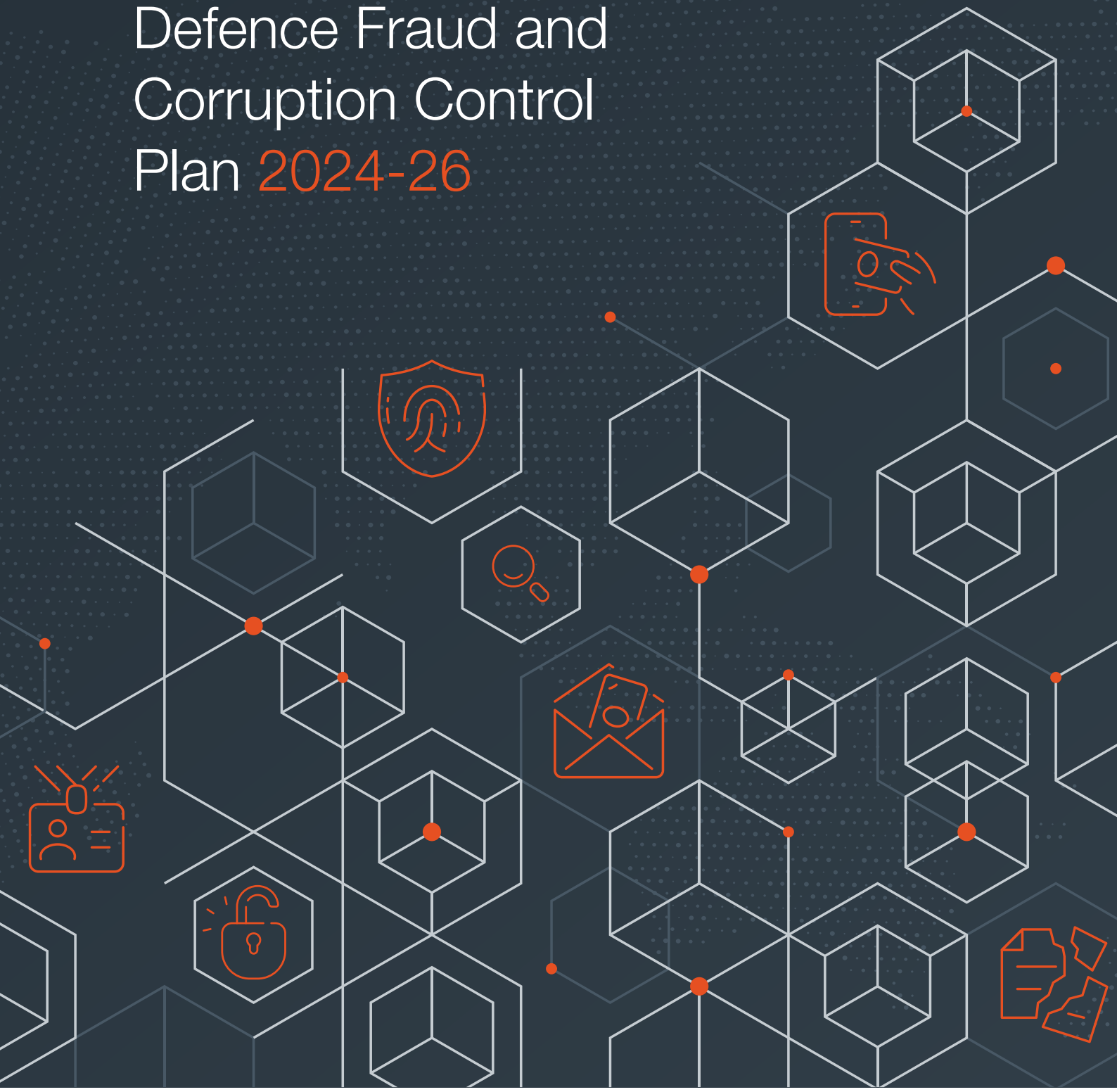
Australian Government
Defence

Defence Fraud and Corruption Control Plan 2024-26



To defend Australia and its national interests in order to advance Australia's security and prosperity

www.defence.gov.au

ACKNOWLEDGEMENT OF COUNTRY

Defence acknowledges the Traditional Custodians of the lands, seas and air in which we live, work and train. We pay our respects to their Elders past and present. We also pay our respects to the Aboriginal and Torres Strait Islander men and women who have contributed to the defence of Australia in times of peace and war.

Defence Integrity Division, Associate Secretary Group
Department of Defence

PO Box 7910, Canberra BC ACT 2610
Email: fraud.risk@defence.gov.au
Web: www.defence.gov.au

CG: MAY027-24

Foreword

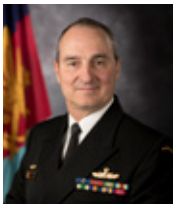
Defence operates in a complex and fast-paced domestic and international environment. As part of the 2024 Integrated Investment Program, the Government has injected an additional $5.7 billion over the next four years and $50.3 billion over the next decade in Defence funding. This will see the Defence budget grow to more than $100 billion by 2033-34 to deliver the 2024 National Defence Strategy.

The scale and complexity of our operating environment exposes us to significant fraud and corruption risks. We are committed to embedding integrity and accountability throughout Defence and do not tolerate fraudulent or corrupt behaviour.

All Defence personnel including contractors share in the responsibility to identify and report suspected fraud or corruption, behave ethically, and promote a culture of integrity, honesty and accountability in the workplace. These core behaviours must underpin all of our actions and decisions to ensure we manage our resources efficiently and effectively, and fulfil our responsibilities to protect public money and property.

The Defence Fraud and Corruption Control Plan outlines our commitment to preventing, detecting and responding to fraud and corruption. It provides guidance to Defence personnel, and those who undertake business with Defence, on their responsibility to safeguard Defence against fraud and corruption.

We encourage all Defence personnel and those who conduct business with Defence to familiarise themselves with this Plan, report incidents of suspected fraud and corruption, and work with us to maintain trust and confidence in Defence.



Greg Moriarty
Secretary
September 2024

Admiral David Johnston
Chief of the Defence Force
September 2024


07057
42

Contents

Introduction

The Defence Fraud and Corruption Control Plan 2024-26 (the Plan) documents Defence's commitment and approach to prevent, detect and respond to fraud and corruption.

The Plan aligns to the Defence Risk Management Framework and the mandatory requirements of the Commonwealth Fraud and Corruption Control Framework 2024, established under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The Defence Operating Context

Defence is a complex and diverse Commonwealth agