement; security; unacceptable behaviour[5] and sexual misconduct; vehicle accidents on Defence establishments; and military-specific offences. Defence's 2024–25 Annual Report stated that it received 1,196 unacceptable behaviour complaints (an increase of less than one per cent from 2023–24), 215 sexual offence allegations (an increase of 29 per cent from 2023–24), and 333 fraud allegations during 2024–25 (a decrease of nine per cent from 2023–24).

Legislative and policy framework

1.3 APS personnel and ADF members are subject to different legislative frameworks and conditions of employment and service. Key differences include the below.

- APS personnel — the *Public Service Act 1999*, which establishes the APS Code of Conduct framework and requires agencies to have written procedures for determining whether an APS employee has breached the APS Code of Conduct.[6]
- ADF members — the *Defence Act 1903* and *Defence Force Discipline Act 1982* (DFDA), which forms part of the military justice system and establishes military-specific offences, such as absence without leave or disobeying a lawful command (see paragraphs 1.5–1.8).

1.4 Other laws and policy frameworks set out the obligations for Australian Government entities conducting investigations (which are applicable to both ADF members and APS personnel), including the following:

- 2022 Australian Government Investigations Standard (AGIS) — provides a principles-based standard for Australian Government entities conducting 'administrative, civil, or criminal (type) investigations';

4 Department of Defence, *Defence Annual Report 2024–25*, Defence, Canberra, p. 119, October 2025, available from https://www.defence.gov.au/sites/default/files/2025-10/Defence-Annual-Report-2024-25.pdf [accessed 31 March 2026].

5 Unacceptable behaviour is defined in Defence's Complaints and Alternative Resolutions Manual as 'unreasonable conduct at work or in any situation that may be connected to Defence that is offensive, belittling, abusive or threatening to another person or adverse to morale, discipline or workplace cohesion.'

6 The APS Code of Conduct is set out in section 13 of the *Public Service Act 1999* and sets standards for the behaviour and conduct of APS employees.
Australian Public Service Commission, *APS Code of Conduct*, APSC, Canberra, 10 May 2022, available from https://www.apsc.gov.au/working-aps/integrity/integrity-resources/code-of-conduct [accessed 11 February 2026].

- Public Governance, Performance and Accountability Rule 2014 (PGPA Rule) — requires entities to have 'an appropriate mechanism for investigating or otherwise dealing with' suspected or actual incidents of fraud or corruption[7];
- *Public Interest Disclosure Act 2013* (PID Act) — requires entities to investigate disclosures if they meet relevant criteria[8];
- Protective Security Policy Framework (PSPF) — requires that 'Procedures are developed, implemented and maintained to investigate security incidents in accordance with the principles of the Australian Government Investigations Standards'[9];
- *Government Procurement (Judicial Review) Act 2018* — sets out obligations for Commonwealth entities to investigate complaints made about procurements undertaken by that entity; and
- Commonwealth Fraud and Corruption Control Framework 2024 — established under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and requires entities to establish and document criteria for making decisions at critical stages in suspected fraud and corruption incidents and to consider referring matters to the Commonwealth Director of Public Prosecutions (CDPP) in cases where an investigation gathers enough evidence to substantiate a criminal charge.[10]

Military justice system

1.5 The military justice system is a legal framework underpinning Defence military discipline and command structures. It is critical to maintaining command, reputation, retaining people and operational effectiveness while complying with Commonwealth laws (see paragraphs 1.3–1.4).[11] It 'seeks to achieve an appropriate balance between the right of commanders to maintain good order and discipline in the ADF, and the rights of individual ADF members'.[12] While it is applicable to ADF members, APS personnel can be involved in military justice proceedings. The military justice system is complex and is separated into the 'discipline system' and 'administrative system', see Figure 1.1.

7 The PGPA Rule is established under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). The PGPA Act requires that entities are governed in a manner that is 'not inconsistent' with Australian Government policies, such as AGIS.
Department of Finance, *PGPA legislation, associated instruments and policies*, Finance, Canberra, available from: https://www.finance.gov.au/government/managing-commonwealth-resources/pgpa-legislation-associated-instruments-and-policies [accessed 11 February 2026].

8 For a disclosure to be dealt with under the PID Act, it must relate to conduct by a Commonwealth entity, public official or contracted service provider and must constitute 'disclosable conduct'. The full list of disclosable conduct is outlined in section 29 of the PID Act.
Australian Government, *Federal Register of Legislation, Public Interest Disclosure Act 2013*, available from https://www.legislation.gov.au/C2013A00133/latest/interactions [accessed 11 February 2026].

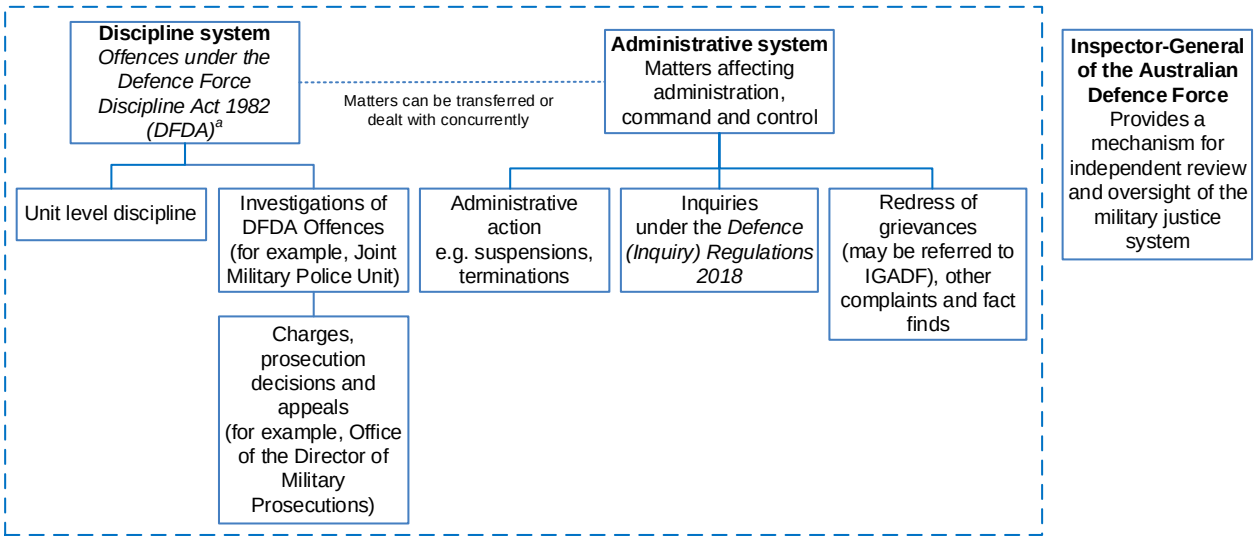
9 The PSPF prescribes what Australian Government entities must do to protect their people, information and resources. It is underpinned by the PGPA Act requirements.

10 Australian Government, *Commonwealth Fraud and Corruption Control Framework 2024,* Commonwealth Fraud Prevention Centre, Canberra, March 2024, available from https://www.counterfraud.gov.au/library/framework-2024 [accessed 11 February 2026].

11 Department of Defence, *Military justice system*, Defence, Canberra, available from https://www.defence.gov.au/about/governance/military-justice-system [accessed 9 April 2026].

12 A commander within the ADF exercises lawful authority over subordinates by virtue of rank or assignment.

Figure 1.1: Military justice system — applicable to ADF members



Note a: Under the *Defence Force Discipline Act 1982*, the discipline system may also deal with offences under other legislation, including the *Crimes Act 1914* and *Criminal Code Act 1995.*

Source: Adapted from Defence documents.

1.6 The 'discipline system' is governed by the *Defence Force Discipline Act 1982* (DFDA) and provides a framework for the investigation and prosecution of offences. DFDA offences include military-specific offences, such as absence without leave or disobeying a lawful command, as well as conduct that may also be an offence under other Commonwealth laws, such as fraud and assault.

1.7 The 'administrative system' is governed by the Defence (Inquiry) Regulations 2018 and Defence Regulation 2016[13], which allows commanders and supervisors to manage performance and conduct. It includes administrative inquiries, administrative action[14], and mechanisms for ADF members to seek review or redress of decisions.

1.8 Use of the administrative system is not limited to specific offences and is based on the discretion of commanders. Conduct dealt with under the administrative system may also constitute an offence under the DFDA or other Commonwealth laws and may be dealt with concurrently or separately through the discipline system or outside the military justice system.

Defence administrative arrangements

1.9 Defence has developed Administrative Policy Arrangements, which establish the authority and hierarchy for Defence documents under Commonwealth policies. Accountable Authority Instructions and other enterprise-level instructions prescribe the conduct of Defence personnel and confer powers, functions and duties. Enterprise-level policies and manuals are issued under these arrangements. Instructions and policies issued at the Service, Group and Defence Investigative Authority (DIA) level are subordinate to enterprise-level policies and manuals. This hierarchy and its

13 These regulations are established under the *Defence Act 1903.*

14 Administrative action may include: suspension from duty with or without pay; formal warnings; corrective training; termination of service; change of employment category; denying or delaying of promotions; removal from an appointment or locality; and recommendations to the Australian Government Security Vetting Agency regarding a person's security clearance, which may in turn affect their service.

relationship to key documents referred to throughout this report is outlined in Appendix 3 and broadly covers both ADF members and APS personnel.

1.10 The Defence Fraud and Corruption Control Plan 2024–26 outlines Defence's approach to the prevention, detection and response to fraud and corruption.[15] It identifies the key fraud and corruption risks for Defence including: fraudulent behaviour in relation to procurement and contracting activities; fraudulent claims for entitlements and allowances; and theft, misuse or misappropriation of Defence assets and information.

Defence investigations, inquiries and fact-finding activities

1.11 Investigations within Defence are conducted by four DIAs, established under the Defence Instruction (see paragraphs 2.16–2.18) that sets out requirements for incident reporting and management.

- Investigations and Public Interest Disclosures Branch (IPIDB) — part of the Defence Integrity Division.
- Joint Military Police Unit (JMPU)[16] — part of the Joint Support Services Division.
- Security Threat and Assurance (STA) Branch — part of the Defence Security Division.
- Human Resources Services Branch — part of the People Services and Wellbeing Division.

1.12 The Defence Instruction requires that 'all Defence personnel who have a reasonable suspicion that a notifiable incident has occurred, must immediately report the incident to a Defence Investigative Authority'. Notifiable incidents are defined in the Defence Instruction (see paragraph 2.9) and, at a summary level, include: criminal offences; fraud, corruption and conflicts of interest; security breaches; deaths or injury associated with Defence activity; and breaches of laws or rules of armed conflict, human rights, or international law. This audit includes examination of the handling of notifiable incidents through Defence's investigative framework.

1.13 Defence has established the Defence Procurement Complaints Scheme (DPCS) within the Capability Acquisition and Sustainment Group (CASG) to manage procurement-related complaints, including those made under the *Government Procurement (Judicial Review) Act 2018* (see paragraphs 2.46–2.50). The DPCS operates alongside other Defence complaint handling mechanisms, including privacy, reviews of action for APS personnel in relation to employment decisions, human rights, aircraft noise, and work health and safety. This audit refers to DPCS as relevant evidence emerged during the course of the audit. Other complaint handling mechanisms were not referred to.

1.14 Defence's investigation framework operates as a system-of-systems, where matters may involve multiple authorities over their lifecycle. Matters may be referred between DIAs and Defence has mechanisms to refer matters to, or partner with, external entities, including the Australian

15 Department of Defence, *Defence Fraud and Corruption Control Plan 2024–26*, Defence, Canberra, September 2024, available from https://www.defence.gov.au/sites/default/files/2024-10/DefenceFraudandCorruptionControlPlan2024-26.pdf [accessed 11 February 2026].

16 JMPU was established in March 2018, with the Australian Defence Force Investigative Service (ADFIS) amalgamated into JMPU in January 2020. Prior to this transition, each Service maintained its own military police and investigative elements. Navy and Army have retained some Service-specific policing functions and JMPU's remit extends beyond investigations to provide the ADF's integrated joint policing and law enforcement capability.

Federal Police (AFP), state and territory police, the National Anti-Corruption Commission (NACC) and the Commonwealth Director of Public Prosecutions (CDPP).

1.15 The role of the Inspector-General of the Australian Defence Force (IGADF) is established under the *Defence Act 1903.* It provides the Chief of the Defence Force (CDF) with a mechanism for internal review of the military justice system (see paragraphs 1.5–1.8) and an avenue through which failures and deficiencies in the system can be exposed and examined, 'independent of the ordinary chain of command'. The Inspector-General is an independent statutory official appointed by the Minister for Defence. The IGADF is not recognised as a separate Commonwealth entity under the PGPA Act, is appropriated by Defence and is administratively located under the CDF in Defence's organisation structure.

1.16 Functions of the IGADF include:

- inquiring into or investigating matters concerning the military justice system;
- conducting performance reviews and audits of the military justice system;
- advising on matters concerning the military justice system, including making recommendations for improvements;
- promoting military justice values across the Defence Force; and
- inquiring into or investigating a matter concerning the ADF as directed by the CDF or Minister.[17]

1.17 These functions are supported by the Inspector-General of the Australian Defence Force Regulation 2016, which provides for the IGADF to:

- inquire into the death of an ADF member, where the death appears to have arisen out of, or in the course of, the member's service in the ADF;
- inquire into ADF member complaints under the Redress of Grievance Scheme;
- inquire into or investigate complaints relating to ADF military police[18]; and
- advise on, or determine, the procedure for handling complaints relating to ADF military police, including conducting audits of the implementation of the complaint-handling procedure.[19]

1.18 The IGADF, through its Directorate of Inquiries and Investigations, conducts investigations and inquiries into alleged offences by ADF military police, as well as inquiries into reported failures of military justice.

17 Three inquiries were recorded as being conducted at the request of the CDF between 1 January 2020 and 30 June 2025, covering the provision and administration of medical care to ADF members and 'unacceptable behaviour'. Between 1 January 2020 and 11 February 2026, the IGADF has not been directed or requested by the Minister for Defence to conduct an inquiry.

18 The Inspector-General of the Australian Defence Force Regulation 2016 uses the term 'service police'. The ANAO has used the term 'ADF military police' to reflect the terminology used by Defence in practice.

19 IGADF advised the ANAO in February 2026 that it does 'not specifically audit the implementation or compliance with the complaint handling procedure'.

1.19 In addition to inquiries conducted by the IGADF, inquiries within Defence may be conducted by 'Inquiry Officers' or 'Commissions of Inquiry', as an administrative component of the military justice system into 'matters concerning the Defence Force' as directed by the Minister, the CDF or the Secretary and CDF acting jointly, or their delegates.[20]

1.20 Investigations, inquiries and fact-finding activities serve distinct purposes and are subject to different requirements.

- Investigations are intended as a focused, evidence-based process to examine instances where misconduct, or a criminal or a service offence may have occurred. The purpose of an investigation is to establish facts relevant to potential culpability to support criminal, disciplinary or administrative action.
- An inquiry is an administrative mechanism designed to understand events, decisions, systemic issues, or organisational risks. The emphasis in inquiries is on making recommendations to enable learning, accountability, and prevention rather than to determine culpability.
- Fact-finding activities are conducted to support administrative decision-making, which are established within Defence policy and are not legislated.[21]

1.21 Investigations, inquiries and fact-finding activities may make adverse findings against individuals or entities. Actions Defence may take in response to adverse findings include: taking action against ADF members under the disciplinary and/or administrative elements of the military justice system; the recovery of fraud-related debts; imposing sanctions against APS personnel under the *Public Service Act 1999*[22]; referring matters to (or working in partnership with) law enforcement agencies, intelligence agencies, the NACC, other Commonwealth departments, and/or the CDPP for potential prosecution; other administrative action, such as the provision of counselling and training; and no further action.

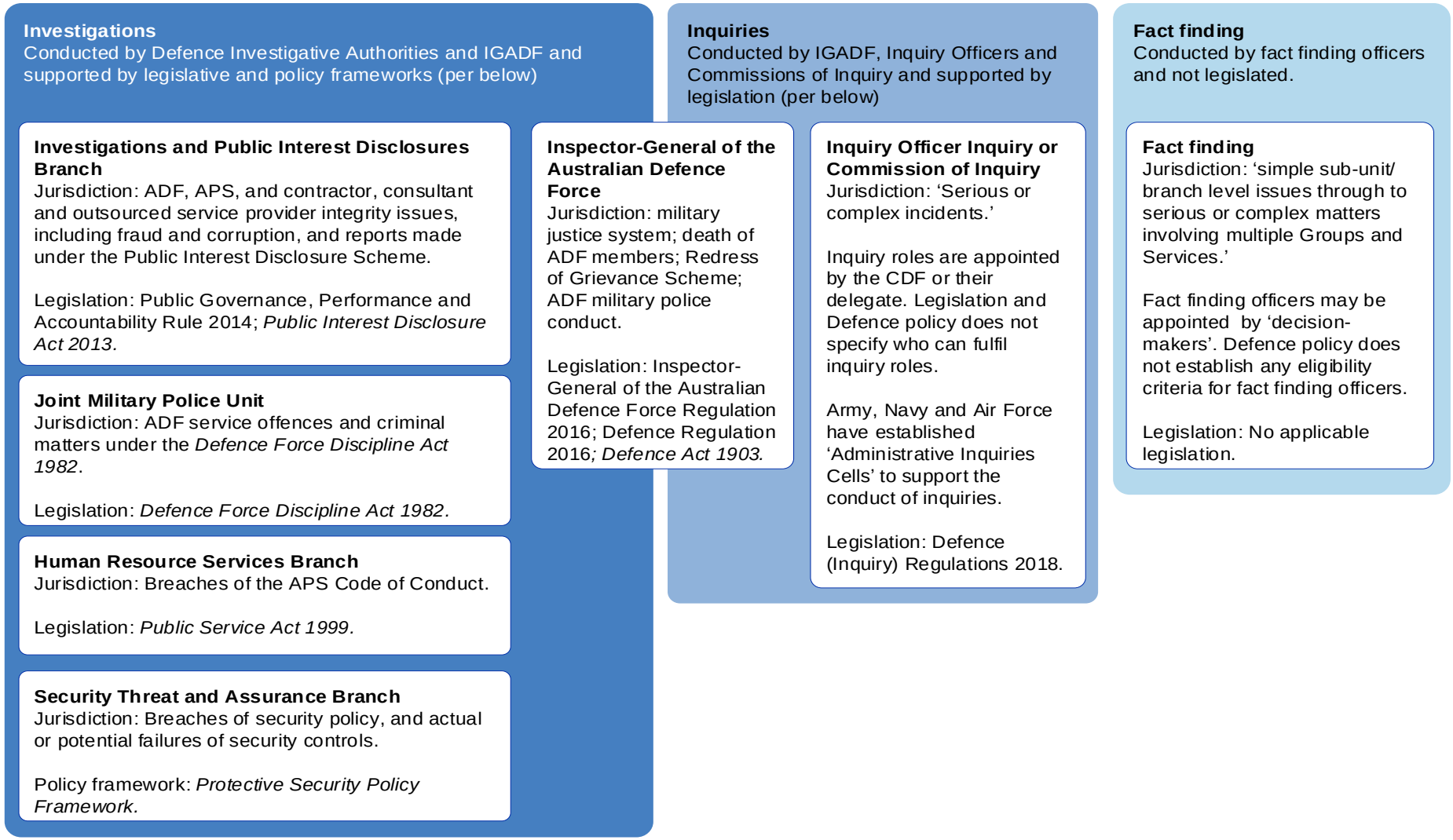
1.22 Figure 1.2 outlines Defence's arrangements for investigations, inquiries and fact-finding activities. This shows the complexity of Defence's investigations and inquiries arrangements and that different legislation and policies apply depending on the nature of a matter, including whether it is applicable to APS personnel or ADF members.

20 Inquiry Officer Inquiries and Commissions of Inquiry are conducted under the Defence (Inquiry) Regulations 2018 to 'facilitate the making of decisions relating to the Defence Force'. Commissions of Inquiry may be appointed by the Minister, CDF, or CDF and Secretary acting jointly, while Inquiry Officer Inquiries are appointed by the CDF.

21 Defence's *Good Administrative Decision-Making Manual* (discussed further at paragraphs 2.30–2.33) states that 'Legislation that empowers the decision-maker to act on 'reasonable suspicion' or on the basis of a "reasonable belief" … may create an implied duty to fact find.'

22 Sanctions can include: termination of employment; reduction in employment classification; reduction in salary; re-assignment of duties; and reprimands.

Figure 1.2: Defence investigations, inquiries and fact-finding activities

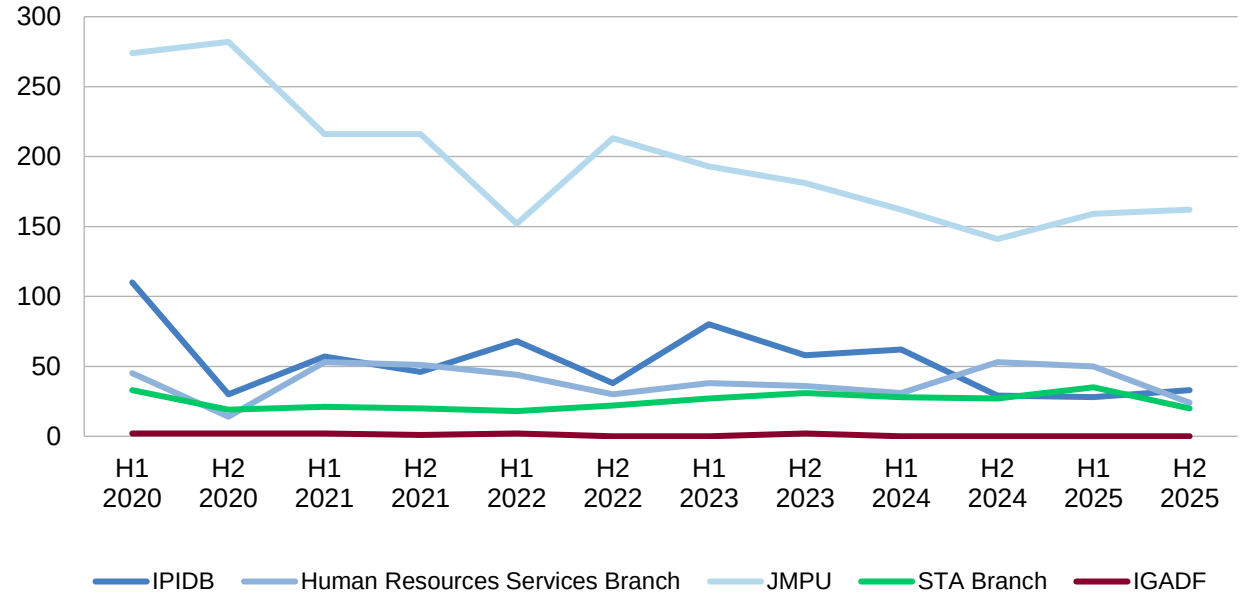


Source: ANAO analysis of Defence documentation.

1.23 Figure 1.3 outlines the volume of commenced investigations recorded by DIAs in Defence case management systems, aggregated into six-monthly periods, between 1 January 2020 and 31 December 2025. As discussed at paragraph 3.14, limitations in case management system performance and reporting have affected Defence's ability to provide the ANAO with comprehensive data on reported incidents and investigations across Defence for the audit period (1 January 2020 to 31 December 2025).

1.24 For three DIAs (Human Resources Services Branch, IPIDB, and STA Branch) and the IGADF, the volume of investigations recorded has remained relatively stable over the period. Investigations recorded by JMPU have decreased since 2020.[23]

Figure 1.3: Volume of investigations, 1 January 2020 to 31 December 2025



Note: The figures for the IGADF only include DFDA investigations conducted by IGADF's Directorate of Inquiries and Investigations. The IGADF advised the ANAO in May 2026 that the Directorate of Inquiries and Investigations, 'normally conducts 1-3 investigations into service police members each year'. Figure 1.3 excludes 120 inquiries commenced by the Directorate of Inquiries and Investigations between 1 January 2020 and 11 December 2025.

Source: ANAO analysis of Defence data.

Reviews into Defence investigations and inquiries

Royal Commission into Defence and Veteran Suicide

1.25 The Royal Commission into Defence and Veteran Suicide was established on 8 July 2021 to examine systemic issues and risks relevant to suicide behaviours of serving and ex-serving Defence members. On 9 September 2024, the Commission's final report was published and highlighted issues within Defence relating to the 'fairness, transparency and rigour of internal investigative

23 Defence advised the ANAO in March 2026 that case management system constraints 'limit the depth and precision of data analysis that can be undertaken. These system limitations have affected the ability to efficiently extract, filter and compare data sets, thereby restricting the level of trend analysis and insights that can be generated from retrospective information.' JMPU annual reporting has noted that the reduction in investigations aligns with the introduction of COVID lockdowns during 2020–21 as well as a 'broader stabilisation' following the disruptions caused by lockdowns.

processes', the potential weaponisation of the military justice system by commanders, and a failure to use available data to assess risks to current and former ADF members.[24]

1.26 The report made 122 recommendations, including: improving support for victims of sexual misconduct; conducting reviews into sexual violence and the effectiveness of the military justice system; improving training for the conduct of fact-finds and inquiries; IGADF staff skills and qualifications; and updating and publishing IGADF quality assurance and timeliness measures.

1.27 The Australian Government agreed or agreed-in-principle to 104 recommendations, with Defence taking carriage, jointly or solely, of 76 recommendations. As at February 2026, Defence documentation indicates it has implemented 21 recommendations. Recommendations relevant to investigations, and Defence's progress in implementing them, are outlined in Appendix 4. IGADF advised the ANAO in November 2025 that the implementation of recommendations relating to them are being considered by the Australian Government alongside recommendations of the IGADF twenty-year review.

IGADF twenty-year review

1.28 In September 2023, the Australian Government approved the conduct of a review into the arrangements and composition of the IGADF, twenty years after the IGADF's establishment in January 2003. In September 2024, the government released the 'twenty-year review' of the IGADF and included recommendations aimed at strengthening the IGADF's inquiry powers and enhancing the IGADF's independence.[25]

Commonwealth Ombudsman

1.29 In December 2023, the Commonwealth Ombudsman released its report *Does Defence handle unacceptable behaviour complaints effectively?*[26] The report found that options for making complaints outside of the chain of command were limited and that complex policies and lack of training presented a risk that complaints are handled unfairly and inconsistently.

1.30 The report made nine recommendations aimed at improving complaints handling processes, improving training and communication, and addressing potential bias and conflicts of interest. Defence advised the ANAO in March 2026 that the Complaint, Resolution and Support Services (CRSS) unit, which sits within the Human Resources Services Branch, became operational in January 2026 'as a whole of enterprise mechanism for receiving complaints of unacceptable behaviour' and for providing Defence personnel with 'additional options to lodge complaints

24 Royal Commission into Defence and Veteran Suicide, *Final Report*, September 2024, available from https://defenceveteransuicide.royalcommission.gov.au/publications/final-report-all-volumes [accessed 11 February 2026].
In addition to the Royal Commission, a December 2024 NSW coronial inquest made criticisms of an IGADF inquiry conducted into the death of an ADF member, including that the inquiry did not appear to seek relevant expert advice and stated that it was not clear that the inquiry was 'designed to engage in any particularly critical process of self-reflection' of how the ADF handled the matter.

25 Office of the Inspector-General of the Australian Defence Force, *Twenty-year review of the Office of the Inspector-General of the Australian Defence Force*, IGADF, Canberra, March 2024, available from https://www.igadf.gov.au/system/files/2025-06/IGADF%20Twenty-Year%20Review%20Report%20-%20with%20enclosures_0.pdf [accessed 11 February 2026].

26 Commonwealth Ombudsman, *Does Defence handle unacceptable behaviour complaints effectively?,* Ombudsman, Canberra, December 2023, available from https://www.ombudsman.gov.au/__data/assets/pdf_file/0016/302191/Defending-Fairness-Does-Defence-handle-unacceptable-behaviour-complaints-effectively.pdf [accessed 17 February 2026].

outside their chain of command or reporting line, including the ability to submit complaints anonymously'.

Rationale for undertaking the audit

1.31 An effective investigation function supports integrity, transparency and accountability, and assists in safeguarding the wellbeing of impacted individuals. The Senate Foreign Affairs, Defence and Trade Legislation Committee[27] has raised concerns regarding Defence investigations, inquiries and fact-finding activities at previous hearings. A summary of key themes includes:

- timeliness and robustness of investigative processes;
- decisions to prosecute personnel and contracted companies for fraudulent conduct;
- potential repercussions against people reporting incidents within Defence;
- conduct and recording of fact-finding;
- wellbeing of victims involved in investigations; and
- extent to which the IGADF has been subject to previous ANAO scrutiny.[28]

1.32 Previous ANAO audits have identified deficiencies in the way Defence handles procurement and contractor integrity issues, including not identifying and reporting notifiable incidents.[29]

Audit approach

Audit objective, criteria and scope

1.33 The audit objective was to assess the effectiveness of the Department of Defence's administration of investigations.

1.34 To form a conclusion against this objective, the following high-level criteria were adopted:

- Has Defence established fit-for-purpose arrangements for the conduct of investigations?
- Has Defence effectively implemented its arrangements for investigations?

1.35 The audit examined the handling of reported incidents through Defence's investigations and inquiries framework. The audit scope included examination of relevant current and historic Defence policies and guidance for APS and ADF investigations, inquiries and fact-finding activities. It also included case study examination of closed investigations conducted by DIAs and closed inquiries and investigations conducted by the IGADF between 1 January 2020 and 31 December 2025.

27 Parliament of Australia, *Senate Standing Committees on Foreign Affairs Defence and Trade,* Australian Government, Canberra, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade [accessed 25 March 2026].

28 In June 2023, Senator Jacqui Lambie wrote to the Auditor-General requesting a performance audit be conducted into the effectiveness and efficiency of the IGADF. Further correspondence from Senator Lambie was received in October 2023, November 2023 and October 2024. Senator Lambie's correspondence, and the Auditor-General's responses are available at https://www.anao.gov.au/work/request/audit-of-the-inspector-general-of-the-australian-defence-force.

29 For example, see Auditor-General Report No.50 2024–25 *Department of Defence's Sustainment of Canberra Class Amphibious Assault Ships (Landing Helicopter Dock),* paragraphs 3.55–3.68, available from https://www.anao.gov.au/work/performance-audit/department-of-defence-sustainment-of-canberra-class-amphibious-assault-ships-landing-helicopter-dock [accessed 24 May 2026].

- Fraud value was used as a selection metric for investigation case studies, as it enabled a comparison of similar cases across DIAs and the IGADF and supported assessment of how matters that may cross jurisdictional boundaries are referred and consulted on.
- Timeliness was used as a selection metric for the IGADF inquiry case study.

1.36 Other mechanisms, including fact-finding processes, complaints made through Defence complaints handling pathways, and inquiries conducted under the Defence (Inquiry) Regulations 2018, were considered where relevant to an investigation or notifiable incident reporting processes. The audit did not examine Redress of Grievance processes or inquiries into the deaths of ADF members, conducted through the IGADF's Directorate of Select Incident Review.

Audit methodology

1.37 The audit methodology included discussions with relevant Defence officials and an examination and analysis of Defence records. The audit was open to contributions from the public.

1.38 The ANAO has cooperative evidence gathering arrangements in operation with entities. Defence advised the ANAO on 15 November 2024, at the commencement of audit fieldwork, that it was unable to provide certain information to the ANAO on a cooperative basis due to legislative restrictions. On 6 December 2024, the Auditor-General issued two separate notices to Defence including one to the Secretary of Defence and the CDF, and another to the IGADF to provide information pursuant to section 32 of the *Auditor-General Act 1997*. This enabled Defence to provide access to information taking account of legislative requirements. Following receipt of the notices, Defence provided the ANAO with access to relevant information.

1.39 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $952,000.

2. Arrangements for the conduct of investigations

Areas examined

This chapter examines whether the Department of Defence (Defence) has fit-for-purpose arrangements in place for the conduct of investigations.

Conclusion

Defence has partly effective arrangements in place for the administration of investigations. Defence's investigations framework does not clearly align its different investigation functions or enable them to work together effectively, including referrals between Defence Investigative Authorities (DIA). As a result, investigations may not be managed in a consistent or coordinated way, creating a risk that responses are not timely, fair, or proportionate.

Defence has not established an enterprise-wide approach to investigative jurisdictions, including clear referral pathways between investigative authorities and safeguards for the management of incidents by Defence investigative functions. Defence cannot assure that incidents are directed to the most appropriate DIA or that the same incident would receive the same outcome regardless of the reporting pathway. Defence has not complied with Australian Government Investigations Standard (AGIS) requirements for investigators to hold qualifications.

Areas for improvement

The Australian National Audit Office (ANAO) made four recommendations aimed at: clarifying DIA and the Inspector-General of the Australian Defence Force (IGADF) jurisdictions and processes for the management of reported incidents; establishing clear and consistent arrangements for managing procurement-related complaints upon establishment of the new Defence Delivery Agency; reviewing and updating DIA-level guidance and establishing review requirements at an enterprise-level; and documenting investigator qualifications.

2.1 Fit-for-purpose investigation frameworks support the consistent management of reported incidents, promote proportionate and fair investigation outcomes, and reduce the risk of investigative processes being misused.

2.2 Commonwealth legislation and policies require entities to have arrangements in place to conduct investigations. The 2022 Australian Government Investigations Standard (AGIS) sets out whole-of-government requirements for investigations. The AGIS defines an investigation as 'an activity to collect information or evidence to a particular standard of proof related to an alleged, apparent or suspected breach'.[30] AGIS standards are not applied to the conduct of inquiries.

30 This definition expanded on the 2011 AGIS definition which defined investigations as 'a process of seeking information relevant to an alleged, apparent or potential breach of the law, involving possible judicial proceedings.'

Has Defence established an appropriate framework for managing investigations?

Defence has established requirements for notifiable incidents to be reported to a DIA. There is overlap between the roles of DIAs, and the conduct of fact-findings and inquiries. Reporting pathways for notifiable incidents are not always aligned with Defence policies and rely on judgement. This creates a risk that reported incidents are not managed equitably and proportionately, or with the appropriate level of DIA oversight.

2.3 As shown in Figure 2.1, between April 2005 and June 2025, Defence established key enterprise-level documents to support the conduct of investigations, administrative inquiries and fact-finding.

Figure 2.1: Timeline of enterprise-level documents

Source: ANAO analysis of Defence documentation.

2.4 Key enterprise-level documents detailing the arrangements for investigations, administrative inquiries and fact-finding have different accountable officers assigned. For example:

- Defence Instructions ADMIN 45-4 Defence Investigation Standards (see paragraph 2.19) and FIN 12-1 The Control of Fraud in Defence and the Recovery of Public Moneys (see paragraph 2.15) were established by the Secretary and Chief of the Defence Force (CDF);
- 2026 Defence Instruction (see paragraphs 2.16–2.18) outlines the Deputy Secretary Governance as the 'accountable officer' for incident reporting and management;
- Incident Reporting and Management Manual (Edition 2) and the Interim Incident Reporting and Management Policy (see paragraphs 2.13–2.15) were issued by the First Assistant Secretary Defence Integrity (or their equivalent at the time);

- Complaints and Alternative Resolutions Manual (CARM) is managed by the Defence People Group, with individual chapters allocated different sponsors including the Assistant Secretary Human Resources Services Branch, the Inspector-General of the Australian Defence Force (IGADF), the Director of Complaints and Resolution, and the Sexual Misconduct Prevention and Response Office (SeMPRO);
- Defence Investigations Standards Manual (see paragraphs 2.19–2.21) was sponsored by the Provost-Marshal of the Australian Defence Force (PM-ADF)[31]; and
- Good Administrative Decision-Making Manual (see paragraphs 2.30–2.33) is issued by the Chief Counsel.

Investigations

2.5 Framework documents do not clearly establish the role and jurisdiction of DIAs at an enterprise level. Defence's investigative framework is complex, supported by different processes for each DIA, and different legislative frameworks applicable to Australian Defence Force (ADF) members and Australian Public Service (APS) personnel. As a result, lack of jurisdictional clarity, alignment and interoperability could present risks to equitable treatment of similar matters across DIAs.

2.6 The *Defence Act 1903* establishes the functions of the IGADF, and the 2026 Defence Instruction sets out how incidents are to be reported and managed by the four DIAs. Table 2.1 outlines the jurisdiction of the four DIAs and IGADF as established in legislation, enterprise-level documents and supporting DIA-level documents.

Table 2.1 DIA and IGADF jurisdictions and legislation

Investigative entity	Key areas of responsibility
Investigations and Public Interest Disclosures Branch (IPIDB)	Investigations, reviews and assessments of: • allegations of fraud and corruption in or affecting Defence; • potential offences under the *Defence Act 1903*; • allegations of serious misconduct, lack of probity, commercial impropriety, collusive tendering, conflicts of interest, and corrupt conduct committed by or involving Defence personnel where there is a nexus to the activities or operations of Defence; and • reports made to the Defence Public Interest Disclosure (PID) Scheme. These responsibilities are outlined in Accountable Authority Instruction 1.
Joint Military Police Unit (JMPU)	Investigation of offences under the *Defence Force Discipline Act 1982* (DFDA) applicable to ADF members, such as absence without leave or disobeying a lawful command, and criminal matters, including ADF member fraud and sexual misconduct within Defence. Investigation of 'major security incidents' with agreement from STA Branch. These responsibilities are outlined in JMPU's Military Police Manual (see paragraphs 2.60–2.66).

31 The PM-ADF serves as the Commander of the Joint Military Police Unit (JMPU) and exercises authority over Defence service policing capabilities.

Investigative entity	Key areas of responsibility
Human Resources Services Branch	Investigation of suspected breaches of the APS Code of Conduct, including sexual harassment, violence, bullying, fraudulent use of Defence Travel Cards and inappropriate access to Defence information. Inappropriate access to Defence information may also represent a breach of the Defence Security Principles Framework (DSPF) and requires reporting to the Security Threat and Assurance Branch. These responsibilities are outlined in Defence's Code of Conduct Policy and Procedures, and supporting Code of Conduct Policy guidance.
Security Threat and Assurance (STA) Branch	Investigations of actual or suspected breaches of security policy, and actual or potential failures of security controls. The DSPF defines 'security incidents' to include 'Unauthorised access to and/or use of Defence information and communications equipment or systems' and requires that security incidents must be reported to the Security Incident Coordination Centre, within the STA Branch. These responsibilities are outlined in STA Branch's Security Investigation Operating Guidelines and the DSPF (see paragraphs 2.51–2.59).
Inspector-General of the Australian Defence Force (IGADF)	• Investigating or inquiring into matters concerning the military justice system. • Inquiring into the death of an ADF member, where the death appears to have arisen out of, or in the course of, the member's service in the Defence Force. • Inquiring into complaints made by ADF members under the Redress of Grievance scheme. • Investigating or inquiring into complaints relating to ADF military police. • Advising on, or determining, the procedure for handling complaints relating to ADF military police, including conducting audits of the implementation of the complaint-handling procedure. Complaints raised with the IGADF may include matters related to fraud. These responsibilities are outlined in the *Defence Act 1903* and Inspector-General of the Australian Defence Force Regulation 2016.

Source: ANAO analysis of Defence documentation.

2.7 Jurisdictions set out in Defence enterprise-level and DIA-level documents are unclear and overlap responsibility areas, including for matters of sexual misconduct, fraud and security. For example: inappropriate access to Defence ICT systems may fall under the jurisdiction of STA Branch or the Human Resources Services Branch; and fraudulent use of Defence Travel Cards by APS personnel may fall under the jurisdiction of IPIDB or the Human Resources Services Branch. This means that similar matters may be dealt with under different DIAs, increasing the risk that matters are not handled equitably and proportionately. Neither the Defence Instruction or other enterprise-level policies clearly define the jurisdictions or responsibilities of the four DIAs, or how they work together to assess or triage incidents. As discussed at paragraph 3.101, ANAO review of investigation case studies identified that DIAs do not always sufficiently consult with each other or with relevant authorities.

2.8 A September 2020 management initiated review conducted by Synergy on Defence's investigative functions found that challenges in coordination between DIAs and overlapping jurisdictions led to duplication of effort, and impacts to investigation timeliness and effectiveness of outcomes. The review identified five improvement opportunities, including: the implementation

of a centralised integrity investigations function to incorporate all DIAs and standardise Defence investigation processes; and the establishment of an investigation review committee to conduct an initial assessment of matters being considered for investigation, improve information sharing between DIAs, reduce the need for investigations being transferred between DIAs, and improve the identification of emerging risks or trends. Defence advised the ANAO in March 2026 that it implemented three of the five improvement opportunities. It did not implement a centralised investigative function or an investigation review committee.

Notifiable incidents

2.9 The Defence Instruction establishes a definition of notifiable incidents. Definitions of notifiable incidents established in other enterprise-level and DIA-level documents do not align with the Defence Instruction and are subject to judgement. The Defence Instruction requires that 'Defence personnel who have a reasonable suspicion that a notifiable incident has occurred, must immediately report the incident to a Defence Investigative Authority'. Box 1 sets out how the Defence Instruction defines notifiable incidents.

Box 1: Notifiable incidents

Any incident that:

- raises a reasonable suspicion that a criminal offence may have been committed under the criminal law of the Commonwealth, States or Territories, or the criminal law of another country;
- raises a reasonable suspicion that a serious offence has been committed under the Defence Force Discipline Act 1982, not including incidents that are regarded as minor (Schedule 1A offences), which would ordinarily be dealt with by a commanding officer or under the Disciplinary Infringement Scheme;
- involves allegations of fraud, corrupt practices or behaviour, including suspected serious or systemic corruption that engages Defence's mandatory referral obligations to the National Anti-Corruption Commission, collusive tendering, or a lack of probity involving Commonwealth resources, including Defence personnel, property or premises;
- involves undisclosed or mismanaged conflicts of interest;
- is a suspected security incident whether intentional, negligent or accidental, resulting in a failure to comply with a security requirement outlined in the Defence Security Principles Framework or that may impact on a clearance holder's suitability to hold a security clearance;
- involves a death, serious injury, illness, disappearance or a dangerous incident of Defence personnel or non-Defence personnel involved in any Defence activity, or at any Defence property or premises (even where there may be no reasonable suspicion of an offence having been committed);
- is deemed by a manager or a commander to be serious, sensitive or urgent, not covered by the definitions above. That is, one that may bring Defence into disrepute; attract adverse media or parliamentary attention; or may adversely affect the efficiency of Defence, or impact operational effectiveness or capability; and

- are Prescribed Serious Operational Incidents which includes acts or allegations of breaches of Laws of Armed Conflict, Rules of Engagement, Targeting Directives, Human Rights or International Law, including those involving foreign units partnered with the Australian Defence Force, and allegations or incidents of Australian Defence Force involvement in civilian casualties.[a]

Note a: Prescribed Serious Operational Incidents were added to the definition of notifiable incidents in June 2023, following completion of the IGADF Afghanistan Inquiry in November 2020, which recommended improvements to the process for reporting breaches of the law of armed conflict.

Source: ANAO analysis of Defence documentation.

2.10 Despite the 2026 Defence Instruction defining a notifiable incident, other Defence documents use different definitions, and its application relies on judgement. For example, the Defence Instruction states that 'minor offences' under Schedule 1A the DFDA are not considered notifiable incidents. These offences include, among others: absence from duty; insubordinate conduct; disobeying a lawful command; intoxicated while on duty; cyber bullying; and prejudicial conduct. Some of these offences may also be treated as 'serious service offences' under the DFDA, which are classified as notifiable incidents under JMPU's Jurisdiction Model (see Table 2.3). Whether an offence is considered minor or serious in nature is ultimately determined at the discretion of relevant commanders. There is merit in Defence establishing and promulgating guidance to commanders to mitigate the risk of inconsistent judgement and discretion, and to support the appropriate referral of relevant incidents to the JMPU.

2.11 Defence's Code of Conduct Policy Guidance states that allegations of 'serious misconduct that warrant immediate referral' to the Human Resources Services Branch include incidents of sexual harassment. This is not consistent with Defence's Complaints and Alternative Resolutions Manual (CARM), which states that 'JMPU is the appropriate Defence Investigative Authority for sexual offences with a Defence nexus. It does not matter whether the complainant or respondent is ADF, APS or a contractor'. The JMPU is responsible for determining and coordinating with the appropriate jurisdiction for the matter. Defence advised the ANAO in March 2026 that it is reviewing its Code of Conduct policy guidance to 'better reflect' the initial notification requirements to JMPU, and that this is anticipated to be completed by the end of June 2026.

Notifiable incident reporting and management

2.12 Since August 2022, key investigation requirements have been removed, including requirements to analyse and report on systemic weaknesses identified through investigations.

2.13 In August 2019, the First Assistant Secretary, Audit and Fraud Control (now known as the First Assistant Secretary Defence Integrity) issued Edition 2 of the Incident Reporting and Management Manual, which required all notifiable incidents to be referred to a DIA.

2.14 In August 2022, this manual was replaced by the Interim Incident Reporting and Management Policy as a temporary measure. The interim policy required managers and commanders to ensure all reported incidents were recorded in a Defence Incident Record and on the Defence Policing and Security Management System (DPSMS) (see paragraph 3.4). It also stated that 'Where an incident is recorded in the Army Incident Management System there is no requirement to raise a Defence Incident Record'. These inconsistent requirements had also been included in Edition 2 of the Incident Reporting and Management Manual and in Army FORCOMD Directive 22-2 Incident Management, Reporting and Recording, released in March 2022.

2.15 The interim policy also replaced Defence Instruction FIN 12-1 The Control of Fraud in Defence and the Recovery of Public Moneys, which was jointly issued by the CDF and Secretary in April 2005.[32]

2.16 In September 2024, the interim policy was replaced by the updated Defence Instruction. Several requirements from Defence Instruction FIN 12-1 and the interim policy were not retained, including requirements for:

- analysis and reporting on patterns of offences and systemic weaknesses in Defence revealed through fraud assessments and fraud investigations;
- annual reporting to the Secretary and CDF on fraud investigation outcomes and trends;
- pursuit of fraud prosecutions in line with the *Prosecution Policy of the Commonwealth*;
- reporting fraud affecting another agency to that agency in line with privacy laws;
- JMPU to provide fraud investigation reports to IPIDB; and
- DIAs to update managers and commanders on the progress of relevant assessments or investigations.[33]

2.17 The Defence Instruction requires incidents reported to managers and commanders to be recorded 'as close to the time of the incident as practicable' in Defence's authorised case management system, the Defence Enterprise Resource Planning Case Management System (DECMS). Prior to being updated in January 2026, the Defence Instruction did not define Defence's authorised case management system.

2.18 The Defence Instruction also includes a link to a Defence intranet site (established in September 2019) that provides reporting links and DIA contact details for reporting incidents such as fraud and corruption, security, breaches of military discipline, Public Interest Disclosures, and procurement complaints.

Defence Investigation Standards Manual

2.19 In June 2009, Defence introduced Defence Instruction ADMIN 45-4 Defence Investigation Standards and a supporting Defence Investigation Standards Manual following a July 2006 audit of ADF Investigative Capability. Defence's 2006 audit, requested by the CDF after multiple reviews and inquiries between 1998 and 2005, identified shortcomings in ADF investigations and found 'considerable variation' in investigation standards between DIAs. The audit recommended that Defence 'adopt a common investigation standard … to be complied with by all Defence Investigative Authorities (DIAs) and their investigators.'

32 Despite a scheduled review date of April 2008, the version of the Instruction FIN 12-1 that was replaced by the interim policy was dated April 2005. The instruction included references to outdated legislation, such as the *Financial Management and Accountability Act 1997* (replaced by *Public Governance, Performance and Accountability Act 2013* in July 2014) and the Commonwealth Fraud Control Guidelines 2002, which were updated in 2011 before being replaced by the Fraud Rule and a Commonwealth Fraud Control Policy with the introduction of the PGPA Act in July 2014.

33 The Royal Commission into Defence and Veteran Suicide noted that regular updates can assist impacted parties in managing stress and anxiety. See, for example, Royal Commission into Defence and Veteran Suicide, *Final Report, Volume 3*, p. 496, September 2024, available from https://defenceveteransuicide.royalcommission.gov.au/publications/final-report-all-volumes [accessed 11 February 2026].

2.20 The Defence Investigation Standards Manual stated it was 'based on the AGIS' and 'not to be confused with, investigation procedures and techniques that will be published elsewhere.' The manual mandated compliance with the AGIS at an enterprise-level and outlined Defence-specific investigation requirements including:

- DIAs to have established written procedures covering engagement with other agencies, the legal and ethical behaviour of staff, and obtaining legal advice;
- DIAs to ensure that their procedures 'clearly articulate the legislation, powers and directives under which they operate'; and
- the Head of each DIA to provide training to ensure that all relevant personnel 'have the appropriate qualifications, knowledge, skills and attitude' required to meet Defence investigation standards.

2.21 The Defence Investigation Standards Manual was not reviewed between its introduction in June 2009 and July 2023 and did not include a scheduled review date.[34] In December 2023, Defence cancelled the manual, citing that '[t]he DIAs now seek to reduce the policy burden, agreeing that the use of the 2022 AGIS is all that is required to underpin their respective investigative requirements and operating procedures.' Since its cancellation, the requirement to comply with the AGIS and the Defence-specific requirements have not been documented at an enterprise level.[35]

Defence Inquiries

2.22 The role of inquiries and fact-finding in relation to notifiable incidents is not clearly established across both enterprise-level and DIA-level documents, presenting a risk that they are conducted without DIA awareness or oversight. As discussed at paragraph 3.93, there were instances where fact-finding activities have been conducted in response to notifiable incidents without the incident being reported to a DIA as required under the Defence Instruction.

2.23 Under the Defence (Inquiry) Regulations 2018, Defence may conduct inquiries to 'facilitate the making of decisions relating to the Defence Force' and to 'assist command in securing the proper functioning of the Defence Force'. The Regulations provide for the establishment of Inquiry Officer Inquiries and Commissions of Inquiry and note that inquiries 'are not about individuals as such and are not an external accountability mechanism.'

2.24 In August 2024, Defence issued edition 4 of its Administrative Inquiries Manual to 'assist commanders to determine whether an inquiry under the Defence (Inquiry) Regulations 2018 is appropriate'.

2.25 The manual outlines factors and safeguards where an inquiry may be appropriate, including the death or serious injury of someone who is not an ADF member, and significant security-related incidents. The manual does not cover investigations conducted under the DFDA, fact-finding, inquiries conducted by the IGADF, or Public Interest Disclosures. The manual is not aligned with the

34 The version of the manual cancelled in December 2023 included references to out-of-date policies and legislation including Defence Instruction Operational 13-04 Release of Classified Defence Information to Other Countries (replaced by the Defence Security Manual in April 2014), the Defence Security Manual (replaced by the *Defence Security Principles Framework* in July 2018), and the *Financial Management and Accountability Act 1997* (replaced by *Public Governance, Performance and Accountability Act 2013* in July 2014).

35 The requirement for DIAs to conduct investigations in accordance with the AGIS was also established in the Defence Security Manual, which was replaced by the Defence Security Principles Framework (DSPF) in July 2018. The DSPF does not include requirements to comply with the AGIS.

requirements of the Defence Instruction. As outlined at Box 1 (see page 29), notifiable incidents that must be reported to a DIA include: any incident that 'involves a death, serious injury … of personnel involved in any Defence activity, or at any Defence premise'; or any incident 'resulting in a failure to comply with … the Defence Security Principles Framework'. The manual does not outline notifiable incidents or require such incidents to be referred to a DIA (see paragraph 2.9).

2.26 The manual states that inquiries conducted under the Defence (Inquiry) Regulations 2018 cannot determine whether a disciplinary or criminal offence has occurred, as doing so may prejudice any later proceedings under the DFDA or criminal law. Where potential criminal conduct is identified, the manual requires the relevant parts of the inquiry to cease and be referred to the Appointing Authority, who determines the next steps.[36] The manual does not require inquiries to be conducted in accordance with the AGIS.

2.27 While the manual requires that Appointing Authorities confirm inquiry officials are free from actual or perceived bias or conflicts of interest it does not mandate that Appointing Authorities themselves are free from bias or conflicts of interest.

Fact-finding activities

2.28 Prior to August 2015, Defence had established a 'Quick Assessment' process to rapidly assess known facts and identify gaps, to inform decisions on how to respond to an incident. Quick assessments were not investigations, were not a pre-cursor to investigations, and were required to be completed within 24 hours.

2.29 In August 2015, Defence replaced the Quick Assessment process with a fact-finding process after a 2014 review found that incidents were attracting 'disproportionate investigative effort'.[37] Defence also introduced the Defence Incident Record system at that time to provide a consistent and high-level summary of incidents, actions taken and recommendations, and were required to be completed within 24 hours of an incident becoming known.

2.30 In July 2022, Defence issued a Good Administrative Decision Making Manual, applicable to APS personnel and ADF members. The manual, updated in March 2026, requires that all notifiable incidents be reported to a DIA prior to conducting a fact-finding and states that, 'Fact-finding into serious or complex incidents (particularly personnel incidents) is generally not appropriate beyond determining sufficient facts to enable immediate actions such as mandatory reporting, risk mitigation and referral to the appropriate authority or specialist area for formal investigation'.[38] Prior to being updated in March 2026, the manual stated that it was not appropriate for fact-finding to be conducted into the 'substantive issues' surrounding notifiable incidents without DIA approval.

36 The Appointing Authority under the Defence (Inquiry) Regulations 2018 includes the Minister, CDF, and Secretary, or their delegates.

37 The 'Rethinking systems of inquiry, investigation, review and audit' review noted that weaknesses associated with the use of non-statutory fact-finding included: a decrease in the range of material that would be exempt from freedom of information requests; Commanders and managers may lack the skills and experience to apply flexibility to fact-finding; and potential conflict of roles and responsibilities between DIAs and the chain of command.

38 STA Branch guidance provides for the conduct of fact-finding into some categories of notifiable incidents without STA Branch engagement (see paragraph 2.53).

2.31 The manual also states that fact-finders 'should seek legal advice if concerned as to the ability to undertake factfinding where an agency is simultaneously asserting jurisdiction over the same matter.' The manual does not prohibit fact-finding into matters of sexual misconduct, but states that the fact-finder should contact the Sexual Misconduct and Prevention Response Office to support appropriate response and victim support arrangements.

2.32 CDF Directive 25/2019 (see paragraphs 2.74–2.75) requires that all ADF military police professional standards matters be subject to fact-finding at the unit level to determine whether further investigation or inquiry action is necessary.

2.33 The manual provides guidance on selecting fact-finding officers but does not require independence or the declaration of conflicts of interest, as per AGIS requirements.[39] It cautions that care should be taken before undertaking or proceeding with any fact-finding where disciplinary or criminal investigation processes are underway, as this may prejudice those proceedings.[40] The manual also states that decision-makers may be required to observe procedural fairness and that failure to do so may require decisions to be set aside and re-made.

2.34 The use of fact-finds to examine notifiable incidents represents a shift from earlier Defence policies and creates a risk that responses to such incidents may lack independence, transparency, or procedural fairness.[41] Fact-finds have historically been treated as an administrative process rather than disciplinary. The expanded scope of the 2022 AGIS now applies to administrative investigations. The application of AGIS to Defence investigations is outlined at Table 2.2.

2.35 Defence has not established a consistent enterprise-level framework for investigations, inquiries and fact-finding activities. Defence's framework does not deliver alignment and interoperability of investigative functions and reporting pathways. The definition of a notifiable incident is contained in the 2026 Defence Instruction. Other Defence documents establish definitions of notifiable incidents that do not align with the Defence Instruction, resulting in inconsistent requirements for referrals to a DIA. The role of fact-finding and inquiries in relation to notifiable incidents is unclear, creating a risk that such matters are examined without DIA awareness or oversight.

39 A similar finding was made in a December 2023 Commonwealth Ombudsman report (see paragraphs 1.29–1.30) which recommended that 'Defence require personnel involved in the handling of a complaint to consider specifically whether a conflict of interest or bias, perceived or actual, exists in relation to the complaint, and keep a written record of this consideration and any accompanying risk mitigation.'

40 Defence's DFDA Law Manual states that 'Information gathered outside a DFDA investigation will be of limited use when charging or trying a service offence.'

41 The Royal Commission into Defence and Veteran Suicide noted evidence which indicated that 'some fact finds have been poorly conducted' and have had 'detrimental impacts' on the wellbeing of Defence members. ANAO observations on the conduct of fact-finding is discussed at paragraphs 3.91–3.95.

Recommendation no. 1

2.36 The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, strengthen enterprise-level guidance to clearly outline the jurisdiction of each Defence Investigative Authority and IGADF and provide for the effective management of reported incidents and investigations.

Department of Defence response: *Agreed.*

Has Defence developed training and guidance to support investigations?

DIAs and the IGADF have established guidance to support investigations. Recognising the complexity of Defence's investigations system, DIA-level guidance does not always establish clear jurisdictions or referral processes between DIAs, or for deciding whether an investigation or inquiry is warranted. This impacts the alignment and interoperability of Defence's investigative functions. Defence has not established enterprise-level arrangements to ensure that investigative and inquiry processes achieve outcomes that are equitable and proportionate to the conduct. Defence guidance has not been regularly reviewed, and Defence does not hold qualification records for all investigators or supervisors involved in investigations. These deficiencies increase the risk that Defence and Commonwealth investigation policies are not consistently applied or complied with.

DIA-level and IGADF processes and guidance

2.37 Not all DIA and IGADF guidance has been regularly reviewed or clearly establishes jurisdictions or referral mechanisms between the DIAs or to the Australian Government Security Vetting Agency (AGSVA). This presents a risk that matters may not be dealt with equitably, proportionately, and in alignment with Defence policies. An overview of DIA-level processes and guidance is outlined at Table 2.2.

Table 2.2: Summary of DIA-level and IGADF processes and guidance

Investigative entity	Document description	ANAO observation	Has Defence mandated AGIS?
Investigations and Public Interest Disclosures Branch (IPIDB)	**Governance documents for matters including:** use of case management systems, decision-making, and the preparation of investigation reports (see paragraphs 2.38–2.45).	Finalised governance documents established between November 2024 and March 2026. As at March 2026, governance documents for incident triage and assessment, investigation interviewing, and evidence management are in draft.	Yes.

Investigative entity	Document description	ANAO observation	Has Defence mandated AGIS?
Security Threat and Assurance Branch (STA Branch)	**DSPF Principle 77 and Control 77.1** outline definitions of security incidents, incident reporting requirements, and incident assessment processes (see paragraphs 2.51–2.59).	The DSPF Principle and Control were reviewed in May 2025. The First Assistant Secretary, Defence Security is the 'owner' of Principle 77 and the Assistant Secretary STA is the 'owner' of Control 77.1.	Yes.
	Security Investigation Operating Guidelines provides guidance for the conduct and recording of investigations (see paragraphs 2.55–2.57).	The Security Investigation Operating Guidelines were reviewed in October 2024 and are issued by the Assistant Secretary STA.	
Human Resources Services Branch	**Code of Conduct Policy and Procedures** outline requirements for procedural fairness, delegations for decision-making, and recording of decisions (see paragraphs 2.67–2.70).	The current Code of Conduct Policy and Procedures were released in May 2023 and November 2022 respectively by the Defence People Group and the Assistant Secretary of People Policy and Employment Conditions.	No. Human Resources Services Branch procedures do not stipulate whether AGIS is applied to Code of Conduct investigations.
Joint Military Police Unit (JMPU)	**Military Police Manual, Volume 2** outlines JMPU jurisdiction, incident reporting requirements, investigation processes and requirements (see paragraphs 2.60–2.66).	Volume 2 of the Military Police Manual was reviewed in March 2023 and issued by the CDF.	Yes.
Inspector-General of the Australian Defence Force (IGADF)	**Directorate of Investigations and Inquiries (DII) Handbook** outlines the process for conducting inquiries under the IGADF Regulation 2016, and notes that DFDA investigations are 'informed by the Military Police Manual' (see paragraphs 2.76–2.80).	The DII handbook was amended in February 2026 and is sponsored by the Director Inquiries and Investigations. As at May 2026, the handbook was undergoing further review.	Yes, only for DFDA investigations under the Military Police Manual. AGIS is not applied to inquiries.
	CDF Directive 25/2019 outlines the Military Police Code of Conduct and the role of the IGADF in investigating ADF military police matters (see paragraphs 2.74–2.75).	CDF issued the directive in November 2019. The directive was to be 'incorporated into enduring policy … no later than December 2021'. As at March 2026 a review of the instruction was underway, and has been ongoing since January 2023 (see paragraph 2.75).	

Source: ANAO analysis of Defence documentation.

Investigations and Public Interest Disclosures Branch

2.38 IPIDB was resourced with 14 personnel in investigation functions in 2024–25.[42] During the audit period (1 January 2020 to 31 December 2025), IPIDB recorded 2,061 reported incidents and commenced 639 investigations. Investigations were conducted into matters including: fraud (38 per cent), maladministration (17 per cent), and procurement misconduct (11 per cent).

2.39 IPIDB developed draft Fraud Control Instructions (FCI) in 2020 to support fraud related investigations and recovery of debts. The FCIs described IPIDB's responsibilities, engagement with internal and external entities, and processes for assessing incidents and conducting investigations. IPIDB has also issued separate Standard Operating Procedures for PIDs, released in April 2023. The Standard Operating Procedures have been regularly reviewed, and most recently updated in January 2026.

2.40 The FCIs had an effective date of 1 December 2020 and a scheduled review date of 1 December 2022. Defence was unable to provide evidence of formal review, or a final signed version. The FCIs referenced outdated legislation and policies, did not record a document history, and did not identify an accountable officer.[43] Defence advised the ANAO in March 2026 that a 'review of the FCIs was undertaken in November 2022 as part of a Modernisation Program, which was later discontinued' and that updated governance documents have been issued between 2024 and 2026 to 'target specific investigative functions and requirements'. Defence advised the ANAO in May 2026 that these updated documents 'override the FCIs from their date of earliest introduction, effective 30 August 2022'.

2.41 These documents include guidance and requirements for the use of case management systems, IPIDB jurisdiction, engagement with the National Anti-Corruption Commission (NACC), decision-making authority, and the preparation of investigation reports. As at March 2026, governance documents covering the triage and assessment of reported incidents, investigation planning and interviewing, and evidence management were in draft.

2.42 The Defence Instruction requires all personnel to declare conflicts as they arise using the AF220 Defence Conflict of Interest Declaration Form. Defence advised the ANAO in February 2026 that IPIDB manages independence and conflicts of interest in accordance with the Defence Instruction and that Defence Integrity Division holds the enterprise-level register for recording conflicts.

2.43 IPIDB guidance requires investigators to consult or consider engagement with other DIAs and entities in certain circumstances including: less serious and complex ADF fraud with JMPU; matters that are categorised as not routine or minor with the Australian Federal Police (AFP); serious or systemic corruption with the NACC[44]; and potential APS code of conduct breaches with the Human Resources Services Branch.

42 Defence advised that the figures provided are estimates based on the number of staff working at the end of each financial year.

43 References included in the FCIs that were outdated at the time included: the Defence Security Manual (replaced by the DSPF in 2018); the 2014 Commonwealth Fraud Control Framework (replaced by the 2017 Commonwealth Fraud Control Framework); and the *Financial Management and Accountability Act 1997* (replaced by the PGPA Act in July 2014). The FCIs also included updated references to the PGPA Act.

44 The NACC was established in July 2023 to detect, investigate and report on serious or systemic corruption in the Commonwealth public sector.

2.44 As outlined at Table 2.1, matters that fall under IPIDB's jurisdiction, such as fraud and conflicts of interest, may constitute a breach of the APS Code of Conduct. IPIDB and Human Resources Services Branch guidance does not establish clear jurisdiction boundaries or clear criteria for consultation on matters that may fall under the remit of both IPIDB and Human Resources Services Branch. Defence advised the ANAO in May 2026 that 'Fraud and corruption matters may be pursued criminally (by IPIDB) or administratively (by [the Human Resources Services Branch]), with various factors such as alleged value of loss, seriousness of the conduct, availability of evidence, and relevant prosecution policies, informing the most suitable approach for each incident.' As discussed in Case Study 3, the Human Resources Services Branch did not consult with IPIDB in relation to a $14,800 timesheet fraud investigation.

2.45 The PSPF requires entities to report incidents impacting a person's suitability to hold a security clearance to AGSVA. Matters that require reporting to AGSVA include: incurring a significant debt; changes in criminal history; disciplinary procedures; and security incidents. Defence advised the ANAO in March 2026 that AGSVA requirements for IPIDB have 'been incorporated into draft governance guidance awaiting endorsement and is included for consideration in the Investigation Report template, used when finalising a matter.'

Defence Procurement Complaints Scheme

2.46 In March 2019, Defence's Enterprise Business Committee (EBC), chaired by the Associate Secretary, agreed to the establishment of the Defence Procurement Complaints Scheme (DPCS) to manage all procurement-related complaints.[45] Responsibility was assigned to the Capability Acquisition and Sustainment Group (CASG). The proposal did not explain how the arrangements aligned with DIA jurisdictions or how complaints involving conflicts of interest or fraud would be treated.[46]

2.47 Defence advised the ANAO in March 2026 that since April 2021, procurement complaints have been received directly by CASG, rather than through the Audit and Fraud Control Division (now known as Defence Integrity Division) as originally proposed to the EBC, to improve timeliness and reduce duplication of effort. CASG has developed a Procurement Complaints Handling fact sheet and flow chart for handling complaints, which includes referring conflict of interest and fraud matters to IPIDB.

2.48 Defence advised the ANAO in October 2025 that CASG consults with IPIDB in instances where matters may fall under IPIDB's jurisdiction (such as fraud), however there is no documented guidance for managing potential jurisdiction overlap and referring cases to IPIDB. CASG reviews of procurement complaints are not conducted under AGIS. While CASG guidance states that investigating officers should not be 'involved with decisions regarding procurement method … tender evaluation, the contract award or the administration of the relevant contract', CASG procedures do not explicitly mandate independence. While AGIS does not specifically address

45 The EBC is responsible for ensuring the effective operation of Defence business and provides 'strategic control over the corporate and military enabling functions' within Defence.

46 A proposal for the DPCS had originally been presented to the EBC in January 2019. Feedback from IPIDB personnel in January 2019 in response to the original proposed model noted that: it did not account for complaints that 'may have a fraud/corruption basis' or obligations under the PID Act; the use of the term 'investigation' was 'problematic' as it suggested an activity that was being conducted by a DIA; and updates to incident reporting policies may be required. The model agreed by the EBC in March 2019 did not address these concerns.

procurement complaints, examining these complaints without independence or alignment to AGIS creates risks, particularly where integrity issues, such as suspected fraud or corruption is identified during CASG's review. Clearer definitions of CASG's jurisdiction or role in reviewing procurement complaints would help ensure procurement integrity issues are handled appropriately.

2.49 In February 2025, a briefing provided to the Defence Secretary advised that IPIDB's caseload increasingly involves complex procurement-related misconduct including fraud and conflicts of interest, indicating potential systemic weaknesses and attitudes across Defence.

Recommendation no. 2

2.50 The Department of Defence, in preparation for the establishment of the Defence Delivery Agency from 1 July 2027, establish clear and consistent arrangements for managing procurement-related complaints that are currently handled by the Capability Acquisition and Sustainment Group.

Department of Defence response: *Agreed*.

Security Threat and Assurance Branch

2.51 STA Branch was resourced with 101 personnel in 2024–25. During the audit period (1 January 2020 to 31 December 2025), STA Branch recorded 7,196 reported incidents and commenced 301 investigations. Investigations were conducted into matters including: inappropriate disclosure or release of information (33 per cent), unauthorised access (14 per cent), and disruptive behaviour (10 per cent).

2.52 Principle 77 Security Incident Management and Investigation in the Defence Security Principles Framework (DSPF), updated in May 2025, requires all security incidents to be reported to the Security Incident Coordination Centre (SICC) within the STA Branch.

2.53 Principle 77 is supported by DSPF Control 77.1, updated in May 2025, which states that investigations conducted by the STA Branch are to be undertaken in accordance with the Protective Security Policy Framework (PSPF) and AGIS, 'where appropriate.'[47] The control provides guidance for responding to security incidents and states:

> In the course of responding to a security incident, a Commander/Manager may need to conduct a Fact Find to gain more information, to identify vulnerabilities and determine the appropriate treatment action to contain the situation. … Commanders/Managers should not conduct a Fact Find into security incidents with an assessed SIIL [Security Incident Impact Level] of HIGH or EXTREME unless directed by SICC, the SIU [Security Investigations Unit within STA] or another DIA.

2.54 The DSPF does not set a mandatory review cycle for its principles and controls, instead stating that it is a 'flexible policy framework' and that 'DSPF documents will be reviewed and updated as necessary'.[48]

47 Defence advised the ANAO in February 2026 that this language reflects the requirements of the PSPF and that 'there have been no [Security Investigation Unit] security investigations conducted that have not been undertaken in accordance with the PSPF, DSPF or AGIS.'

48 Outdated references in Principle 77 include: the Incident Reporting and Management Manual; the 2011 Australian Government Investigation Standards; and prior versions of the PSPF (the PSPF was updated in November 2024, including adding, modifying and removing controls under a new policy structure, and updated further in July 2025).

2.55 The STA Branch has also issued Defence Security Investigation Operating Guidelines, approved by the Assistant Secretary STA, which outline the STA Branch's role in conducting security investigations and reporting outcomes and recommendations.[49]

2.56 The guidelines state for an issue to be considered for investigation, it must be of 'sufficient significance' and relate to: a suspected breach, avoidance or failure to meet DSPF requirements; the identification of a failure or ineffective security control; or a series of security matters indicating a systemic or emerging issue. The guidelines include a matrix for assessing significance, and state that '[i]n some cases, matters that have a Low to Medium Security Incident Impact Level (SIIL) will not be of sufficient significance to warrant investigation.' In instances where investigations determine that an individual is a security risk, the guidelines require that investigators report this to AGSVA.

2.57 The guidelines were issued in May 2020 and do not include a scheduled review period. They were updated in October 2024 to reflect the introduction of the Defence Enterprise Resource Planning Case Management System (DECMS) in May 2024 and the 2022 AGIS but still reference an outdated version of the PSPF.

2.58 Where an incident proceeds to investigation, a Security Incident Referral Checklist must be completed by the SICC, which requires the SICC to identify the DIA the incident will be handled by, the assessed Security Incident Impact Level, and whether there are any other factors to warrant investigation. The checklist does not include the Human Resources Services Branch as a DIA. As outlined at Table 2.1, some security incidents, such as inappropriate access to Defence ICT systems, may fall under the jurisdiction of STA Branch or the Human Resources Services Branch. STA Branch guidance does not outline any specific factors to be considered when determining whether a matter should be referred to another DIA.

2.59 STA Branch guidance does not specify requirements for investigator independence. Defence advised the ANAO in February 2026 that STA Branch conflicts of interest are managed through Defence's existing conflict of interest process (see paragraph 2.42), including initial case discussions and the re-allocation of investigators where a conflict of interest is identified.

Joint Military Police Unit

2.60 JMPU was resourced with between 483 and 490 personnel in 2024–25.[50] During the audit period (1 January 2020 to 31 December 2025), JMPU recorded 21,736 reported incidents and commenced 2,351 investigations. Investigations were conducted into matters including: entitlement fraud (16 per cent), 'sexual assault and related offences' (15 per cent), and 'acts intended to cause injury' (14 per cent).

2.61 The JMPU has issued a Military Police Manual, dated 14 March 2023, under the authority of the CDF. The manual requires DFDA investigations to comply with the AGIS, including the use of

49 The STA Branch has also developed Standard Operating Procedures (SOPs) covering exhibit management and the referral and assessment of incidents by SICC.

50 This figure includes Reserve members and represents the total ADF military police workforce, encompassing both general duties members (including patrol, crime prevention and force protection roles) and those employed in investigative positions. Defence advised the ANAO in May 2026 that 'While all Military Police are qualified in accordance with AGIS to conduct investigations, posting type, role allocation and operational tempo significantly reduce the proportion of personnel available to undertake investigative duties at any given time'. Table 2.6 outlines the number of personnel who had been recorded against investigations in Defence data between 1 November 2022 and 9 December 2024 for each DIA.

investigation plans, regular updates to stakeholders, and proper evidence management. It includes templates such as investigation plans, evidence matrices and privacy notices, although the investigation plan template does not provide fields to record delegate approval or dates. JMPU has also developed templates for assessment reports and referrals of Briefs of Evidence to the Office of the Director of Military Prosecutions (ODMP).

2.62 The manual requires investigators to be independent. Defence advised the ANAO in February 2026 that JMPU conflicts of interest are managed through Defence wide processes rather than separate JMPU policies, with declared conflicts recorded in case records and system access restricted when required.

2.63 The manual comprises of four volumes, with investigation procedures set out in Volume 2. It defines the jurisdiction of JMPU and establishes an ADF Military Police Investigation Jurisdiction Model, identifying five levels of offences and responsibility for investigation. Table 2.3 outlines that offence definitions overlap and that the Jurisdiction Model does not provide a clear or consistent approach to identifying and investigating notifiable incidents. As discussed at paragraph 2.10, whether an offence is considered minor or serious under the DFDA is ultimately determined at the discretion of relevant commanders. Defence has not established guidance or safeguards to assist commanders in making this judgement, which would mitigate the risk of inequitable or disproportionate outcomes. Implementing enterprise-wide oversight and reporting arrangements would further mitigate this risk.

Table 2.3: ADF Military Police Jurisdiction Model

Offence level	Offence type	Investigation responsibility
Disciplinary Infringements	A minor breach of discipline by ADF members of, or below, the rank of Lieutenant (Navy), Captain (Army) or Flight Lieutenant (Air Force). Breaches include: absence from duty, insubordinate conduct, and disobeying a lawful command.	Unit or General Duties Military Police if 'deemed sensitive /reputational'
Level 1	DFDA Schedule 1A offences, including absence from duty, insubordinate conduct, and negligence in performance of duty. As outlined at Box 1, the Defence Instruction states these incidents are not notifiable incidents. The Military Police Manual notes that these incidents are not to be recorded on the Defence Policing and Security Management System (DPSMS). The Manual also states that 'All reported incidents must be recorded on DPSMS, even when it is known that the incident may not relate to a Service offence. Entering an incident onto DPSMS does not necessitate that an investigation is to commence, rather it is a means of recording that an incident has been reported.' The Defence Instruction requires that incidents reported to managers and commanders must be recorded 'as close to the time of the incident as practicable, in the authorised case management system'.	Unit or General Duties Military Police if 'deemed sensitive/reputational'

Offence level	Offence type	Investigation responsibility
Level 2	'Serious service offences' under section 101 of the DFDA, which are service offences 'punishable by a maximum punishment, or fixed punishment, of imprisonment for life or a period exceeding 6 months'. This includes offences that may also be considered under Level 1 (which are not notifiable incidents), as well as more serious offences, such as abandoning a post or assaulting a superior officer. Major security incidents (with agreement from STA Branch), or fraud offences (with agreement from IPIDB). The Military Police Manual notes that 'Level 2 matters are Notifiable Incidents'.	Unit (if deemed appropriate) or General Duties Military Police The Manual does not provide guidance on when it would be 'deemed appropriate' for a unit to investigate a Level 2 matter, or who makes that determination.
Level 3	Prescribed service offences under section 104 of the DFDA, which are service offences 'punishable by imprisonment for more than 2 years', with no specified maximum imprisonment period. This includes offences that may also be considered under Level 2. The Manual states that prescribed offences are to be referred to the ODMP for advice. 'Sensitive matters' and criminal offences under Commonwealth, state or territory legislation. This includes offences such as murder, manslaughter or grievous bodily harm. While the Manual does not state that Level 3 or 4 incidents are Notifiable Incidents, as outlined at Box 1, the Defence Instruction defines notifiable incidents to include matters that raise 'a reasonable suspicion that a serious offence has been committed under the *Defence Force Discipline Act 1982.*	ADF Investigators
Level 4	A 'critical, complex and/or major incident, or sudden death.'	ADF Investigators

Source: ANAO analysis of Defence documentation.

2.64 The manual sets out arrangements for referring matters to IPIDB and states that the First Assistant Secretary Defence Integrity 'will determine which Defence Investigative Authorities will investigate fraud offences which exceed a loss of $20,000 to the Commonwealth involving ADF members'. This monetary threshold was removed from enterprise-level policy in August 2022.

2.65 The manual also requires complaints related to the conduct of ADF military police to be referred to the IGADF. The manual does not set out a process or requirement for referral of matters to the STA Branch or AGSVA. Defence advised the ANAO in July 2025 that recommendations to notify AGSVA are 'usually included in the investigation's final report' and that the decision to notify AGSVA following a JMPU investigation rests with the relevant unit. This approach is not consistent with IPIDB, STA Branch or the Human Resources Services Branch, which have established guidance or processes for the referral of matters to AGSVA. As discussed in Case Study 2, there is no evidence that a $68,808 entitlement fraud matter investigated by JMPU was referred to AGSVA for consideration of the individual's security clearance suitability. The manual includes guidance for the referral of matters to Defence's Sexual Misconduct Prevention and Response Office (SeMPRO) where appropriate.

2.66 The current version of Volume 2 of the manual is dated 14 March 2023 and includes a scheduled review date of 18 March 2024.[51] Defence advised the ANAO in February 2026 that a review of the manual was conducted in March 2024, however 'no documented evidence exists to confirm the conduct or completion' of the review and that it will implement 'formal, traceable, and auditable documentation for all future reviews' of the manual. Prior reviews of the manual took place in January 2020, November 2020, March 2021 and March 2023.

Human Resources Services Branch

2.67 The Human Resources Services Branch (the Branch) was resourced with 9 personnel in 2024–25. During the audit period (1 January 2020 to 31 December 2025), the Branch recorded 664 reported incidents and commenced 469 investigations. Investigations were conducted into matters including: 'failure to follow directions or policy' (36 per cent), and 'unacceptable behaviour' (29 per cent).

2.68 The *Public Service Act 1999* requires that entities establish written procedures to determine whether an APS employee has breached the Code of Conduct. The Branch has established Code of Conduct procedures that outline requirements for procedural fairness, delegations for decision-making, conduct of interviews and recording of decisions. The procedures state that 'the decision maker may seek the assistance of an investigator to investigate the alleged breach'. The Branch has also established templates for investigations including: a Code of Conduct Referral Checklist; evidence matrix; and determination and notice letters. The determination and notice letters include prompts for investigators to consider referring the matter to AGSVA, which are supported by AGSVA reporting templates.

2.69 The Branch's procedures and templates do not stipulate whether AGIS is applied to Code of Conduct investigations and do not establish independence requirements for investigators. Defence advised the ANAO in February 2026 that management of conflicts of interests for the Branch occurs 'throughout the Code of Conduct process' and that when a conflict is identified, the matter is reallocated to an alternative investigator or decision maker. Defence further advised that there was no register for declaring, recording or managing conflicts of interest during investigations and that the Branch has since implemented a register 'to document such decisions in the future, which will help ensure consistent recording, improved accountability, and greater transparency in investigative processes.'

2.70 The Branch's procedures do not provide detailed guidance on investigation practices such as the management of evidence, dealing with suspected criminal behaviour, or consulting with or referring matters to other DIAs or entities. As discussed in Case Study 3, the Branch did not consult with IPIDB in relation to a $14,800 timesheet fraud investigation and there were deficiencies in the recording of investigation evidence. Defence advised the ANAO in March 2026 that work has 'commenced on developing procedures relating to consultation with or referral of matters to other DIAs or entities.'

2.71 The Branch uses the Handling Misconduct guide developed by the Australian Public Service Commission. The Handling Misconduct guide provides guidance for dealing with misconduct

51 The manual references outdated documents including: the Defence Investigations Standards Manual (cancelled in December 2023); the Incident Reporting and Management Manual and Defence Instruction FIN 12-1 (replaced by the Interim Incident Reporting and Management Policy in August 2022); and the Interim Incident Reporting and Management Policy (replaced by the Defence *Instruction* in September 2024).

referrals and conducting investigations, including gathering and reviewing evidence, providing procedural fairness and drafting investigation reports. While the guide includes requirements for the selection of an independent decision-maker, it does not outline independence requirements for investigators and only references the application of AGIS for fraud investigations.

Inspector-General of the Australian Defence Force

2.72 The IGADF was resourced with 211 personnel in 2024–25 including 67 permanent personnel and 144 non-ongoing or ADF reserve members.[52] The professional standards team, within the Directorate of Inquiries and Investigations was resourced with three DFDA investigators, seconded from the JMPU. During the audit period (1 January 2020 to 31 December 2025), IGADF conducted a total of 295 assessments, investigations and inquiries into professional standards matters including: 'contravention of professional standards' (38 per cent), 'misconduct' (21 per cent), and 'harassment and threatening behaviour' (six per cent). The 'contravention of professional standards' category included matters related to misconduct and unacceptable behaviour.

2.73 The IGADF has established the Directorate of Inquiries and Investigations (DII), responsible for the receipt and assessment of submissions, complaints and referrals regarding the application of the military justice system and the conduct of ADF military police.

2.74 CDF Directive 25/2019 Military Police Professional Standards Framework outlines the Military Police Code of Conduct and the role of the IGADF in investigating ADF military police matters. The Directive requires that it is subject to IGADF review at least annually 'to ensure the currency and appropriateness of both the Code of Conduct and the process of managing professional standards matters involving Military Police.' The IGADF advised the ANAO in May 2025 that it has participated in 'periodic reviews' of the instruction however 'IGADF is not bound by CDF Directive 25/2019 consistent with [IGADF's] statutory independence.' The Directive states that it applies to all ADF military police 'regardless of whether that member is serving in a Military Police role or any other role'. The *Defence Act 1903*, which establishes the functions of the IGADF states that the IGADF's role is to provide the Chief of the Defence Force with mechanisms for review of the military justice system 'independent of the ordinary chain of command' (see paragraph 1.15).

2.75 A review of the instruction has been underway since January 2023, including: the drafting of a new Code of Conduct to allow the military police chain of command 'to handle unit-level administrative and minor disciplinary issues'; and consideration of 'the most appropriate policy framework in which [the new Code of Conduct] should be published'. The Directive noted that it would remain in place 'until incorporated into enduring policy' which the CDF expected to occur 'no later than December 2021'. Defence advised the ANAO in March 2026 that a 'revised Military Police Code of Conduct has been drafted' but not yet incorporated into an 'endorsed policy instrument', and that Directive 25/2019 is expected to remain in effect until the end of 2026. IGADF advised the ANAO in May 2026 that it 'does not own or author the Military Police Professional Standards Framework or the Military Police Code of Conduct. These are both owned by Defence'.

2.76 DII has also established a DII Handbook that outlines processes for IGADF investigations under the DFDA and inquiries under the Inspector-General of the Australian Defence Force Regulation 2016 (IGADF Regulation). The handbook states that it 'is not Defence policy and other

52 Staff within the IGADF are comprised of APS personnel and ADF members, including ADF reservists, made available by the Secretary of Defence and CDF. IGADF advised the ANAO in March 2026 that 'most ADF Reservists engaged by the IGADF do not provide full-time service'.

relevant Defence policy (for example the Administrative Inquiries Manual and the Complaints and Resolution Manual) are to be referred to for policy guidance.'[53] The handbook has recorded review dates since May 2023.

2.77 The handbook establishes independence requirements for Assistant IGADFs and states that, before commencing an inquiry, the Assistant IGADF 'is required to consider the key complainants and respondents and assess if they are able to undertake the inquiry in an impartial, unbiased and independent manner.' Assistant IGADFs are required to submit an annual statement of independence which are 'centrally managed', as well as a statement for specific cases.

2.78 The handbook does not establish independence requirements for inquiry officers, or for assessment officers who conduct an initial assessment of referrals and recommend an appropriate course of action.[54] It also does not establish processes for handling matters that involve potential criminality, or processes for the referral of matters to AGSVA. IGADF advised the ANAO in November 2025 that Assistant IGADFs conducting inquiries 'are directed not to conduct a criminal or disciplinary investigation or to conclude that an offence has been committed by any person'. In instances where criminal conduct or a service offence is identified 'the inquiry into that aspect of the matter is to cease' and the circumstances are to be reported to the relevant authority.

2.79 The DII Handbook provides that the IGADF may undertake an investigation under the DFDA or an inquiry under the IGADF Regulation for complaints regarding ADF military police. The Military Police Manual, which establishes requirements for DFDA investigations, states that it is 'issued under the authority of the CDF' and applies to all ADF military police, including those who undertake DFDA investigations. IGADF advised the ANAO in July 2025 that Defence policy and the Military Police Manual 'does not bind the OIGADF [Office of the IGADF]'. IGADF advised the ANAO in March 2026 that it is updating the DII Handbook 'to make clearer reference to the Military Police Manual' and the application of AGIS requirements. As discussed in Case Study 5, deficiencies were identified with an IGADF investigation into entitlement fraud, including not being able to evidence completion of required investigation assessment and planning documents and not providing regular updates to stakeholders.

2.80 The handbook does not include guidance or procedures for determining whether an inquiry or investigation is more appropriate. Unlike investigations: AGIS requirements, including qualification requirements, do not apply to IGADF inquiries; IGADF inquiries are not bound by the rules of evidence[55]; may be conducted in public or private; and establish different limitations for legal representation.[56]

53 The Administrative Inquiries Manual states that it does not apply to IGADF inquiries (see paragraph 2.25).

54 The handbook notes that the 'majority of inquiries are conducted by Assistants IGADF … not by inquiry officers.'

55 The rules of evidence govern what information may be placed before a court for determination of an issue. The Military Police Manual states that 'Every investigation decision made by [military police] will be in accordance with the laws and rules of evidence'.

56 For example, the IGADF Regulation states that a person's legal representation may only address the inquiry at such times as determined by the Inspector-General, Assistant IGADF or inquiry officer. For investigations conducted under the DFDA, legal practitioners must be allowed to 'be present during the questioning and to give advice to the person, but only while the legal practitioner does not unreasonably interfere with the questioning.'

Alignment with AGIS

2.81 The AGIS establishes a standard for Australian Government entities conducting administrative, civil or criminal investigations and states that any deviation from the AGIS 'is a decision and must be recorded.' The AGIS are expressed as four 'principle streams' with supporting requirements:

- Personnel — requirements for investigators to be fair, unbiased, and appropriately skilled and qualified, and for investigations to be conducted in accordance with relevant legislation and regulations.
- Information and evidence management — requirements for managing the disclosure of investigation information, and the use of information management systems to support investigation recording and decision-making.
- Investigative practices — requirements for the establishment of Risk Management Frameworks and investigation procedures, the collection and handling of evidence, and the recording of decisions.
- Quality assurance — requirements for the establishment of a Quality Assurance Policy and the conduct of quality reviews and audits.

2.82 Table 2.4 outlines the extent to which investigations processes and guidance established by each DIA and the IGADF reflects and aligns with requirements established under each AGIS principle.

Table 2.4: ANAO assessment — DIA and IGADF guidance alignment with AGIS requirements

AGIS principle streams	IPIDB	JMPU	Human Resources Services Branch	STA Branch	IGADF[a]
Personnel	◕	◕	◑	◑	◕
Information and evidence management	◕	◕	◑	◕	◕
Investigative practices	◕	◕	◔	◑	◕
Quality assurance	◔	◑	○	◔	◔

Key: ● Fully aligned ◕ Largely aligned ◑ Half aligned ◔ Partly aligned ○ Not aligned

Note a: IGADF uses the Military Police Manual for DFDA investigations. Assessment of IGADF is based on review of the DII Handbook as well as the Military Police Manual, where appropriate.

Source: ANAO analysis of Defence documentation.

2.83 DIA and IGADF guidance has not covered or aligned with the AGIS principles, including:

- quality assurance (see paragraphs 3.60–3.84);
- disclosure and request of documents with internal and external stakeholders;
- transfer or referral of matters to other DIAs or external entities;
- handling information impacted by Legal Professional Privilege;
- investigator competence and qualifications (see paragraphs 2.86–2.96);

- use of case management systems and the management and review of evidence;
- considering the admissibility of evidence in investigation planning; and
- establishment of investigation risk management frameworks.

2.84 DIA guidance has not been regularly reviewed and updated, increasing the risk that changes to Defence and Commonwealth investigation policies are not sufficiently considered in DIA investigative practices. Investigative processes differ across DIAs. While such differences reflect the varying nature of investigative work undertaken by DIAs, the lack of clearly established jurisdictions and referral mechanisms between DIAs presents a risk that matters may not be dealt with equitably.

Recommendation no. 3

2.85 The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force:

(a) update Defence Investigative Authority and IGADF guidance to align with Commonwealth and Defence policies and provide clear direction on the triaging and referral of incidents between investigative functions;

(b) implement enterprise-level policy to mandate regular review of investigation guidance and process documents; and

(c) establish enterprise-level requirements to support the equitable management and proportionate outcomes of investigations, such as for the referral of matters to the Australian Government Security Vetting Agency.

Department of Defence response: *Agreed.*

Qualification and training requirements

2.86 The AGIS establishes qualification requirements for investigators and requires that:

- investigators hold a Certificate IV in Government Investigations (or equivalent); and
- those involved in the supervision of entity investigations hold a Diploma of Government Investigations (or equivalent).

2.87 The AGIS also requires entities to:

- document the qualifications required to conduct investigations and the timeframe in which investigators should obtain the qualifications; and
- consider the legal risk associated with engaging investigators, supervisors or operational decision makers without an appropriate qualification.

2.88 Table 2.5 outlines the extent to which guidance for each DIA and the IGADF addresses AGIS qualification requirements. The Defence Investigation Standards Manual (cancelled in December 2023) reflected AGIS qualification requirements at an enterprise level.

Table 2.5: DIA and IGADF qualification requirements[a]

AGIS Requirement	IPIDB	JMPU	STA Branch	Human Resources Services Branch	IGADF
Required qualification and the timeframe to obtain the qualification has been documented.	Yes	Yes	No	No	N/A[b]

Note a: Qualification requirements that align with the AGIS have not been established for fact-finding officers or by CASG. Procedures developed by CASG state that 'Training for Investigating Officers is available through the Campus course 'Fact Finding in Incident Management'.

Note b: The IGADF utilises three investigators seconded from JMPU to conduct DFDA investigations, who are subject to the requirements of PMADF Directive 15-2024 (see paragraph 2.91).

Source: ANAO analysis of Defence documentation.

2.89 Neither Defence nor the IGADF have documented consideration of the legal risk associated with personnel not holding an appropriate qualification. Defence advised the ANAO in March 2026 that the IPIDB requirement for equivalent qualifications or career experience to be assessed by Senior Executive as an appropriate equivalent 'inherently incorporates consideration of legal risk' and that legal risk has been considered when establishing qualification criteria.

2.90 Two DIAs (IPIDB and JMPU) have documented the minimum training requirements for investigators. Relevant qualification requirements for JMPU are outlined in PMADF Directive 15-2024 Military Police Qualifications, signed in November 2024. Prior to this Directive, JMPU had not documented investigator training requirements in accordance with the AGIS.

2.91 IGADF uses seconded JMPU investigators for DFDA investigations. These investigators are subject to the requirements of PMADF Directive 15-2024. Assistant IGADFs conducting inquiries are required to 'hold a form of relevant qualification, which can include': Advanced Inquiry Officer Course; Certificate IV in Government Investigations; or relevant legal qualifications. As discussed at paragraph 2.80, AGIS requirements do not apply to IGADF inquiries.

2.92 The DIAs and IGADF have established additional mandatory training requirements for investigators covering topics including: the use of investigation case management systems (STA Branch); procedural fairness and managing Code of Conduct investigations (Human Resources Services Branch); and courses on 'Compassionate Foundations' and 'Trauma-informed Practices' (IPIDB and IGADF). Assistant IGADFs are required to complete courses on 'Assessing and Protecting Official Information' (this course is aimed at all Defence personnel who handle official information as part of their duties) and 'Introduction to Administrative Inquiries' (this course is aimed at Defence personnel who undertake Inquiry Officer Inquiries). Defence has not established standardised training requirements for investigators at an enterprise level.

2.93 Inquiry officers located with inquiry cells established by Army and Air Force are required to hold a Certificate IV in Government Investigations.[57] Navy has established a similar requirement in

57 Inquiry cells for each Service were established following the completion of a Re-Thinking Systems of Review report in 2014 (see paragraph 2.29), which identified issues with inquiries including perceived lack of independence and experience of inquiry officers, and lapses in procedural fairness and the gathering and analysis of evidence. Chief of Army Directive 11/21 Directorate of Army Administrative Inquiries states that the requirement for Army inquiry officers to hold a Certificate IV in Government Investigations may be 'waived in writing by the Director'.

draft policy. Inquiry officers may be issued with a Certificate IV in Government Investigations following successful completion of Defence inquiry officer and fact-finding courses, and experience in previous fact-findings and inquiries. Defence is a Registered Training Organisation and may issue nationally recognised qualifications (such as a Certificate IV in Government Investigations).

2.94 To assess compliance with the AGIS qualification requirements by the DIAs and the IGADF, all personnel who had been recorded against investigations in Defence case management system data between 1 November 2022 (after the introduction of the 2022 AGIS) and 9 December 2024 were identified.[58] Table 2.6 outlines the extent to which Defence has recorded investigator qualifications.[59]

Table 2.6: Investigator qualifications between November 2022 and December 2024, based on case management system data

Category	IPIDB	JMPU	STA Branch	Human Resources Services Branch	IGADF
Investigators with Certificate IV, Diploma or higher	10 (50%)[a]	144 (92%)	6 (75%)	7 (50%)[b]	1 (100%)
Investigators with other relevant qualifications[c]	–	12 (8%)[d]	–	–	–
Investigators with no recorded investigation qualifications	10 (50%)[e]	1 (<1%)	2 (25%)[f]	7 (50%)[g]	–
Total	**20 (100%)[h]**	**157 (100%)**	**8 (100%)**	**14 (100%)**	**1 (100%)[i]**

Note a: This includes five investigators who are recorded as having either a Certificate IV or Diploma in Government Investigations 'or equivalent'.

Note b: This includes two investigators who obtained a Certificate IV in Government Investigations after the investigation period being assessed in this table (November 2022 to December 2024). The Human Resources Services Branch advised the ANAO that, as at March 2026, it had 'a total of five investigators all of which have attained the Certificate IV.'

Note c: This category only includes personnel who have not been identified as holding a Certificate IV or Diploma in Government investigations.

Note d: This includes nine investigators with investigation qualifications obtained through the Defence Force School of Policing, which JPMU considered as equivalent to a Diploma of Investigations.

Note e: Defence advised the ANAO in March 2026 that all fourteen IPIDB investigative personnel employed as at 31 December 2025 'held appropriate qualifications'.

58 IPIDB maintains a separate register of investigator qualifications. To ensure a consistent assessment was applied across all DIAs and IGADF, the ANAO identified investigators based on Defence case management system data. As discussed at paragraph 3.14, system performance and reporting limitations have been identified, which limited Defence's ability to provide the ANAO with comprehensive data on reported incidents and investigations across Defence for the audit period. This may impact the completeness of investigator data as assessed in Table 2.6.

59 Defence advised the ANAO in July 2025 that personnel recorded against an investigation in Defence data 'does not necessarily equate to an investigator — additional members may be added … where they have a need to access and/or edit a case, for example intelligence members, fraud recovery members, assessment officers'. Defence identified two JMPU personnel in the data for the relevant period who were not military police members and three STA Branch personnel who were not investigators. These personnel have been excluded from the figures.

Note f: Defence advised the ANAO in March 2026 that as at 1 February 2026, all STA Branch investigators held a 'Certificate IV, Diploma or higher'.

Note g: This includes two investigators who are 'seeking to enrol' or are currently enrolled in a Certificate IV in Government Investigations.

Note h: Defence advised the ANAO in May 2026 that based on IPIDB's separate register of investigator qualifications, IPIDB had a total of 37 personnel working in investigator roles between November 2022 and December 2024 and that, of these personnel, 30 either held or obtained relevant qualifications, two obtained qualifications outside of the 12-month timeframe, and five did not hold relevant qualifications. As discussed at paragraph 2.94, this table reflects personnel who had been recorded against investigations in Defence data (see footnote 58).

Note i: As discussed at paragraph 2.72, the IGADF utilises three investigators seconded from JMPU to conduct DFDA investigations. For the sampled period (1 November 2022 to 9 December 2024) one individual was recorded against two IGADF DFDA investigations. The total excludes five personnel identified by IGADF as not being investigators and who do not conduct DFDA investigations. Four of these personnel were identified as Assistant IGADFs. None of the Assistant IGADFs were identified by IGADF as holding a Certificate IV in Government Investigations, and AGIS does not mandate qualification requirements for inquiries. IGADF advised the ANAO in March 2026 that 'many Assistant IGADFs have completed advanced inquiry officer training or hold law degrees or are highly experienced jurists. These professional qualifications and experience exceed the standards set out in the AGIS.'

Source: ANAO analysis of Defence documentation.

2.95 None of the four DIAs were able to provide evidence of appropriate qualifications being held for all investigators conducting investigations for the period sampled. Defence does not hold qualification records for 11 per cent of investigators assigned to investigations between 1 November 2022 and 9 December 2024.

2.96 There were also instances where personnel responsible for oversight or supervision of investigations did not hold, or could not provide evidence of holding, a Diploma-level qualification under AGIS. This includes:

- the Director of the Directorate of Conduct and Performance (within the Human Resources Service Branch) as well as three Assistant Directors within the Directorate who have approved Determination of Breach notices or the findings of preliminary reviews; and
- three former and current Directors of the Directorate of Inquiries and Investigations in IGADF, of which two held a Bachelor of Laws, and one completed an Advanced Inquiry Officer course and had 'recognised equivalent experience'.

Recommendation no. 4

2.97 The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, ensure that AGIS required investigator qualifications, including accepted equivalencies, are in place and recorded for all investigators involved in investigations.

Department of Defence response: *Agreed.*

3. Implementation of arrangements for investigations

Areas examined

This chapter examines whether the Department of Defence (Defence) has effectively implemented its arrangements for investigations.

Conclusion

Investigations have not always been conducted in accordance with Defence policy. Between January 2020 and December 2025, the average time to finalise investigations after an incident was reported was 196 days for DIAs and 269 days for IGADF military police professional standards assessments, inquiries and investigations. These protracted timeframes may present risks to the wellbeing of affected personnel if not appropriately managed. Fact-finding activities have been conducted into notifiable incidents without proper referral to DIAs, as required by Defence policy. Defence has not established enterprise-level reporting for incident and investigation trends, timeliness and outcomes that are not related to fraud, limiting Defence's assurance that similar matters are dealt with equitably, proportionately and in alignment with Defence policies.

Areas for improvement

The Australian National Audit Office (ANAO) made five recommendations aimed at: monitoring, reporting and performance measurement; administration and recovery of fraud-related debts; quality assurance; fact-finding activities; and the conduct of investigations. The ANAO also identified one opportunity for improvement aimed at improving case management system reporting.

3.1 Enterprise-level monitoring, reporting and quality assurance arrangements are critical to providing senior leaders with assurance that Defence's investigations framework is operating as intended, managing risk effectively, and supporting continuous improvement. Between 1 January 2020 and 31 December 2025, Defence recorded 31,657 incidents in its investigation case management system.

3.2 In an environment of a high volume of reported incidents investigated by multiple Defence Investigative Authorities (DIAs) and the Inspector-General of the Australian Defence Force (IGADF), with different requirements, enterprise-level oversight is essential to drive equitable, and proportionate outcomes, informed by lessons learned.

Has Defence established monitoring and quality assurance arrangements for investigations?

Defence has implemented quarterly reporting to governance committees on fraud-related incidents and investigations. There is no enterprise-level reporting on the trends, timeliness and outcomes of incidents and investigations across DIAs and the IGADF that are not related to fraud. Defence has not established enterprise-level performance measures or AGIS aligned quality assurance arrangements for investigations, presenting a risk that investigations are not handled equitably and proportionately. Investigations and inquiries are not always conducted

in a timely manner or in accordance with targets for investigation timeliness, where they have been set by investigative functions. Fraud recoveries have not been undertaken in a timely manner and unrecovered fraud debts have not been managed in accordance with the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

3.3 In May 2024, Defence implemented the Defence Enterprise Resource Planning Case Management System (DECMS), which formed part of Defence's Enterprise Resource Planning (ERP) Program, to provide a 'reliable and single source of data [to] enable real-time reporting, allowing for the timely provision of critical information'.[60] A proposal for the new system outlined that Defence's previous case management approach had been fragmented, lacked integration, involved duplication of information, and required improved case management capabilities.[61]

3.4 Prior to the implementation of DECMS, Defence used 16 separate case management systems for recording incidents, inquiries and investigations, including:

- Defence Policing and Security Management System (DPSMS) to record Defence Investigation Authority (DIA) investigation activities and IGADF professional standards investigations and inquiries;
- Conduct Reporting and Tracking System (CRTS) to record Joint Military Police Unit (JMPU) investigations conducted under the *Defence Force Discipline Act 1982* (DFDA);
- Army Incident Management System (AIMS) to record reportable incidents in Army;
- Conduct and Performance system to record complaints, misconduct, and performance management matters involving Defence personnel;
- Australian Defence Force Administrative Inquiry Tracking System (ADFAITS) to record inquiries conducted under the Defence (Inquiry) Regulations 2018; and
- ComTrack Defence to record Australian Defence Force (ADF) and Australian Public Service (APS) complaints and grievances.

3.5 In May 2024, data from source systems was migrated into DECMS following quality assurance checks. Post-migration data integrity issues were identified by Defence including the duplication of data from incidents recorded in multiple systems, and incorrect incident start dates. These issues have impacted the accuracy of reporting. DIAs have raised concerns about system functionality, including reporting and searching limitations, and system performance and availability. Defence advised the ANAO in May 2026 that system improvements had been implemented or were underway. This included implementation of a trend dashboard in September 2025 and the enabling of reporting based on keyword searches for the Security Threat and Assurance (STA) Branch in January 2026 and for the JMPU in July 2026.

3.6 The STA Branch utilises a case management spreadsheet 'when DECMS is offline or there is an unexplained outage' as a contingency. The Investigations and Public Interest Disclosures Branch (IPIDB) records all Public Interest Disclosures (PID) in DECMS, however manually records PID

60 The ERP program involves the streamlining of Defence business processes associated with hundreds of separate Defence ICT applications into one system, with the intent of enabling better governance, faster processing and lower maintenance and support costs.

61 Deficiencies identified by Defence in previous system capabilities included: inability to create customisable workflows and analytics; difficulty consolidating various data sources; sustainability risks for systems that had reached, or were close to reaching, end-of-life; and challenges maintaining information security.

decisions under section 29(2A) of the *Public Interest Disclosure Act 2013* on a spreadsheet as DECMS does not 'currently support the legislative reporting requirements for the Commonwealth Ombudsman' under the *Public Interest Disclosure Act 2013*.[62] Defence advised the ANAO in May 2026 that system changes were in progress 'to align DECMS functionality with PID legislative requirements.' As discussed at paragraph 3.14, system performance and reporting limitations have limited Defence's ability to provide the ANAO with comprehensive data on reported incidents and investigations across the department for the audit period.

Opportunity for improvement

3.7 The Department of Defence could consider further improvements to case management system reporting capabilities to ensure the system adequately supports Defence's investigative functions and provides a wholistic view of incidents and investigations across Defence.

Requirement to use case management systems

3.8 The Australian Government Investigations Standard (AGIS) requires that 'Entities must develop clear procedures and supporting tools to record, retain, register, review, reveal and produce investigation information.' Prior to its cancellation in December 2023, the Defence Investigation Standards Manual required DIAs to have written procedures for investigation activities and that the procedures 'are to recognise DPSMS as the DIA's primary case management system'. The Defence Investigation Standards Manual has not been replaced, as such there is no enterprise-level document that establishes a requirement for DIAs to develop written procedures for the use of case management systems. As discussed at paragraph 2.17, the 2026 Defence Instruction requires all reported incidents to be recorded in DECMS. Table 3.1 outlines whether the four DIAs have mandated the use of DPSMS or DECMS to record and manage incidents and investigations.

Table 3.1: Defence procedures governing the use of case management systems

DIA	ANAO assessment of case management system requirements	
	Prior to May 2024, was DPSMS mandated?	Since May 2024, is DECMS mandated?
Investigations and Public Interest Disclosures Branch (IPIDB)	**Yes.** The draft Fraud Control Instructions (FCIs) required the use of DPSMS 'to record all incidents, decisions, investigation and recovery activity.'	**Yes.** DECMS business rules, finalised in September 2025, require the use of DECMS to 'manage all information relating to the recording, analysis and investigation of notifiable incidents.'
Joint Military Police Unit (JMPU)	**Yes.** The Military Police Manual requires that all incidents and investigations are recorded on DPSMS.[a]	**Yes.** JMPU business rules require the use of DECMS to manage all information relating to the recording, analysis and investigation of notifiable incidents. The Military Police Manual has not been updated to reflect DECMS.

62 Section 29(2A) of the *Public Interest Disclosure Act 2013* outlines circumstances where 'personal work-related conduct' can be considered as disclosable conduct (see footnote 8).

DIA	ANAO assessment of case management system requirements	
	Prior to May 2024, was DPSMS mandated?	Since May 2024, is DECMS mandated?
STA Branch	**Yes.** The Security Investigation Operating Guidelines required the use of DPSMS 'to record all matters, decisions, investigations and recovery activity.'	**Yes.** The Security Investigation Operating Guidelines were updated in October 2024 to reflect the implementation of DECMS.
Human Resources Services Branch	**Partial.** The Branch established procedures for the use of DPSMS however did not mandate that DPSMS be used for all investigations.	**Partial.** The Branch has established procedures for the use of DECMS however does not mandate that DECMS be used for all investigations.

Note a: As outlined at Table 2.3, the Military Police Manual also states that Level One Offences under JMPU's Jurisdiction Model do not constitute notifiable incidents and are not to be raised on DPSMS.

Source: ANAO analysis of Defence documentation.

3.9 In March 2025, DECMS guidance was developed by IGADF which states that 'All IGADF matters are to be recorded in DECMS'. The IGADF's use of DECMS for inquiries 'did not commence at go-live on 17 May 2024' as 'there were system issues which raised privacy concerns.' IGADF advised the ANAO in May 2026 that the privacy concerns included that 'IGADF matters were not operating as confidential, standalone cases' and that 'areas of Defence could be inappropriately notified of the existence of IGADF inquiries, contrary to established confidentiality and privacy expectations.' The privacy issues were resolved in 'late 2024' and from August 2025, IGADF had commenced using DECMS for recording inquiries, including for cases back to 1 July 2024.

3.10 DECMS supports the centralised recording of fact-finding. The Defence Instruction requires all reported incidents to be recorded in DECMS but has not established enterprise-level arrangements mandating its use for recording fact-finding activity conducted in response to incidents. The Good Administrative Decision-Making Manual also does not establish a requirement to record fact-finding in a specific system or centralised location.

3.11 Defence advised the ANAO in May 2026 that fact-finding officers are assigned the relevant incident in DECMS and that 'Once Fact Finding is completed, the information is forwarded to the decision maker, who is required to manage the incident, including management of documents and completion of activity tasks, within DECMS'.

Incident data

3.12 Investigations and inquiries do not meet established DIA-level performance measures for timeliness. Defence has not established enterprise-level performance measures for investigations.

3.13 Deficiencies were identified in the DECMS data, including:

- 107 investigations or inquiries with a 'Case Status' of 'Closed' with no recorded 'Case End Date';
- 354 investigations or inquiries with a 'Case Status' of 'Closed' where the 'Case Outcome' was 'Not assigned'; and
- 22 incidents and 15 investigations with duplicate case reference numbers but different values in key fields such as 'Case Outcome' and start and end dates.

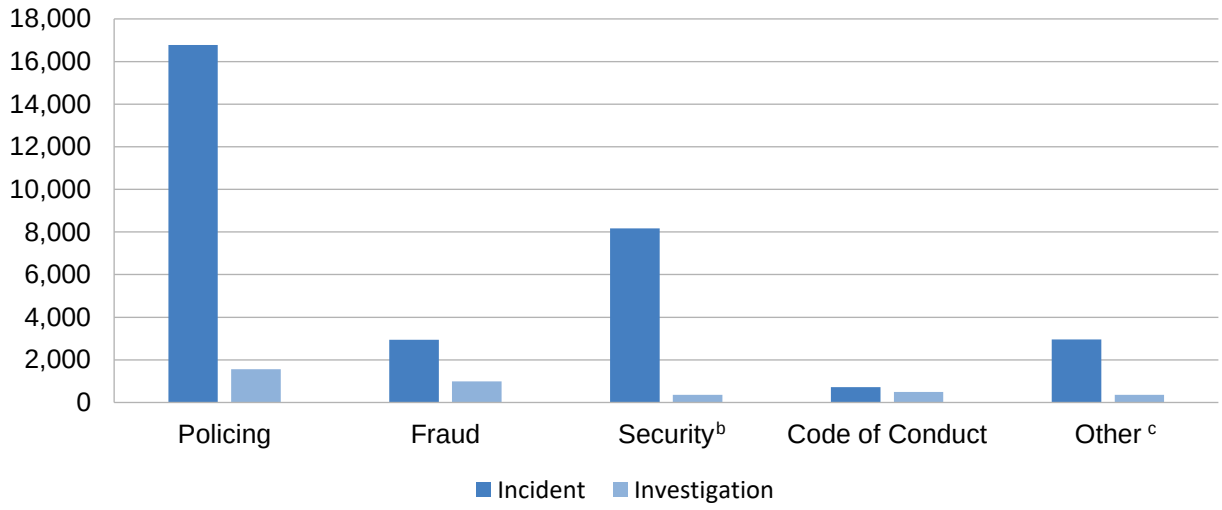
3.14 As outlined at paragraph 3.5, system performance and reporting limitations have been identified. This has limited Defence's ability to provide the ANAO with comprehensive data on reported incidents and investigations across Defence for the audit period (1 January 2020 to 31 December 2025).

3.15 DECMS data provided by Defence records 31,657 reported incidents allocated to DIAs between 1 January 2020 and 31 December 2025. This included incidents with an 'Incident category – Level 1' of:

- policing — 16,770 incidents (53 per cent) including traffic incidents, sexual offences, theft, endangering morale, and absence without leave;
- fraud — 2,943 incidents (nine per cent) including conflicts of interest, corruption, and entitlement and allowance fraud;
- security — 8,173 incidents (26 per cent) including inappropriate handling, access or loss of Defence data, unauthorised disclosure of Defence information, lost or stolen security passes, and suspicious activity;
- Code of Conduct — 721 incidents (two per cent) including poor performance, conflicts of interest, non-performance of duties and ICT misuse; and
- 87 incidents (less than one per cent) that did not have a recorded incident category.

3.16 Figure 3.1 outlines the volume of incidents and investigations, by category, as recorded in DECMS between 1 January 2020 and 31 December 2025. This shows that the progression of incidents to investigation varies depending on the incident category. This variation may be due to the diverse nature of incidents reported to each DIA and differing evidentiary burdens for investigations. Security incidents were the least likely to proceed to investigation (four per cent), and code of conduct incidents were most likely to proceed to investigation (69 per cent).

Figure 3.1: Incidents and investigations by category, 1 January 2020 to 31 December 2025[a]



Note a: DECMS data included: 69 investigations allocated to the Human Resources Services Branch where the investigation category included fraud; 74 investigations allocated to the JMPU where the investigation category was recorded as 'Security'; 20 incidents recorded as 'Code of Conduct' or 'Policing' that involved elements of fraud; and 11 investigations involving elements of fraud that were recorded under non-fraud-related categories including 'failure to follow directions', 'misconduct' and 'policing'.

Note b: Defence advised the ANAO in March 2026 that 'the total number of Security Reports received for the period 1 January 2020–15 May 2024 was 54,799'. Not all Security Reports are escalated to an 'incident' in DECMS.

Note c: 'Other' comprises 2,963 incidents with categories including: 'Duty Log' (1,951); 'Misconduct' (318); 'Maladministration' (176); 'Prohibited Substances' (56); 'Procurement Complaint' (54); 'Nuisance Calls' (49); 'Conduct' (46); 'Work Health and Safety' (43); 'PID Offences' (28); 'ADF Member Incident' (24); and 'Grievance' (24).

Source: ANAO analysis of Defence data.

3.17 The IGADF records inquiries in DECMS. For non-professional standards inquiries it was unable to provide system data which distinguished between submissions received and subsequent inquiries, limiting the ANAO's ability to conduct analysis of IGADF inquiry data.

3.18 In addition to recording these inquiries in DECMS, the IGADF maintains an excel spreadsheet recording non-professional standards inquiries to support internal reporting and management. Of the 79 closed inquiries recorded in this spreadsheet between 1 January 2020 and 11 December 2025, unacceptable behaviour was the most common IGADF inquiry topic (44 per cent), followed by failure of process (15 per cent), and administration mismanagement (10 per cent). Inquiry data is also recorded on DECMS, however the use of spreadsheets for manually recording inquiry information presents data integrity and security risks.

Investigation timeframes

3.19 For closed cases recorded in DECMS between 1 January 2020 and 31 December 2025, the average:

- time from the investigation start date to end date, by DIA was: IPIDB — 141 days (median 75 days); Human Resources Services Branch — 147 days (median 119 days); JMPU — 215 days (median 171 days); and STA Branch — 266 days (median 194 days);
- time from an incident being reported to the start date of an investigation by DIA was: IPIDB — 91 days (median 25 days)[63]; Human Resources Services Branch — 55 days (median 15 days); JMPU — 41 days (median seven days); and STA Branch — 27 days (median five days); and
- length of time between incidents being reported and subsequent investigations being finalised across the DIAs was 196 days (median 160 days).[64]

3.20 DECMS data for IGADF military police professional standards cases included fields for 'Case Start Date' and 'Case End Date' but did not include a field for 'Incident Reported Date'. The IGADF DECMS data also did not distinguish between professional standards assessments, inquiries and investigations. IGADF advised the ANAO in May 2026 that 'Internal processes have been amended and staff in the Professional Standards Cell have been directed to ensure all relevant fields within the database are completed correctly and in a timely manner'. The average time between the 'Case Start Date' and the 'Case End Date' for closed professional standards assessments, inquiries and investigations between 1 January 2020 and 31 December 2025 was 269 days (median 216 days).

63 This figure excludes 12 cases with a 'Case Type' of 'Fraud Recovery Case'. These cases are established to record the recovery of fraud related debts.

64 This figure was calculated using all relevant incidents and investigations allocated to DIAs between 1 January 2020 and 31 December 2025. As there is variation in the volume of investigations conducted by each DIA, this will impact the extent to which the timeliness of each DIA contributes to the overall timeliness figure.

3.21 For closed non-professional standards IGADF inquiries between 1 January 2020 and 11 December 2025, the average length of time between 'inquiry directions being issued' and 'inquiry reports being signed' was 386 days (median 334 days). The IGADF advised the ANAO in May 2026 that 'matters examined by the IGADF are of a complex nature and a high emphasis is given to approaching investigations in a trauma informed and trauma responsive manner which will invariably extend the length of time a case remains open. The time period reviewed by the ANAO also includes the COVID pandemic which introduced many complicating factors and delayed the completion of inquiries as travel and the collection of evidence was severely restricted.'

3.22 A September 2023 Independent Landworthiness Board report noted that CDF Directive 25/2019 requires all incidents of alleged breaches of the Military Police Code of Conduct to be referred to IGADF, including minor incidents that could be managed at a unit level.[65] The report observed that the time taken by IGADF to conduct inquiries presented avoidable mental health and employability impacts to ADF military police and noted that affected individuals are not permitted to perform all military police duties while the subject of IGADF inquiries.

3.23 Each DIA has established targets for investigation timeliness. The Human Resources Services Branch has established targets for the completion of code of conduct investigations within 72 days. STA Branch's Security Investigation Operating Guidelines state that 'most investigations are expected be completed within 90 business days' of investigation plan approval and that extensions can be approved by the Assistant Secretary STA based on 'factors arising on a case-by-case basis.'

3.24 JMPU's Military Police Manual states that 'minor' investigations for Level 1 and Level 2 offences (see Table 2.3) are to be completed within 120 working days 'where possible'. The manual does not establish timeframes for investigations into Level 3 or Level 4 offences, however Defence advised the ANAO in March 2026 that JMPU applies the 120 working day timeframe across all investigations.[66] There is merit in JMPU codifying this requirement in the manual.

3.25 Public Interest Disclosures are subject to legislated timeframes in the *Public Interest Disclosure Act 2013* (PID Act), including making a decision about the allocation of a disclosure within 14 days, and the completion of investigations within 90 days, unless an extension is granted by the Commonwealth Ombudsman's Office. Defence advised the ANAO in March 2026 that IPIDB 'established team-level key performance indicators (KPIs) and measures in May 2024' including completing assessments of reported incidents within 21 days and finalising non-criminal cases within 120 days. IGADF's 2023–25 Strategic Plan sets 'goal measures' to complete 85 per cent of referral assessments for military police professional standards matters within 110 days; 85 per cent of redress of grievance complaints within 90 days; and 85 per cent of inquiries into ADF member deaths within one year of inquiry directions being issued.

3.26 During the audit period, DIAs and the IGADF reported on the timeliness of investigation and inquiry activity, including through:

- JMPU's Provost Marshal of the Australian Defence Force (PMADF) biannual report, provided to the Joint Military Police Governance Board (JMPGB);

65 The Landworthiness Board was convened in September 2023 to review Defence's land-based ADF military policing capability, on the direction of the Chief of Army.

66 The manual also states that 'All investigations, are where practicable, to be completed within 30 working days of commencement.'

- Human Resources Services Branch quarterly reporting to the First Assistant Secretary People Services and Wellbeing;
- IPIDB provides biannual reporting to the Commonwealth Ombudsman on compliance with PID Act timeframes, however has not established mechanisms for the regular reporting of timeliness for fraud investigations; and
- the IGADF Annual Report, provided to the Parliament.[67]

3.27 Timeliness targets have not been met for the DIAs or IGADF. The Australian Public Service Commission's (APSC) Handling Misconduct guide notes that investigation timeliness is important as:

> Delays can affect the availability of reliable evidence, and the capacity of the person under investigation to respond fully to the case against them. For these reasons, among others, delays in investigations can reduce the likelihood of reaching a concluded view on whether the person did what they were alleged to have done.

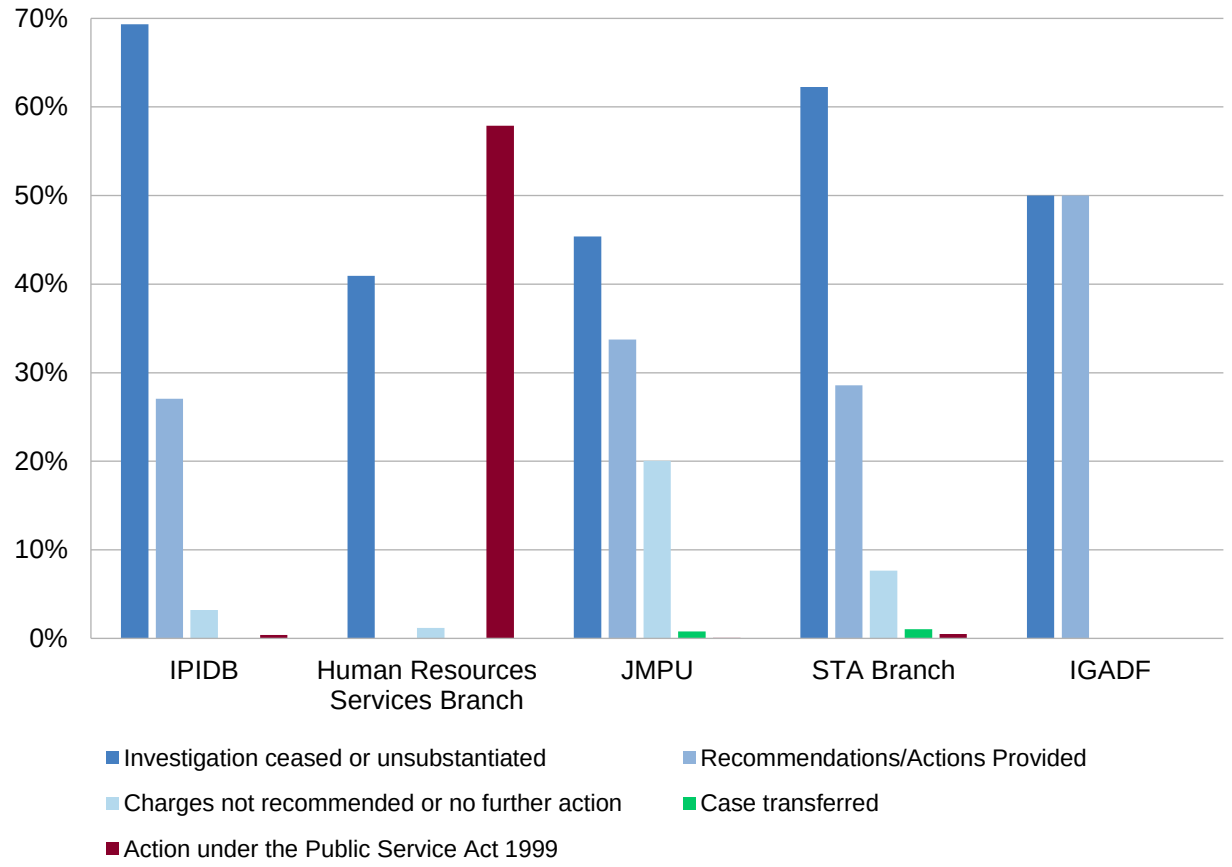
3.28 The Royal Commission into Defence and Veteran Suicide report stated that lengthy inquiry timeframes are 'unsatisfactory' as they can have adverse impacts on the wellbeing of those involved, and recommendations made may lose their relevance and impact over time. In response to the report, the Australian Government agreed to improve transparency and accountability of the IGADF through the publication of guidance or Standard Operating Procedures, including quality assurance and performance measures, where appropriate. While the Royal Commission findings were made in relation to IGADF inquiries, the findings may also be relevant for other investigation and inquiry activities conducted in Defence.

Investigation and inquiry outcomes

3.29 As discussed at paragraph 2.5, Defence's investigative framework is complex, supported by different processes for each DIA, and different legislative frameworks applicable to ADF members and APS personnel. As a result, investigation outcomes differ across Defence's investigative functions. Figure 3.2 outlines investigation outcomes by the DIAs and IGADF as recorded in DECMS between 1 January 2020 and 31 December 2025.

67 Inspector-General of the Australian Defence Force, *Inspector-General of the Australian Defence Force Annual Report 2023–24,* IGADF, Canberra, available from https://www.igadf.gov.au/system/files/2025-07/2023-24%20IGADF%20Annual%20Report.pdf [accessed 31 March 2026].

Figure 3.2: Investigation outcomes by DIA and IGADF between 1 January 2020 and 31 December 2025



Note: This figure excludes 103 cases where the investigation outcome was recorded as 'Not assigned' and 84 cases where outcomes could not be clearly mapped to one of the categories listed in Figure 3.2.

Source: ANAO analysis of Defence data.

3.30 For all DIAs except the Human Resources Services Branch, the most common outcome was investigations being ceased due to insufficient evidence or the matter being unfounded. IPIDB recorded the highest proportion of investigations ceased (69 per cent), and the Human Resources Services Branch recorded the lowest proportion (41 per cent). The high proportion of IPIDB investigations ceased may reflect the higher burden of evidentiary proof required for criminal investigations.

3.31 The 'Recommendations/Actions Provided' outcome category in Figure 3.2 includes administrative action, charges under the DFDA, and action under the *Public Service Act 1999*. Defence DECMS data did not include these more detailed outcomes against cases where the recorded outcome was 'Recommendations/Actions Provided'.

3.32 ANAO analysis of data from Defence's previous case management system (DPSMS) identified that, between 1 January 2020 and 15 May 2024, investigations which substantiated allegations most commonly resulted in either: action under the *Public Service Act 1999* (Human Resources Services Branch); charges under the DFDA (JMPU); or administrative action (STA Branch, IPIDB, and IGADF). As discussed at paragraphs 1.3–1.4, ADF members and APS personnel are subject to different legislative frameworks for administrative and disciplinary matters, including through the DFDA and the *Public Service Act 1999.*

3.33 Defence was not able to provide evidence on actions taken by units and business areas in response to investigation outcomes for at least five cases. One IGADF inquiry from October 2024 was identified where the relevant unit took no subsequent action against a member as the unit was not satisfied that the inquiry sufficiently considered relevant evidence or that procedural fairness had been provided to the member.[68]

3.34 A November 2021 IGADF own-initiative inquiry report into *Implementation of Military Justice Arrangements for Dealing with Sexual Misconduct in the Australian Defence Force* stated there was an 'increasing trend towards the use of administrative action and away from the Defence Force Discipline Act' and that Defence is 'unaware of how consistently and rigorously administrative action is applied'.

3.35 There is overlap in the jurisdiction of DIAs and there is limited guidance on assigning and referring cases between the DIAs (see paragraphs 2.37–2.80). Differences in investigation processes across the DIAs and IGADF present risks that similar cases are not dealt with proportionately or equitably across Defence.

3.36 Acknowledging that matters will involve varying circumstances and evidence, a review of DECMS data identified three DIAs (IPIDB, JMPU and Human Resources Services Branch), which had recorded 63 closed investigations with a recorded incident category or sub-category of 'Conflict of Interest', between 1 January 2020 and 31 December 2025.

- Eleven investigations were conducted by the Human Resources Services Branch, of which three had a recorded outcome of sanctions imposed under the *Public Service Act 1999*.
- Forty-nine investigations were conducted by IPIDB, of which: 13 resulted in recommendations being made; five were referred back to units; and two recorded an outcome of 'No charges'.
- Three investigations conducted by JMPU were either ceased or unsubstantiated.

3.37 One IPIDB investigation into a conflict of interest matter in February 2023 found that undeclared conflicts of interest existed within a unit and that additional undeclared conflicts were 'probable'. The investigation report noted that the matter was handled as an administrative inquiry to protect operational security. This approach was taken in recognition that criminal proceedings would require significant legal action and formal authority to identify protected witnesses and respondents, and that the 'established facts would not necessarily warrant' criminal prosecution.

Reporting arrangements

3.38 Enterprise-level reporting by Defence on the trends and outcomes of incidents and investigations across DIAs and IGADF is not conducted. The 2026 Defence Instruction does not establish requirements for regular reporting by DIAs. Previous Defence instructions established reporting requirements, including:

68 The IGADF twenty-year review (see paragraph 1.28) noted that it was 'aware that in a minority of instances the loop between the IGADF and the ADF has not been closed in respect of an inquiry report's recommendation' and recommended that the IGADF should have an express legislative power to follow up recommendations from IGADF inquiries and investigations.

- Defence Instruction ADMIN 45-4 (see paragraph 2.19) required quarterly reporting on compliance with the Defence Investigation Standards Manual to the quarterly Head Defence Investigative Authorities Conference (HDIAC) (see paragraphs 3.42–3.46); and
- Defence Instruction FIN 12-1 (see paragraph 2.15) required: reporting by DIAs to the Inspector-General Defence Group (now Defence Integrity Division) on systemic weaknesses in Defence and patterns of offences that may be revealed through assessments and investigations of fraud-related matters; and annual reporting to the Secretary and Chief of the Defence Force (CDF) on the outcome of fraud investigations and trends.

3.39 The JMPU provided evidence of quarterly strategic intelligence reporting provided to Defence's Senior Leadership Group, which included detail on incident trends over the relevant quarter.[69] Defence advised the ANAO in May 2025 that the Human Resources Services Branch 'was not classified as a DIA during the period that this Instruction was in force … and therefore was not required to comply' with the fraud reporting requirements of Defence Instruction FIN 12-1.

3.40 The requirement for annual reporting to the Secretary and CDF on the outcome of fraud investigations and trends was retained in Defence Instruction FIN 12-1 until its cancellation in August 2022. Defence advised the ANAO in May 2025 that annual reporting has been provided to the Secretary and CDF through annual reporting from the Defence Audit and Risk Committee (DARC) to the Secretary and CDF, and the Chief Financial Officer's annual significant non-compliance report. This reporting did not include information on the outcomes of fraud investigations and trends within Defence.

3.41 Table 3.2 outlines a summary of reporting arrangements established by DIAs and IGADF. Each investigative function has established reporting arrangements. These arrangements do not provide a consolidated view of investigation and inquiry performance at an enterprise level. This limits the Secretary and CDF's visibility of emerging trends, risks, and opportunities across Defence's investigative functions.

Table 3.2: DIA-level and IGADF reporting arrangements

Investigative entity	Reporting
IPIDB	• Biannual fraud control reporting of fraud losses and recoveries across all DIAs to the DARC and quarterly reporting to the Enterprise Business Committee (EBC) on key investigation updates, outcomes, statistics and trends (see paragraphs 3.48–3.58). • Biannual briefing to the Secretary on referrals made to and from the NACC, and notices and directions issued to Defence by the NACC. • Biannual reporting on Public Interest Disclosures (PIDs) to the Commonwealth Ombudsman, and annual reporting in the Defence Annual Report.[a] • Monthly investigation reporting on active IPIDB matters to the First Assistant Secretary Defence Integrity.
STA Branch	• Quarterly Control Owner reporting to the Defence Security Committee.[b] • Briefs provided to the Associate Secretary at 'approximately six week intervals' to provide an update on the status of sensitive security investigations.

69 The Defence Senior Leadership Group includes all star-ranked and Senior Executive Service personnel.

Investigative entity	Reporting
JMPU	• Annual reporting to the Chiefs of Services Committee to provide an overview of JMPU performance. • Biannual reporting to the Joint Military Police Governance Board (JMPGB) to provide an overview of incident and investigation volumes and trends.[c]
Human Resources Services Branch	• Quarterly reporting to the First Assistant Secretary People Services on incident and investigation volumes and trends. • Annual reporting to the Australian Public Service Commission (APSC) to support the APSC's Annual State of the Service Report.
IGADF	• Monthly brief to CDF to provide an overview of the volume and status of cases, and to outline specific cases of interest.[d]

Note a: This reporting supports the Commonwealth Ombudsman's obligation under the *Public Interest Disclosure Act 2013* to prepare biannual reports on the operation of the Act.

Note b: Quarterly control reporting was conducted 'until the introduction of DECMS in May 2024.' Quarterly reporting recommenced in September 2025 including data backdated to July 2024.

Note c: JMPU was unable to locate JMPGB records for the years 2021 and 2022. Defence advised the ANAO in March 2026 that 'From 2021 onward, the PM-ADF adopted an annual reporting cycle, resulting in the cessation of biannual reporting by JMPU in alignment with this enterprise-level change'. Despite this change, biannual reports were produced for the periods July 2022 to December 2022 and January 2023 to June 2023.

Note d: The IGADF advised the ANAO in March 2026 that the monthly briefs to the CDF 'ceased before October 2025' and that 'IGADF is preparing to publish quarterly data of the type previously included in his briefs to CDF on the IGADF website.'

Source: ANAO analysis of Defence documentation.

Head Defence Investigative Authorities Conference

3.42 Defence Instruction ADMIN 45-4 Defence Investigation Standards required quarterly reporting on compliance with the Defence Investigation Standards Manual to the Head Defence Investigative Authorities Conference (HDIAC), with any instances of non-compliance to be managed by the IGADF. The role of the HDIAC was to 'oversee the development of Defence investigation policy and to guide the direction of the Defence investigative effort on behalf of the CDF, Secretary and Service Chiefs'. It comprised of the head of each DIA, (excluding the Human Resources Services Branch, which became a DIA in July 2022) and representatives from IGADF, the Office of the Director of Military Prosecutions (ODMP), and JMPU as permanent observers.

3.43 Since 2008, the HDIAC has not met quarterly as required under its business rules.[70] The minutes of the December 2019 HDIAC meeting noted that the following meeting would 'focus on the merits of turning off the HDIAC' and that:

> PM ADF [Provost Marshal Australian Defence Force] … proposed that the HDIAC Permanent Members … attend the next JMP GB in Mar 20 as observers with a view to establishing the potential viability of a Joint Military Police/Defence Investigative Authority under a Joint Sec/CDF Directive in lieu of continued HDIAC Mtgs.

70 Unsigned HDIAC business rules, developed in 2008, stated that 'The HDIA will meet quarterly or as required by the permanent members'. Updated business rules in 2013 (unsigned) stated that 'The HDIA conference will meet not less than quarterly, or as directed by the Chair.' One signed version of the business rules was located, dated August 2018.

3.44 The requirement for ongoing HDIAC meetings and the establishment of new arrangements 'in lieu of' continued HDIAC meetings was not discussed at the subsequent April 2020 JMPGB meeting.[71] There are no records of any HDIAC meetings after December 2019.

3.45 Following the final HDIAC meeting in December 2019, there have been no formalised arrangements put in place for meetings between all DIAs to discuss investigations. Defence advised the ANAO in March 2026 that, since October 2023, Defence has conducted an informal monthly 'DIA sync meeting' to cover areas relating to recruitment and staffing, techniques and methods, and training and development. Prior to May 2025, JMPU, which is the DIA responsible for the largest number of investigations, wasn't included in the DIA meetings.

3.46 Enterprise-level reporting on the trends and outcomes of incidents and investigations across DIAs and IGADF is not conducted.[72] Since the cancellation of Defence Instruction FIN 12-1 in August 2022, Defence has not established a requirement for DIAs to report the outcomes and trends of fraud incidents and investigations to IPIDB. Defence has also not put in place enterprise-level arrangements to measure the performance and compliance of its investigative functions. This limits Defence's visibility of enterprise-level investigation risks, trends and outcomes.

Recommendation no. 5

3.47 The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, implement enterprise-level oversight mechanisms to support an end-to-end investigative framework and monitor:

(a) DIA and IGADF performance relating to investigation outcomes and timeliness; and

(b) actions taken by business areas and units in response to investigation findings and recommendations.

Department of Defence response: *Agreed.*

Recording and reporting of fraud losses

3.48 Defence reporting on fraud losses and recoveries is not complete and fraud-related debts have not been managed in accordance with the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). Section 11 of the Public Governance, Performance and Accountability Rule 2014 (PGPA Rule) requires that entities pursue the recovery of debts unless: it is not considered economical to pursue debt recovery; the debt is not legally recoverable; or the debt has been appropriately written off.

3.49 Defence's Accountable Authority Instruction 7 (AAI7) reflects the requirement to recover financial losses. AAI7 states that, while the Secretary for Defence, or their delegate, may decide to

71 The JMPGB is the most senior and primary governance mechanism for joint military policing capability and supports Defence's Chief of Personnel to address enterprise-wide strategic policing matters, gaps, risks, issues and opportunities. The JMPGB is scheduled to meet twice per year and is comprised of the PMADF (JMPU), the IGADF, and representatives from Defence Services and Groups.

72 Similar findings were made by the Royal Commission into Defence and Veteran Suicide which noted that 'Defence is failing to compile, use and learn from the vast amounts of unacceptable behaviour data it collects each year.'

not recover (or write off) a debt, 'Only the Minister for Finance or their delegate can approve a debt waiver that permanently extinguishes a debt'.

3.50 The Defence Investigation Standards Manual (cancelled in December 2023) also included requirements relating to recovery action, including that DIAs:

- have policies in place that outline the legislative requirements for recovery of losses;
- have processes in place for referring matters to the appropriate authority for recovery action; and
- record the financial value of fraud losses and track debt recovery.

3.51 IPIDB's Fraud Control Instructions (FCI) established procedures 'with regard to debt recovery for all fraud and conduct-related debts within Defence … to ensure a consistent, lawful and professional approach to the recovery of fraud and conduct-related debts'. IPIDB's updated governance documents (see paragraphs 2.40–2.41) do not include finalised guidance for the referral and recovery of fraud-related debts. Accountable Authority Instruction 1 (AAI1) outlines one of the responsibilities of the First Assistant Secretary Defence Integrity as 'fraud-related and corruption-related debt recovery'.

3.52 The Defence Integrity Division (DID) provides a quarterly update to Defence's Enterprise Business Committee (EBC) and a biannual fraud control report to the Defence Audit and Risk Committee (DARC).[73] These reports include detail on the number of fraud and corruption incidents reported, investigations closed, the financial loss associated with fraud, and losses recovered. Table 3.3 outlines the estimated fraud losses and recoveries as reported to the DARC between September 2021 and September 2025.

Table 3.3: Estimated fraud losses and recovery reported to DARC between September 2021 and September 2025

Metric	2020–21	2021–22	2022–23	2023–24	2024–25
Number of closed investigations	191	150	141	153	96
Estimated fraud loss[a]	$1,650,305[b]	$596,221	$1,665,578[c]	$2,609,675	$639,044
Value recovered[d]	$302,035	$205,677	$1,448,571[e]	$2,303,729[f]	$99,372

Note a: Estimated fraud loss figures are based on fraud investigations closed during the relevant financial year, regardless of when the investigation commenced.

Note b: This figure was reported in the September 2021 biannual fraud control report. The December 2024 biannual report amended this figure to $1,326,440 (a reduction of $323,865). This case is discussed at paragraph 3.54.

Note c: This figure was reported in the November 2023 biannual fraud control report. The December 2024 biannual report amended this figure to $1,968,057 (an increase of $302,479). Defence advised the ANAO in November 2025 that the amendment was due to quality assurance activities which 'identified that the estimated fraud loss for the 141 cases closed was incorrect.'

Note d: Recovery figures include all fraud recovery payments received in the financial year, regardless of the year in which the investigation was closed.

73 The EBC is responsible for exercising strategic control over the corporate and military enabling functions of Defence. The DARC's role is to provide independent advice to the Secretary and CDF and review the appropriateness of Defence's financial and performance reporting, system of risk oversight and management, and system of internal control.

Note e: This figure includes a fraud case related to a Defence contractor with a fraud value of $1,377,897, of which the full amount was recovered (see Case Study 1).

Note f: This figure includes a fraud case related to a Defence contractor with a fraud value of $2,119,144, of which the full amount was recovered (see paragraphs 3.55–3.56).

Source: ANAO analysis of Defence documentation.

3.53 The estimated losses to Defence vary year on year, with variations in 2022–23 and 2023–24 largely driven by fraudulent activity by Defence contractors. Defence's recovery of funds significantly increased between 2022–23 and 2023–24, largely reflecting the recovery of funds for two individual cases related to high-value contractor frauds.

3.54 The estimated fraud loss for 2020–21 was amended in December 2024 after the loss was attributed to an administrative error rather than fraud. The June 2021 case involved a vendor providing incorrect account details to Defence, resulting in Defence payments being made to the incorrect vendor in March and May 2018.

- The payments were withdrawn from the vendor account by an unknown actor and the vendor did not engage with Defence following efforts to recover the erroneous payments.
- Defence considered it plausible that the vendor knew it was receiving funds it was not entitled to and that 'an opportunistic criminal offence may have been committed by person/s unknown that operated the [incorrect vendor] Account from where the funds were withdrawn, embarking on criminal investigation would be protracted and complex'.
- Defence decided not to pursue a criminal investigation citing 'There are other more efficient avenues available to Defence to pursue recovery of the funds that are less likely to attract unwanted attention to such a sizeable error by Defence. Therefore, a criminal investigation is not warranted, appropriate or recommended.' Defence negotiated repayment of the full debt amount from the vendor's bank in October 2025.

3.55 In August and September 2023, IPIDB received allegations of Defence contractor fraud across ten Defence projects between November 2020 and August 2023.

- An Investigation Plan developed in October 2023 focused on the awarding of contracts for two Defence projects. An investigation report, finalised in May 2024, found that an employee of the contractor invoiced Defence for work not completed. Defence was reimbursed $2,119,144.
- The report stated that a criminal prosecution was not pursued based on factors including: funds were repaid; there was 'no fraud committed against Defence'; the matter was reported to the National Anti-Corruption Commission and New South Wales Police; and resourcing implications if an investigation was to be considered to determine whether a criminal offence had been committed under the *Criminal Code Act 1995*. As an example and acknowledging that each case is assessed on the facts and merits of that case, this contrasts with a previous IPIDB investigation, completed in January 2020, which noted that the CDPP have referred to a $20,000 fraud as serious and 'warranting consideration of a custodial sentence'. Noting this and the size of the potential contractor fraud, there would have been merit in Defence engaging with the CDPP and other relevant federal agencies such as the AFP to ensure a referral was not warranted.

3.56 The key deficiencies in this case included the following.

- A previous complaint against this contractor had been raised in November 2022, which was not recorded in DPSMS, contrary to IPIDB guidance, which required all incidents and decisions to be recorded in DPSMS.
- The investigation report noted that IPIDB conducted inquiries regarding the over-inflation of quotes. It further stated that the over-inflation of quotes and invoices 'are outside the remit of [the Directorate of Investigations]' and that 'Responsibility of these issues rests with SEG [Security and Estate Group] as the contract manager'. Defence referred the matter to the relevant business area, however there is merit in Defence establishing clear reporting mechanisms to enable instances such as these to be considered in aggregate and identify patterns that may indicate more serious risks.
- One of the contractor staff involved in providing investigation evidence to Defence was alleged by the original complainant as having been made aware of potential fraudulent activities against Defence and failing to take action in response. The complainant provided documentation to support their assertion. There is no evidence that Defence considered this element of the complaint or assessed what risks it may have presented to the integrity of the investigation.
- Four projects were identified involving allegations of inflated invoices. The investigation report noted that these allegations 'were found to be true' for three of the four projects and did not provide a clear conclusion for one project.
  - Credit notes were issued for two of the four projects to the value of $69,022. Defence was unable to locate the credit notes for the other two projects but advised that relevant purchase orders were adjusted to the value of $54,179. The total adjustment across the four projects of $123,201 was not included in the overall fraud value of $2,119,144 reported to the DARC.

3.57 The figures reported to the DARC and EBC are based on incidents and investigations with a category recorded as 'fraud'. Figure 3.1 outlines there were incidents and investigations that involved elements of fraud, which were categorised under non-fraud categories in case management system data. Deficiencies in fraud data and the management of fraud incidents included the following.

- At least five cases were identified as not having corresponding fraud-related entries in case management systems, including one September 2024 case of timesheet fraud (valued at $14,955).
- Not recording fraud values for incidents. For example, an August 2022 case of meal fraud valued at $734 was categorised as a 'fraud' incident in DPSMS but did not have an associated fraud value or recovery amount recorded in the system. Defence was unable to advise whether the loss for this case was recovered or written off.
- Unrecovered fraud-related debts have not been written off, including where the recovery efforts were unsuccessful, not undertaken in a timely manner, or abandoned due to the time elapsed. In one case, Defence accepted partial repayment to settle a larger debt in October 2022 but could not provide evidence of the delegate's approval to do so.

- Non-recovery of fraud-related debts for matters referred back to units for action. In August 2022, an IPIDB investigator identified an instance where the ODMP decided not to prosecute a rental allowance fraud of approximately $16,000 and the matter was referred back to the unit for action. The email noted that 'no action to recover the funds was pursued because of the decision by ODMP … It seems that some units are making unilateral decisions not to refer these debts … for recovery, instead choosing to do nothing.'
- Instances where: fact-finding was conducted into fraud-related incidents that were not reported to a DIA; potential meal fraud matters were not recorded on DPSMS; and fraud losses and recoveries were not recorded or conducted.

3.58 The impact of these issues is that Defence's ability to recover fraud-related debts is reduced and the reporting of fraud-related incidents and investigations to the DARC and EBC does not reflect the full scale of fraudulent activity reported and investigated within Defence. Further, Defence's reporting includes information on fraud losses and recoveries, but it does not include detail on the value of fraud losses written off. This limits the DARC and EBC's visibility over Defence's compliance with Section 11 of the PGPA Rule (see paragraph 3.48).

Recommendation no. 6

3.59 The Department of Defence ensure that Commonwealth and Defence policy requirements for the recovery and write off of fraud-related debts are enforced and that the value of write offs are reported appropriately within the department.

Department of Defence response: *Agreed.*

Quality assurance

3.60 None of the DIAs nor the IGADF have established quality assurance arrangements that align with AGIS, and three DIAs have undergone external quality assurance reviews since January 2020. These reviews identified deficiencies in record keeping, the provision of procedural fairness, the consideration of investigation evidence, and decision-making impartiality.

3.61 The AGIS sets out quality assurance requirements including, the requirement for entities to have a Quality Assurance Policy for investigations, with regular quality assurance activities, and a formal external assurance activity every two years.[74] Outcomes of the quality assurance activity are to be reported to the relevant entity Committees or Executive.

3.62 Defence has not established quality assurance requirements for investigations at an enterprise level.[75] None of the four DIAs or IGADF have established a Quality Assurance Policy as required under AGIS. Three DIAs (IPIDB, Human Resources Services Branch and STA Branch) underwent a management initiated review in January 2020 (see paragraph 2.8).

74 The AGIS outlines five types of quality assurance activities: informal self-review; informal peer review; informal supervisory review; formal internal audit; and formal external audit.

75 Prior to its cancellation in December 2023, the Defence Investigation Standards Manual required that 'All DIAs are to have a written procedure by which their investigations may be the subject of an internal review, analysis, and evaluation or quality assurance.'

3.63 DIAs have established quality assurance arrangements and conducted quality assurance activities as outlined below.

Investigations and Public Interest Disclosures Branch

3.64 The Fraud Control Instructions (FCIs) stated that the AFP would, 'on occasions, conduct Quality Assurance Reviews (QAR) of [IPIDB's] investigative performance.' Defence advised the ANAO in November 2025 that no AFP reviews have been conducted since 1 January 2020. IPIDB provided evidence of an AFP investigation review conducted in March 2019. The review found that the investigation was conducted largely in accordance with the AGIS, but noted that conversations held with the CDPP, attempts to locate the person of interest, and critical decisions made throughout the investigation, were not recorded on DPSMS.

3.65 Two contracted-out quality assurance reviews (September 2020 and January 2022), and one 'own motion investigation' by the Commonwealth Ombudsman (September 2022) were conducted during the audit period (1 January 2020 to 31 December 2025). The reviews found deficiencies in IPIDB's investigation arrangements including that IPIDB was 'partially compliant with the AGIS' due to: inconsistent evaluation of referrals; investigation plans lacking key information on offences, evidence sources, resourcing and timeframes; poor record keeping; investigation reports that were not well structured and did not sufficiently reference supporting evidence; insufficient consideration of exonerating evidence; and procedural requirements that did not align with AGIS.[76] Defence advised the ANAO in November 2024 that IPIDB conducts quality assurance reviews at the completion of every investigation including self-review, peer review, and supervisor review. These reviews are considered 'informal' quality reviews under the AGIS.

Security Threat and Assurance Branch

3.66 STA Branch's investigation procedures require the Director Security Investigations Unit to conduct a quality assurance check of investigation plans and reports before progressing them to the Assistant Secretary STA for approval, and quality assurance checks to be conducted for data entered into DECMS when allegations are referred to another DIA. The procedures do not include requirements for formal internal or external quality assurance reviews.

3.67 A quality assurance review conducted by the Department of Home Affairs in June 2025 found that assessed security investigations were conducted in accordance with AGIS. The review identified one area for improvement, relating to the tracking of recommendations from security investigations.

Human Resources Services Branch

3.68 The Human Resources Services Branch uses the APSC's *Handling Misconduct Guide* to support the conduct of investigations (see paragraph 2.71). The guide recommends entities implement quality assurance mechanisms such as:

- checklists to ensure that procedural steps have been completed appropriately and good records kept;

76 IPIDB's investigation processes did not fully align with 2011 AGIS requirements including in relation to: media engagement; the assessment of incidents; preparation of Briefs of Evidence; exhibit management; and quality assurance. ANAO's assessment of DIA and IGADF process alignment with AGIS is discussed at paragraphs 2.81–2.83.

- periodically auditing a sample of misconduct files to evaluate if correct procedures and record keeping requirements are being followed; and
- analysing misconduct data to track case progress and outcomes and identify trends and high-risk individuals.

3.69 The Branch has not established procedures for the above mechanisms or for formal internal or external quality assurance reviews. External reviews of the Branch are 'primarily through outcomes of Reviews (ie Merit Protection Commission, Fair Work Commission and Federal Circuit Court).'

3.70 Between 1 January 2020 and 31 December 2025, the Branch completed 469 investigations, of which Defence advised that 41 (nine per cent) were reviewed by the Merit Protection Commissioner (MPC). The ANAO examined 28 cases reviewed by the MPC, and of these, the MPC recommended in 15 cases (54 per cent) that Defence's original decision be partially or fully amended due to deficiencies in investigative processes. This included: failure to provide procedural fairness; findings not supported by sufficient evidence or based on insufficient understanding of legislative requirements; and apprehended bias and lack of impartiality in decision-making. In March 2022, one matter considered by the Fair Work Commission identified a failure to consider exculpatory evidence, and investigation findings that were not supported by evidence.

3.71 The APSC's Handling Misconduct Guide states that entities should 'assess the outcomes of reviews conducted by the MPC to identify any concerns about the quality of decision-making in the agency that may point to systemic issues or a need to improve capability'. Defence advised the ANAO in March 2026 that a review of MPC decisions was undertaken in March 2025 'to identify systemic issues and remediation action which has since been put in place to improve capability'.

Joint Military Police Unit

3.72 The Military Police Manual outlines requirements for annual Technical Standards Inspections (TSIs) at all Joint Military Police Stations to assess record keeping and compliance with legislation and policy. Supporting TSI procedures require that TSI 'statistical data is available' for each Joint Military Police Governance Board (JMPGB) meeting.

3.73 The requirement for annual TSI inspections of Joint Military Police Force (JMPF) stations was introduced in August 2020, to take effect from January 2021. Between January 2021 and December 2025, six of the 10 Joint Military Police Stations have been subject to an annual inspection.[77] Of the four stations that were not subject to annual inspections, two (Melbourne and Sydney) have been inspected each year except for 2021, one (JMPU Headquarters Select Investigation Team) was inspected in 2023 and 2025, and one (Butterworth) was only inspected in 2023.

3.74 TSIs identified deficiencies relating to: exhibit management; compliance with case management system record keeping requirements; not conducting periodic reviews of incidents; not completing assessment forms and reports in response to incidents; failure to follow correct procedures for search warrants; and referral of incidents back to units that 'should be assessed by the JMPF [Joint Military Police Force] Assessment Board'. One of the 13 TSI reports reviewed was not signed off by relevant personnel as required by the report template.

77 The 10 stations are Adelaide, Brisbane, Canberra, Darwin, Melbourne, Perth, Sydney, Townsville, JMPU Headquarters, and the Royal Malaysian Air Force Base in Butterworth, Malaysia.

3.75 An abridged TSI conducted into JMPU Headquarters' Select Investigation Team in 2023 identified 'multiple examples' of failures to comply with DPSMS record keeping requirements including: not entering key data such as investigation notes, primary investigator, and the identity of alleged offenders; entering information in incorrect DPSMS fields; and not uploading required investigation documentation, such as investigation reports.[78] The report recommended a 'full audit within six months' and noted that the findings potentially reflected 'a longer-term systemic issue'. The full audit was conducted in July 2025 which identified a 'marked improvement', with minor record keeping and exhibit management issues remaining. Defence advised the ANAO in March 2026 that JMPU's Select Investigation Team 'have been formally incorporated into the JMPU annual TSI audit program'.

3.76 Of the four JMPGB meetings that were held between January 2021 and April 2025 for which minutes could be located, there was one instance (March 2025) where TSI results were discussed.[79] The paper presented to the JMPGB noted recurring issues with compliance with DECMS record-keeping requirements.

3.77 The Military Police Manual does not include requirements for external review of JMPU investigation activities. Since January 2020, there have been no external quality assurance reviews conducted into JMPU investigation compliance or performance. It further notes that 'random checks of Defence Policing and Security Management System (DPSMS) entries should be conducted, when time permits, to ensure compliance with policy and quality of reporting.' Defence advised the ANAO in September 2025 that 'There is no evidence of random checks of DPSMS having been conducted'.

IGADF

3.78 The Directorate of Investigations and Inquiries (DII) Handbook requires that an internal legal review is conducted over decision briefs and briefs of evidence for professional standards cases and inquiry reports prior to submission for delegate approval. During the audit period (1 January 2020 to 31 December 2025) the IGADF had not established requirements for external quality assurance and had not been subject to external quality reviews as:

> JMPU have not conducted annual technical inspections of our records. An interim QA process involves the IGADF DPSMS Manager reviewing the content of DPSMS data against any Objective and case file records prior to closure.

3.79 The Military Police Manual provides that PMADF exercises 'technical control' over all ADF Military Police (MP) and that 'MP elements outside the JMPU, who are undertaking policing tasks or functions, must maintain standards prescribed by the PM-ADF.'[80] JMPU 'informally engaged' with IGADF 'In the last half of 2023 … offering to conduct technical standard inspections of IG-ADF'. Minutes from the March 2025 JMPGB meeting state that the need to maintain IGADF independence was discussed and that IGADF maintains technical assurance of ADF military police seconded from JMPU, through Deputy IGADF oversight. IGADF advised the ANAO in May 2026 that 'as an

78 The Select Investigations team is 'responsible for handling particularly sensitive and complex matters.'

79 As outlined at Table 3.2, Defence was unable to locate records for JMPGB meetings for 2021 and 2022. Defence advised the ANAO in February 2026 that one JMPGB meeting was conducted in 2024. The JMPGB's Terms of Reference state that the Board should meet at least twice per year.

80 Responsibilities of the PMADF, including the exercise of technical control of all ADF Military Police is established in CDF Directive 09/2022 Provost Marshal-Australian Defence Force / Commander Joint Military Police Unit: Responsibilities and Accountabilities.

independent statutory office that oversights the JMPU, it is not appropriate for the JMPU to audit the IGADF.'

3.80 Deputy IGADF oversight is conducted through: the implementation of a formal reporting chain to the Deputy IGADF; monthly updates between the Director of Inquiries and Investigations with the Inspector-General and Deputy IGADF; and Deputy IGADF review and approval of investigation reports. These arrangements do not cover the range of assessments conducted under JMPU TSIs, which include a formalised assessment of investigative processes including: whether incidents have been appropriately assessed; completion of risk assessments and investigation plans; recording of investigation activity; maintenance of exhibits; conduct of interviews and searches; and investigation reporting and closure.

3.81 IGADF advised the ANAO in March 2026 that it 'will seek to establish a mechanism for independent external reviews to provide further assurance on DII practices (and where appropriate other Office of the IGADF activities)'.

Military justice performance reviews and audits

3.82 As discussed at paragraph 1.16, the IGADF conducts military justice performance reviews and audits to assess ADF member understanding of, and compliance with, military justice requirements. This includes assessing the extent to which units comply with notifiable incident reporting requirements and the conduct of fact-findings. The IGADF has developed a Directorate of Military Justice Performance and Review Handbook which outlines requirements for the frequency of audits, selection of units, distribution of reports and the monitoring of audit recommendations.

3.83 Deficiencies identified through IGADF audits include: poor record keeping for investigations and fact-finds; fact-finds being conducted into potential notifiable incidents; not reporting notifiable incidents in accordance with the Defence Instruction; and not reporting relevant matters to the Australian Government Security Vetting Agency (AGSVA). As an example, one IGADF audit conducted in April 2024 noted unit commentary that JMPU sometimes placed 'the burden of undertaking a DFDA investigation back on the unit' and that in one case, a fraud related matter was referred back to the unit 'for reasons that remain unclear'. Defence advised the ANAO in May 2026 that 'decisions to manage matters at unit level are informed by a range of legitimate considerations, including evidentiary complexity, resourcing, legal advice, and an assessment of the most effective and proportionate response'.

Recommendation no. 7

3.84 The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, establish quality assurance arrangements for Defence Investigative Authorities and the IGADF that align with AGIS requirements, including requirements for regular independent external review.

Department of Defence response: *Agreed.*

Privacy breaches

3.85 The *Privacy Act 1988* establishes standards for the collection, use, and disclosure of personal information, and provides the legislative basis for the Notifiable Data Breaches Scheme. Under this scheme, a notifiable breach occurs when there is unauthorised access to, or unauthorised disclosure

of, personal information that is likely to result in serious harm to individuals and the entity hasn't been able to prevent the likely risk of serious harm with remedial action. In these cases, entities are required to notify impacted individuals.

3.86 There were two Defence Incident Records on Defence's intranet that contained sensitive personal information regarding unacceptable behaviour incidents. Defence advised the ANAO in June 2025 that the records were likely uploaded to Defence's intranet from an automated system process and that work was underway to determine if there is a technical solution to address the issue. Defence also advised that the records 'remain available to anyone with the link saved but cannot be searched for or found without the link' and that 'no logs are available of who may have had access' to the records. In response to further ANAO queries, Defence advised that it did not consider the matter to be a notifiable data breach under the *Privacy Act 1988* as '[t]he identified documents have not been accessed by individuals unauthorised to access the documents'. There is merit in Defence obtaining additional assurance that this issue is not more widespread and does not constitute a notifiable data breach.

3.87 In a separate case reviewed by the ANAO, a security incident was reported to the Defence Security Operations Centre (DSOC) in April 2021. An initial assessment conducted by the DSOC in April 2021 identified that an officer within the Office of the Director of Military Prosecutions (ODMP) had been using their personal email and laptop to store sensitive military justice related documents. An STA Branch investigation subsequently determined that these documents 'were likely accessed by an unknown cyber threat actor'. The investigation report did not identify non-compliance with any specific Defence policies. The specific details are outlined below.

- May 2021, Defence submitted a notifiable data breach notification to the Office of the Australian Information Commissioner (OAIC) on the matter.
- October 2021, a 'Harm Assessment' was conducted by an outsourced cyber support service which found that 515 individuals were impacted by the breach and required notification.
- November 2021, Defence requested IGADF inquire into the conduct of the ODMP officer and determine whether there was a 'potential systemic issue' of using personal email addresses among ADF Legal Officers. The ANAO was unable to locate an inquiry plan on file for this matter. The IGADF inquiry identified that up to 12 per cent of ADF legal officers sampled sent information to personal email accounts, and a smaller number had 'concealed the nature of Defence official information' by under-classifying emails when emailing Defence documents.
- The inquiry report noted that, as the officers were selected randomly, no adverse findings were made against the individuals. There is no evidence that any action was taken against the ADF Legal Officers.
- November 2021, a brief provided to the Associate Secretary noted that the OAIC had raised concerns regarding Defence's progress in notifying impacted individuals since becoming aware of the breach in April 2021 and that a notice was required to be posted on Defence's public website as Defence was unable to identify all 515 individuals involved in the data breach. Defence advised the Defence Minister in November 2021 that it would not issue a public notice.

- January 2022, the Associate Secretary wrote to the OAIC seeking an exemption from the requirement to publish information regarding the data breach as it would cause distress to individuals who were not impacted by the breach, noting that not all impacted individuals were able to be identified. Defence was unable to provide evidence of a response from OAIC regarding the exemption. Defence advised the ANAO in December 2025 that it did not publish a notice on its external website and that OAIC was notified of this decision in December 2022.

Have selected investigations been conducted in accordance with the framework?

Investigations and inquiries have not always been conducted in accordance with Defence policy. Deficiencies were identified in: record keeping; investigation and inquiry planning; documentation of key decisions and evidence; the provision of updates to stakeholders; and consultation with relevant authorities. Decisions to investigate or refer matters have been applied inconsistently by Defence, and fact-finding activities have been conducted for notifiable incidents without referral to DIAs, as required by Defence policy.

Referral of incidents for assessment

3.88 Referrals of matters, and decisions to conduct investigations in response to incidents have not been applied consistently within and across DIAs, including in relation to ADF member fraud, sexual misconduct, and security. For example, a July 2023 Defence internal audit found that 3,558 ADF members (49 per cent of those sampled) were non-compliant with the ADF meal entitlements policy, estimating the value of these meals at $357,693.

- JMPU reviewed the 100 members with the highest unentitled meal claims, resulting in the investigation of members who had claimed at least 142 meals (valued at approximately $731) without paying.
- Defence advised the ANAO in May 2026 that ‘as the audit did not identify whether the non-compliances amounted to fraud, or a lack of policy awareness and/or administrative errors no DPSMS incidents were raised for the remaining 3,458 members’. This approach was not consistent with the requirement to record all incidents in DPSMS (see paragraph 2.14). Defence advised the ANAO in March 2026 that there is ‘no record to confirm whether attempts were made to recover any losses in relation to matters that were not investigated’.

3.89 Further, the ANAO identified one instance where a fraud matter, assessed as a Level 3 matter under JMPU’s Jurisdiction Model in April 2020, was not investigated by the JMPU, and the Office of the Director of Military Prosecutions (ODMP) was not consulted on this decision. As outlined in Table 2.3, Level 3 matters are ‘prescribed offences’ under the DFDA. ODMP’s 2019–20 Annual Report stated that ‘an agreement was reached at the end of 2017 to ensure that all potential ‘prescribed offences’ under investigation, in circumstances where a decision was being considered to take no further investigative action by JMPU, would be referred to ODMP for consideration as to the appropriate course of action to be taken.’

3.90 IPIDB referred a May 2024 incident involving a contracted employee forging the signature of an ADF member on an invoice back to the company to resolve. IPIDB assessed that no benefit

was gained by the contractor as the form would 'likely have been signed anyway', and concluded the matter was outside IPIDB's jurisdiction because the person was not a Defence contractor. Accountable Authority Instruction 1 (AAI1), which outlines the First Assistant Secretary Defence Integrity's role in relation to fraud, as well as requirements for personnel to meet standards of governance, performance and accountability, applies to contractors, consultants and outsourced service providers undertaking duties at the direction of Defence.

Fact-finding

3.91 There is no enterprise-level policy which states that DIAs cannot refer reported notifiable incidents to responsible business areas or units for fact-finding or resolution. DIAs have referred notifiable incidents back to units and business areas for fact-finding, including matters related to conflicts of interest, sexual offences, and fraud.

3.92 DIAs have also referred notifiable incidents to CASG for consideration under the Defence Procurement Complaints Scheme (DPCS). For example, on 24 August 2020, the Audit and Fraud Control Division (AFCD), now known as Defence Integrity Division, received a complaint alleging conflicts of interest in a Defence procurement.

- On 25 August 2020, the AFCD referred the matter to CASG. The next day, the same matter was raised with the AFCD by the Defence Minister's office.
- On 27 August 2020, the AFCD determined the matter was a notifiable incident 'requiring oversight by AFCD', reclaimed the matter from CASG and referred it to ADF Headquarters to conduct fact-finding.
- The referral to ADF Headquarters did not provide instruction about not alerting the person of interest, despite guidance that evidence protection should be considered.
- A subsequent IPIDB investigation report, finalised in July 2021, substantiated the allegations and found that CASG had notified the person of interest, providing them with an opportunity to conceal potential evidence. The person of interest advised Defence they altered relevant social media content after they had become aware of the ADF Headquarters fact-finding.

3.93 Fact-finding activities have been conducted in response to notifiable incidents without the incident being reported immediately (or at all) to a DIA, as required under the Defence Instruction. This includes fact-findings in response to allegations of: fraud; probity issues, corruption, or commercial impropriety; security or safety incidents; and sexual offences or misconduct.

3.94 DIAs and the IGADF have identified deficiencies with fact-findings and inquiries including: being subject to bias[81]; findings and conclusions that are not supported by evidence or are outside of the terms of reference; lack of experience; failure to provide procedural fairness; failure to conduct interviews with key witnesses or in accordance with Defence policies and legislation; factual inaccuracies; and poor understanding and application of Defence policies when assessing allegations. Concerns regarding conduct of fact-findings and inquiries formed the basis of at least eleven referrals to DIAs between 1 January 2020 and 31 December 2025.

81 In one case, the decision resulting from a fact-finding was reversed following IGADF requests for information regarding the fact-finding process.

3.95 The conduct of fact-finding activities by units and business areas into notifiable incidents without DIA approval indicates lack of awareness of reporting requirements and associated risks. The lack of systematic recording of fact-finding activities in Defence case management systems means it is unclear how often fact-findings have been used inappropriately or what outcomes have been produced.

Recommendation no. 8

3.96 The Department of Defence implement measures to improve awareness and educate units when fact-finding is appropriate and the approvals requirement for fact-finding into notifiable incidents.

Department of Defence response: *Agreed.*

Assessment of selected investigations and inquiries

3.97 The Military Police Manual states that effective and efficient fraud investigations are best achieved through case-by-case consultation with the other DIAs. This reflects Defence's investigation framework operating as a system-of-systems, where matters may involve multiple authorities over their lifecycle. Under Defence policy, cases involving elements of fraud may be reported to IPIDB, JMPU (for ADF-related fraud cases), the Human Resources Services Branch (for Code of Conduct breaches) and IGADF (for Military Police Code of Conduct breaches). Defence also has mechanisms to refer matters to, or partner with, external entities, including the Australian Federal Police (AFP), state and territory police, the National Anti-Corruption Commission (NACC) and the Commonwealth Director of Public Prosecutions (CDPP). This approach enables complex matters to be addressed, in whole or in part, by the authority best placed to do so. Four of the six case studies in this chapter examine matters related to fraud and the interaction between DIAs and external authorities.

3.98 The Human Resources Services Branch and IGADF have not established arrangements to support the consistent referral of fraud cases to either JMPU or IPIDB for information. Establishing such arrangements would allow Defence to obtain greater enterprise-level oversight on the management of fraud cases, while allowing each DIA to maintain responsibility for their relevant components of cases.

3.99 To assess Defence's application of relevant requirements, one closed investigation from each DIA and IGADF was selected for case study analysis, based on the highest recorded fraud loss between 1 January 2020 and 9 December 2024. Fraud was used as a selection metric as it enabled a comparison of similar cases across DIAs and IGADF and supported assessment of the extent to which DIAs refer and consult on matters that may cross jurisdictional boundaries (see paragraph 1.35).

3.100 The case study selection included one completed investigation conducted by STA Branch into the inappropriate storage of Defence records, which was selected using the methodology above as it was the only STA Branch case with a fraud value recorded in the relevant field (the value was recorded as '0'). One closed IGADF inquiry was also selected for case study analysis, based on the longest time between issuing inquiry directions and the inquiry report being finalised, between 1 January 2020 and 30 June 2025. These cases are outlined in Table 3.4.

Table 3.4: ANAO selected case studies

Case type	Investigative function	Case start and end date	Basis for case selection
Investigation	IPIDB	14 January 2021 – 14 February 2023	Fraud value: $1,377,897[a]
Investigation	JMPU	27 July 2021 – 7 July 2022	Fraud value: $47,854
Investigation	Human Resources Services Branch	5 December 2022 – 28 November 2023	Fraud value: $14,800
Investigation	STA Branch	20 October 2020 – 15 January 2021	Fraud value: $0
Investigation	IGADF	17 August 2023 – 9 January 2024	Fraud value: $17,546
Inquiry	IGADF	1 September 2022 – 14 April 2025	Timeliness: 956 days

Note a: One case was identified with a higher recorded fraud value of $2,119,144. As at 9 December 2024, DPSMS data recorded this case with status of 'open' (noting that DPSMS was replaced with DECMS in May 2024). As such, it was not selected as a case study. Subsequent review of case documents confirmed this case closed on 10 July 2024, and it is discussed separately at paragraphs 3.55–3.56).

Source: ANAO analysis of Defence documentation.

3.101 The ANAO identified deficiencies in compliance with policy requirements across the six selected cases assessed, including common deficiencies such as:

- key documents, investigation evidence, meetings and decisions were not consistently recorded in case management systems, including for other cases referenced throughout this report;
- not following processes for the completion of investigation and inquiry plans;
- not providing or recording required updates to relevant stakeholders; and
- not sufficiently consulting with relevant authorities for fraud-related cases.

3.102 Other deficiencies limited to specific cases included:

- not undertaking assessment activities as directed by supervisors;
- not recording how, or whether, key investigation evidence and witness reliability was considered as part of investigation planning and findings; and
- not referring matters to AGSVA following adverse investigation findings.

Investigations and Public Interest Disclosures Branch

3.103 Case Study 1 outlines a contractor-related fraud that was referred to Defence in December 2020. AusTender data indicates the contractor held 59 contracts with Defence, valued at approximately $433 million, between 1 January 2020 and 1 February 2024. The company entered voluntary administration in February 2024. The case study focuses on Defence's processes only.

Case study 1: Investigations and Public Interest Disclosure Branch

- December 2020: Defence and a statutory government construction authority received allegations of contractor-related fraud. The construction authority referred the matter for Defence's 'consideration and action', advising the construction authority would investigate the matter, and that it had also been referred to an external law enforcement agency.
- January 2021: The Director Investigations requested investigators assess the matter 'in conjunction with' the law enforcement agency including 'the profiling of the Prime Contractor to determine exposure to broader offending'.
- February and March 2021: The DPSMS record was updated to note that: 'Preliminary discussions' had been held with the law enforcement agency and construction authority; 'an Investigation Plan was to be drafted for joint operation' with the law enforcement agency; and that a Joint Agency Agreement would be drafted. No investigation plan was drafted and no Joint Agency Agreement was finalised 'as the assessment did not progress to an investigation'.
- July 2021: DPSMS was updated to note that the law enforcement agency would not proceed with a criminal investigation and that the construction authority had issued a report to the contractor for their response.
- August 2021: The construction authority provided Defence with a report of their investigation findings and the contractor's preliminary response to the findings. The construction authority also provided an additional complaint about the contractor received in July 2021. The construction authority's report found the contractor had submitted falsified quotes to Defence on ten occasions between May 2020 and October 2020. The contractor's response identified 71 further instances of possible fraud across 16 Defence projects.
- July 2022: Defence finalised an Assessment Report highlighting the construction authority's findings that the contractor had breached the *Competition and Consumer Act 2010.* The assessment report determined that no further investigation was required based on factors including that relevant personnel no longer worked for the contractor, and law enforcement agency advice that criminal investigation was 'likely unwarranted as the "…individuals didn't receive a benefit …"'. The Commonwealth Fraud Prevention Centre notes that 'A benefit or loss is not restricted to a material benefit or loss, and may be tangible or intangible. A benefit may also be obtained by a third party.' A 'Statement of Agreed Facts' between the contractor and the construction authority (undated) noted that the fraudulent conduct allowed the contractor 'to retain the difference between the false quote and the amount paid to the subcontractor.' The assessment report stated that Defence's remaining consideration in the matter was to determine whether any Defence officials were complicit, with no such evidence identified.

Outcome: The contractor repaid $1,377,897 to Defence in October 2022.

3.104 Key deficiencies in case study 1 included the following.

- IPIDB investigators did not conduct an assessment of the contractor to determine the potential for broader offending, despite being requested by the Acting Director Investigations. Documentation on Defence's system from March 2019, relating to a

separate matter, documented concerns with the same contractor, including that claims for payment were 'very high in comparison to the works undertaken' and that the contractor's claims may be 'deliberately excessive'.

- Key records, decisions and information were not recorded on DPSMS including: discussions and correspondence with the contractor, the construction authority and the law enforcement agency; the details of identified suspects; and Defence's consideration of evidence provided by the law enforcement agency and of additional allegations of fraud raised against the contractor.
- Monthly case status reports were not provided to relevant stakeholders as required under the Fraud Control Instructions.
- Noting the size of the potential contractor fraud, there would have been merit in Defence engaging with the CDPP to ensure a referral was not warranted. For the two largest recorded fraud losses in case management data between 1 January 2020 and 9 December 2024, Defence did not consider the matters warranted referral to the CDPP.

Joint Military Police Unit

3.105 Case study 2 outlines a fraud-related matter investigated by JMPU.

Case study 2: Joint Military Police Unit

- July 2021: JMPU received an allegation of rental allowance fraud with an estimated value of $68,808. The matter was originally investigated by Defence Housing Australia (DHA) following the member self-reporting details to DHA in July 2021. There is no record on Defence systems that DHA reported the matter to Defence.

  The matter was reported to the JMPU by the relevant unit once they had become aware of the DHA investigation. JMPU investigators recommended the matter be transferred to IPIDB due to the value of the fraud. JMPU's Assessment Board considered the matter and requested further enquiries be undertaken before referring the matter to IPIDB. The Assessment Board's decision was recorded on a Military Police Assessment Form. JMPU investigators subsequently determined that 'if the assessment board is insisting on more thorough enquiries than this before transfer, then the effort expended would make the referral redundant, we may as well have investigated' and that JMPU would conduct the investigation themselves 'more as a local decision than by HQ'.
- August 2021: An Assessment Report was completed, which stated that Assessment Board 'determined that [the Sydney JMPU station] will investigate this matter pursuant to the *Defence Force Discipline Act 1982*.'
- July 2022: The matter was referred to the ODMP for consideration of prosecution.
- August 2022: JMPU raised the matter with IPIDB for consideration at the request of ODMP 'noting the monetary value / debt incurred by the member.' IPIDB advised the ODMP that it would not take carriage of the matter due to a lack of evidence to support civilian prosecution, and the availability of more suitable alternatives, such as prosecution under the DFDA.

- August 2022: ODMP advised Defence that 'As the evidence provided to me by JMPU has previously been considered by [IPIDB], I have decided … not to proceed with … any fraud-related charges.'

Outcome: The matter was referred back to the unit and was not referred to AGSVA. As discussed at paragraph 2.65, Defence advised the ANAO that the decision to notify AGSVA following a JMPU investigation rests with the relevant unit. DPSMS records that the member repaid $47,854 of the $68,808 debt.

3.106 Key deficiencies in case study 2 included the following.

- The decision of the Assessment Board as recorded in the Assessment Form (that further enquiries be undertaken before referring the matter to IPIDB) does not accord with the Assessment Board decision recorded in the subsequent Assessment Report (that the matter would be referred for investigation by JMPU).
- IPIDB raised concerns with JMPU that the case had not been referred to them at an earlier stage and noted that 'JMPU management did not 'refer' the above matter to [IPIDB] because there was a view that they should only 'refer' serious matters ... JMPU also decided to conduct some investigation before it 'referred' the matter to this office. This practice exposes both criminal investigation by this office and DFDA investigations to risk of compromise.'
- The investigation plan did not outline a 'planned completion date for investigation' as required by the template.
- Of the eight monthly interim reports identified, two were not recorded on DPSMS.
- The Brief of Evidence provided to ODMP outlined a fraud value of $68,808. The 'total owed' and 'total recovered' fields in DPSMS recorded a value of $47,854. Defence advised the ANAO in March 2026 that 'the value in the Brief of Evidence reflects the total debt identified during the investigation, not the remaining balance at the time recovery action commenced, which is the figure reflected in DPSMS.' The DPSMS record for this matter does not indicate whether the full $68,808 debt was recovered.
- Correspondence from ODMP outlining the decision not to prosecute did not outline: why IPIDB's consideration of the matter was relevant in informing its decision; whether the evidence provided was sufficient for prosecution; and whether prosecution was in the service interest.[82]
  - A July 2021 military police intelligence assessment noted that JMPU and ODMP 'are not liaising with one another with respect to evidentiary requirements and outcomes of fraud investigations where there may be opportunities for improvement'.
  - The intelligence assessment noted that this is resulting in JMPU 'consistently providing' briefs of evidence to ODMP which may not meet appropriate standards and which ODMP may decide not to prosecute, and that ODMP responses are 'often generic' and do not support improvements to investigative processes.

82 The ODMP Prosecution Policy outlines the decision whether to prosecute as being a two-stage process based on whether the evidence offers a reasonable prospect of conviction, and whether there is a 'service interest' in proceeding with a prosecution.

Human Resources Services Branch

3.107 Case Study 3 provides an example of a matter investigated by the Human Resources Services Branch.

Case study 3: Human Resources Services Branch

- November 2022: The Human Resources Services Branch received a referral of alleged timesheet fraud.
- December 2022: The subject of the complaint was advised that a complaint had been received and that 'at this stage it is not a formal action under the misconduct process. If the information gathered indicates a formal investigation is required [the Branch] will notify you and/or your chain of command as soon as it has been determined by the decision maker.'
- December 2022–April 2023: The Branch conducted investigation activities, including the collection and analysis of evidence.
- May 2023: The Branch provided the employee with a Notification of Suspected Misconduct which advised that, as a result of the Branch's 'preliminary review', the employee may have breached the APS Code of Conduct and a formal inquiry had been initiated.
- July 2023: A Determination of Breach was issued to the respondent which outlined that they had been found to have breached the Code of Conduct, resulting in a debt of $14,800. The Branch did not seek advice from IPIDB in relation to the conduct of this case.

Outcome: A notice of Intent to Sanction was issued in September 2023 outlining a sanction of reduction in salary. The Branch advised AGSVA of the investigation outcome in November 2023. Defence advised the ANAO in March 2026 that the debt was fully recovered in August 2024.

3.108 Key deficiencies for case study 3 included the following.

- The Branch conducted key investigation activities after advising the person of interest that they were not subject to 'formal action under the misconduct process'. No further evidence gathering activities, beyond receiving evidence provided by the respondent in response to the Branch's findings, was recorded on DPSMS after the respondent had been advised that a formal inquiry had been initiated.
  - The Handling Misconduct guide provides that preliminary inquiries do not establish whether the alleged conduct occurred and that agencies should 'seek to avoid duplicating a misconduct investigation prior to deciding whether to notify the employee of an alleged breach of the Code.'
  - It further states that 'Preparing for a misconduct investigation includes … notifying an employee or former employee that they are the subject of a misconduct investigation' as it 'allows the person under investigation to raise any concerns about apprehension of bias'.
  - Defence advised the ANAO in March 2026 that key templates for advising respondents have been updated to make clearer that 'an initial information gathering activity will occur' and to remove advice that this is 'not a formal action' under the misconduct process.

- An investigation plan was not completed for this investigation. Defence advised the ANAO in July 2025 that formal plans are not required for Human Resources Services Branch investigations because the majority of evidence is provided with the referral and remaining elements of the enquiry do not require a plan. Defence further advised the ANAO in March 2026 that 'discussions occur at the commencement of the process between the Investigator and the Delegate to address the investigation planning requirements.'
  - AGIS applies to administrative, civil, and criminal investigations and identifies planning requirements beyond identifying initial avenues of inquiry, including considering: what disclosure obligations may exist; media management strategies; and the need for mutual assistance.
  - The APSC's Handling Misconduct guide states that '[i]t is good practice to develop an investigation plan at the beginning of the process to articulate what needs to be done to establish the facts.'
- Investigation evidence, correspondence establishing a debt repayment agreement with the debtor, and correspondence between investigators and the decision-maker were not recorded on DPSMS. The calculation of the debt amount was based on the employee's hourly rate at the time and did not account for additional benefits that may have accrued through fraudulently claiming additional hours, such as superannuation and leave. Defence advised the ANAO in March 2026 that 'processes have since been amended to only calculate the hourly amount' which is then forwarded to Defence's 'Pay centre' to calculate a full salary amount inclusive of factors such as superannuation and leave.

Security Threat and Assurance Branch

3.109 Case Study 4 provides an example of a security matter investigated by the Security Threat and Assurance Branch.

Case study 4: STA Branch

- September 2020: The STA Branch received a referral alleging that Defence documents classified up to Secret had been inappropriately stored.
- October 2020: The matter was accepted for investigation. The Security Incident Coordination Centre (SICC), within STA Branch, completed a security incident referral form which noted that the Business Impact Level of the incident was 'Extreme'. An investigation prioritisation matrix was also completed which assessed the investigation priority as 'very high'.
- December 2020: An investigation report was completed which found that a Defence official had breached the DSPF through failing to protect classified information from compromise or unauthorised access.

Outcome: The matter was reported to AGSVA.

3.110 Key deficiencies in case study 4 included the following:

- There is no evidence in the DPSMS record that weekly reporting on investigation progress was provided to the Assistant Secretary STA as required by STA guidelines for investigations assigned a 'Very High' priority rating.

- The investigation report noted that the Defence Security Committee did not need to be advised of the investigation outcome as the matter 'failed to meet the very high rating'. The investigation report and prioritisation matrix assessed the matter as 'very high'.

Inspector-General of the Australian Defence Force

3.111 The IGADF's functions include considering complaints relating to ADF military police. When a military police code of conduct matter is referred to IGADF, an assessment is to be conducted to determine whether the matter warrants an inquiry or DFDA investigation. One professional standards DFDA investigation was selected for case study 5.

Case study 5: IGADF investigation

- August 2023: JMPU referred an allegation to IGADF relating to an ADF member receiving an allowance they were not entitled to. Prior to accepting the referral, IGADF requested that the relevant unit conduct a fact-finding. The unit subsequently advised that, based on previous enquiries, they 'believe a service offence has been committed' and they would have to speak to the member for any further explanation. IGADF subsequently accepted the referral for investigation.
- November 2023: A Brief of Evidence was provided to the ODMP, proposing charges under the DFDA. ODMP decided not to proceed with charges.
- December 2023: IGADF referred the matter back to JMPU for further action. IGADF did not consult with IPIDB on this matter.

Outcome: IGADF advised the ANAO in March 2026 that it did not track outcomes for closed matters in 2023 and does not hold any records of action taken in response to the investigation outcome, including whether the loss of $17,546 was recovered. Defence advised that 'Debt recovery and waiver determinations are administrative functions rather than investigative responsibilities, and as such, JMPU does not track or retain records of the final outcome'. DPSMS records that $1,099 of the total loss was recovered.

3.112 Key deficiencies for case study 5 included the following.

- There is no evidence of an initial assessment of the referral being conducted by IGADF, or delegate approval to commence an investigation as required under the DII Handbook and Military Police Manual.
  - The DII handbook states that 'The assessment takes the form of a military police decision brief submitted to the appropriate decision maker. An assessment is conducted to: a. confirm the matter falls within jurisdiction, b. identify the key issues, and c. make a recommendation to the delegate on whether the matter should proceed to a [Professional Standards] investigation or inquiry, and if not, what other action — if any — should be undertaken'.
- There is no evidence of an investigation plan being completed.
- There is no evidence that monthly reporting was provided to the referring unit during the investigation as required under the Military Police Manual. IGADF advised the ANAO in July 2025 that the Military Police Manual is 'strictly not a binding requirement.'

3.113 ANAO review of DFDA investigation cases identified investigations related to matters including: failure to comply with a general order, absence without leave, unacceptable behaviour and fraud. IGADF inquiries covered similar matters. Inquiry and investigation documentation reviewed by ANAO did not outline a rationale as to why IGADF considered an inquiry or a DFDA investigation as the more appropriate response to matters.

3.114 Case Study 6 outlines an IGADF inquiry. The inquiry was selected as it had the longest recorded duration for a closed IGADF inquiry between 1 January 2020 and 30 June 2025. For this inquiry, the time between issuing inquiry directions and the inquiry report being finalised was 956 days. As discussed at paragraph 3.21, for closed non-professional standards IGADF inquiries between 1 January 2020 and 11 December 2025, the average length of time between inquiry directions being issued and inquiry reports being signed was 386 days (median 334 days).

Case study 6: IGADF inquiry

- 2021: IGADF received a submission alleging that historic sexual misconduct incidents had not been managed in accordance with notifiable incident requirements and that sensitive sexual misconduct information had been inappropriately disclosed within Defence.
- One month after the submission was received, IGADF commenced an assessment of the matter. IGADF advised the complainant that the assessment was 'anticipated to take four weeks to complete'.
- Nine months after the assessment was commenced, an assessment report was finalised which recommended an IGADF inquiry into the matter.
- Seven months after the assessment report was finalised, the IGADF issued directions for Assistant IGADFs to inquire into the matter. The directions stipulated that an inquiry plan was to be submitted to the Directorate of Inquiries and Investigations (DII) for approval within 14 days and that a fortnightly update on inquiry progress was to be provided to the DII. An inquiry plan was developed which identified evidence sources, key issues, anticipated inquiry timeframes and resources, and relevant policy documents.
- Twenty months after issuing the inquiry directions, the Inspector-General reviewed the draft inquiry report and requested further work as the report's content did not fully address the inquiry directions.
- Five months after the Inspector-General's review of the draft report, an amended version of the report was signed by the Inspector-General, which substantiated the complainant's allegations of privacy breaches and noted that some incidents of sexual misconduct were not immediately reported to a DIA or recorded on case management systems as required under the Defence Instruction. The report recommended that Defence consider administrative action against relevant personnel and notify the Office of the Australian Information Commissioner in relation to the privacy breaches.

Outcome: The inquiry report and recommendations were provided to Defence for consideration.

3.115 Key deficiencies for case study 6 included the following.

- The email appointing an assessment officer for the case was sent to the officer's non-Defence email address. The email included examples of previously completed IGADF

assessments classified Official Sensitive: Personal Privacy. A subsequent email acknowledged the error and stated 'please only work on this from your [Defence] account. We are currently looking into cases where people have transferred classified documents to their private email accounts in breach of policy so you will want to avoid that where possible.'

- The Directorate of Inquiries and Investigations (DII) noted the draft assessment report was 'hard to follow' and required amendments. Following DII review of the assessment report, DII 'reinterviewed' the complainant and amended the report. As part of the subsequent inquiry process, a further interview with the complainant was requested, who declined on the basis that they had previously provided information through interviews during the assessment phase and that the inquiry process was 'taxing'.
- There is no evidence that the inquiry plan was submitted to the Directorate of Inquiries and Investigations for approval, or that fortnightly updates were provided to the Directorate as required under the inquiry directions. Monthly updates were not always provided to the complainant as required by the DII Handbook, and the complainant sought updates from IGADF on at least two occasions, following delays in the provision of updates.
- A legal review of the inquiry report was conducted as required by the DII Handbook. The review determined that the report was 'well written' and addressed the Terms of Reference. A separate legal review conducted two months later raised concerns that: prior legal review of the draft report was 'wholly inadequate'; the inquiry committed 'repeated breaches of privacy'; inquiry evidence was missing, difficult to locate, had not been sufficiently considered or appeared to have been 'cherry-picked'; interviews did not follow correct processes; and one Assistant IGADF knew one of the witnesses and that the interview of that witness was conducted in an 'overly friendly' manner.
- The Assistant IGADFs responded to the legal review noting that they were new to the role and in a 'learning phase'. The ANAO identified a separate case where an internal review of an assessment report drafted by an Assistant IGADF found that the Assistant IGADF 'either did not read or dismissed evidence' and that the assessment report was written 'in favour of command'.
- A third legal review was conducted three months after the second legal review. The review disagreed with previous concerns raised regarding privacy breaches but noted that:
  - Assistant IGADFs should be 'highly circumspect' in dealing with personal information and that 'this could be impressed upon' Assistant IGADFs;
  - interview templates should be amended; and
  - inquiry teams should 'not consist of first timers alone'.
- IGADF advised the ANAO in November 2025 that relevant templates had been amended in response to the observations.
- Including the pre-inquiry assessment phase, the case took three years and five months to complete.[83] The IGADF advised the ANAO in May 2026 that there were factors outside the

83 ANAO identified a separate submission to IGADF made in December 2021, for which the relevant inquiry report was signed in January 2026.

control of the IGADF which contributed to the lengthy inquiry timeframe including: inquiry participants being medically unfit for interview; delays identifying suitably qualified Assistant IGADFs; delays in the provision of information from relevant Defence areas; and the impacts of COVID shutdowns in 2020 and 2021. As outlined at paragraph 3.28, the Royal Commission into Defence and Veteran Suicide report stated that lengthy inquiry timeframes are 'unsatisfactory' as they can have adverse impacts on the wellbeing of those involved.

3.116 Record keeping deficiencies were observed across the selected six case studies, as well as other cases referenced throughout this report. Good record keeping is a legislative requirement of the PGPA Act, and the *Archives Act 1983,* and is particularly important for activities that may result in adverse outcomes against individuals, such as investigations and inquiries. Failure to record key decisions, the basis for those decisions, and the extent to which relevant evidence is considered in the decision-making process presents risks to the integrity of Defence investigations and the ability of Defence to provide transparency in its decision-making.

Recommendation no. 9

3.117 The Department of Defence, including the Office of the Inspector-General of the Australian Defence Force, ensure:

(a) key investigation and inquiry decisions and documents are recorded for all investigations and inquiries; and

(b) regular updates are provided on investigation and inquiry progress to relevant stakeholders as required under Defence policies and guidance.

Department of Defence response: *Agreed.*

Dr Caralee McLiesh PSM
Auditor-General

Canberra ACT
22 May 2026

Appendices

Appendix 1 Entity responses

Department of Defence

Australian Government
Defence
PO Box 7900 CANBERRA BC ACT 2610

EC26-002626

Dr Caralee McLiesh, PSM
Auditor-General of Australia
Australian National Audit Office
PO BOX 707
CANBERRA ACT 2601

Dear Dr McLiesh

AUDITOR-GENERAL PROPOSED REPORT – ADMINISTRATION OF INVESTIGATIONS IN DEFENCE

Thank you for the opportunity to comment on the proposed report for the Auditor-General performance audit *Administration of investigations in Defence.*

Defence acknowledges the proposed report's assessment that the arrangements in place for the administration of investigations has been partly effective. Defence also notes the proposed report includes a number of recommendations and an opportunity for improvement relating to Defence's investigations framework and systems, investigator qualifications, monitoring and reporting, fraud debt recovery, quality assurance and investigation practices.

Attached to this letter are the Inspector-General of the Australian Defence Force's letter to the Auditor-General **(Enclosure 1)**, Defence's proposed amendments, editorial comments **(Attachment A)**, Defence's response to the proposed recommendations **(Attachment B)**, and Defence's summary response **(Attachment C)**. Together, these documents constitute the formal response of Defence and the Inspector-General of the Australian Defence Forces to the Auditor-General's proposed report.

Defence is committed to working collaboratively with the ANAO to address these matters and is available to discuss further if required.

Our point of contact is the ANAO Liaison Officer who can be contacted via email at anao.lo@defence.gov.au.

Yours sincerely

Cath Patterson
Acting Secretary

14 May 2026

David Johnston AC
Admiral RAN
Chief of the Defence Force

14 May 2026

Inspector-General of the Australian Defence Force

Enclosure 1

Australian Government
Inspector-General of the Australian Defence Force

IGADF/BN124453540

Dr Caralee McLiesh, PSM
Auditor-General of Australia
Australian National Audit Office
PO BOX 707
CANBERRA ACT 2601

Dear Dr McLiesh

Auditor-General Proposed Report – Administration of investigations in Defence

Thank you for the opportunity to comment on the Australian National Audit Office's (ANAO) proposed performance audit report *Administration of investigations in Defence* which also included examining certain functions of the Office of the Inspector-General of the Australian Defence Force (IGADF).

The Office of the IGADF acknowledges the proposed report's findings and recommendations that seek to guide further improvements in the conduct of investigations.

Through the implementation of the recommendations made by the Royal Commission into Defence and Veteran Suicide, as well as broader initiatives, the Office of the IGADF has designed several measures that have strengthened our procedures, provided greater clarity and understanding for those engaging in our processes, enhanced staff training and skill maintenance, and driven improved trauma-informed and trauma-responsive practices.

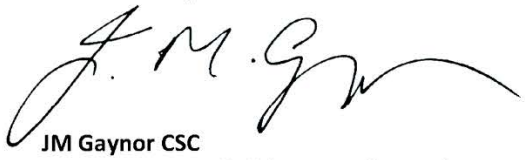
It is also noted that while the audit scope was focused on the administration of investigations, the audit extended to also consider inquiries. Investigations and inquiries operate under distinct frameworks, serve different purposes and require different skill sets. In this context, reflecting these distinctions would assist in supporting a clear and balanced presentation in the final report.

Recognising the Office of the IGADF as a statutory officer within Defence, appointed under the *Defence Act 1903*, and consistent with your request, the Office's proposed amendments, editorials and comments, as well as the response to the proposed recommendations, have been incorporated unedited in Defence's consolidated response.

The Office of the IGADF is committed to working collaboratively with the ANAO to address these matters and is available to discuss further if required.

Should your office require further information on the response, please contact the acting Assistant Secretary – Enabling Functions, Cameron Gill, on 02 5108 6055 or cameron.gill@igadf.gov.au.

Yours sincerely



JM Gaynor CSC
Inspector-General of the Australian Defence Force

Telephone: 1800 688 042
Email: ig.adf@defence.gov.au

PO Box 7924
CANBERRA BC ACT 2610

7 May 2026

Appendix 2 Improvements observed by the ANAO

1. The existence of independent external audit, and the accompanying potential for scrutiny improves performance. Improvements in administrative and management practices usually occur: in anticipation of the Australian National Audit Office (ANAO) audit activity; during an audit engagement; as interim findings are made; and/or after the audit has been completed and formal findings are communicated.

2. The Joint Committee of Public Accounts and Audit (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's corporate plan states that the ANAO's annual performance statements will provide a narrative that will consider, amongst other matters, analysis of key improvements made by entities during a performance audit process based on information included in tabled performance audit reports.

3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:

- strengthening governance arrangements;
- introducing or revising policies, strategies, guidelines or administrative processes; and
- initiating reviews or investigations.

4. In this context, the below actions were observed by the ANAO during the course of the audit. It is not clear whether these actions and/or the timing of these actions were planned in response to proposed or actual audit activity. The ANAO has not sought to obtain assurance over the source of these actions or whether they have been appropriately implemented.

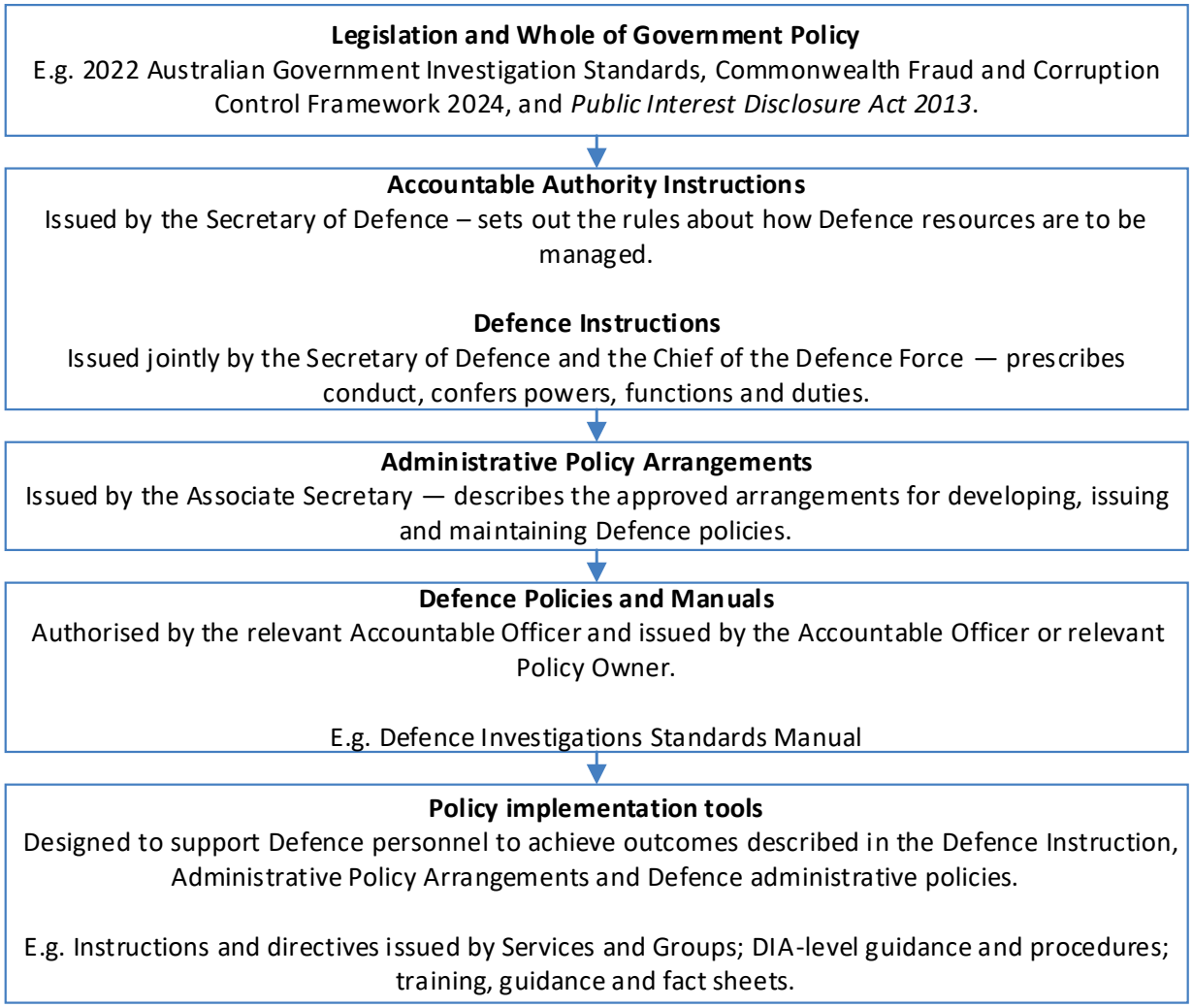
Table A.1: Improvements observed by the ANAO

Paragraph references	Improvements observed
Paragraphs 1.26–1.27	Defence has made progress in implementing recommendations from the Royal Commission into Defence and Veteran Suicide.
Paragraph 2.11	Defence advised the ANAO in March 2026 that it is reviewing its Code of Conduct policy guidance to 'better reflect' initial notification requirements to JMPU, and that this is anticipated to be completed by the end of June 2026.
Paragraph 2.17	Prior to being updated in January 2026, the Defence Instruction did not define Defence's authorised case management system.
Paragraph 2.40	Defence advised the ANAO that updated governance documents have been issued by IPIDB between 2024 and 2026 to 'target specific investigative functions and requirements'.
Paragraph 2.66	Defence advised that it will implement 'formal, traceable, and auditable documentation for all future reviews' of the Military Police Manual.
Paragraph 2.70	Defence advised the ANAO in March 2026 that work has 'commenced on developing procedures relating to consultation with or referral of matters to other DIAs or entities' for the Human Resources Services Branch.

Paragraph references	Improvements observed
Paragraph 2.69	Defence advised the ANAO that the Human Resources Services Branch had no formalised register for declaring or recording conflicts of interest or managing independence during investigations and that the Branch has 'since implemented a register to document such decisions of this nature in future.'
Paragraph 2.90	The Provost Marshal of the Australian Defence Force (PMADF) issued PMADF Directive 15-2024 in November 2024, establishing qualification requirements for JMPU investigators.
Paragraph 3.5	Defence advised the ANAO in May 2026 that DECMS improvements had been implemented or were underway. This included implementation of a trend dashboard in September 2025 and the enabling of reporting based on keyword searches for the Security Threat and Assurance (STA) Branch in January 2026 and for the JMPU in July 2026.
Paragraph 3.20	IGADF advised the ANAO in May 2026 that 'Internal processes have been amended and staff in the Professional Standards Cell have been directed to ensure all relevant fields within the database are completed correctly and in a timely manner'.
Paragraph 3.67	A quality assurance review was conducted into the STA Branch by the Department of Home Affairs in June 2025.
Paragraph 3.71	Defence advised the ANAO in March 2026 that a review of MPC decisions was undertaken in March 2025 'to identify systemic issues and remediation action which has since been put in place to improve capability'.
Paragraph 3.75	In July 2025, the PM-ADF directed that a TSI audit be conducted into JMPU Headquarters Select Investigation Team and that they be added to the yearly TSI schedule.
Paragraph 3.81	IGADF advised the ANAO in March 2026 that it 'will seek to establish a mechanism for independent external reviews to provide further assurance on DII practices (and where appropriate other Office of the IGADF activities)'.
Paragraph 3.108	Defence advised the ANAO in March 2026 that key Human Resources Services Branch templates for advising respondents have been updated to make clearer that 'an initial information gathering activity will occur' and to remove advice that this is 'not a formal action' under the misconduct process.

Source: ANAO analysis of Defence documentation.

Appendix 3 Hierarchy of Defence documents



Source: ANAO analysis of Defence's Administrative Policy Arrangements.

Appendix 4 Royal Commission recommendations

1. The table below outlines recommendations relevant to Defence investigations, inquiries and fact-finding from the Royal Commission into Defence and Veteran Suicide. This list is not intended to be exhaustive.

Table A.2: Royal Commission recommendations

Royal Commission recommendation	ANAO comment
Recommendations 15, 18 and 21: Defence clarify definitions and processes for sexual offences, 'develop a dedicated policy' requiring commanders to immediately take actions to support the safety and wellbeing of victims when sexual misconduct investigations are underway, and the CDF issue a directive providing for a 'presumption of discharge' for ADF members found to have engaged in certain forms of sexual misconduct.	As at February 2026, implementation of these recommendations was ongoing.
Recommendation 25: An independent inquiry into sexual violence in the ADF including 'the effectiveness of the military justice system … in receiving, investigating and adjudicating on sexual and related offences' and 'an examination of the Joint Military Police Unit's investigative powers and capability to conduct sexual offence investigations'.	An inquiry into sexual violence in the ADF was announced by the Minister for Veterans' Affairs and Defence Personnel on 2 December 2025. Defence advised the ANAO in May 2026 that 'this is not a Defence-led recommendation with support from Defence provided via participation in inquiries led by the DVSC [Defence and Veterans' Service Commission].'
Recommendation 28: Improve coordination of the governance, assurance and policy functions of the military justice system.	Defence advised the ANAO in February 2026 that a Military Justice System Assurance Branch has been established within Defence, but implementation of the recommendation is ongoing.
Recommendation 29: Improve training for the conduct of fact-finding activities and inquiries.	Defence advised the ANAO in February 2026 that work 'to review the training and effectiveness of policies remains ongoing'.
Recommendation 30: An IGADF inquiry into the 'weaponisation' of the military justice system be prioritised and commenced before the end of 2024.	The inquiry commenced in August 2024 and was ongoing as at March 2026.
Recommendations 44, 45 and 46: Ensure that IGADF staff have necessary skills and qualifications to discharge IGADF functions, and update and publish IGADF quality assurance and timeliness measures for assessments and inquiries.	IGADF advised the ANAO in November 2025 that the implementation of recommendations that relate to the IGADF are being considered by the Australian Government alongside the recommendations of the Twenty-Year Review. IGADF further advised the ANAO in May 2026 that: Assistant IGADF qualifications are centrally recorded in a register; all personnel commencing with the IGADF are required to record recognised skills and qualifications as part of the on-boarding process; reporting of quality assurance and timeliness is conducted through weekly and monthly meetings with senior leadership; and the IGADF Annual Report articulates the reporting of quality assurance and timeliness achievements over the past 12 months.

Source: ANAO analysis. Also see Royal Commission into Defence and Veteran Suicide, *Final Report,* September 2024, available from https://defenceveteransuicide.royalcommission.gov.au/publications/final-report-all-volumes [accessed 11 February 2026].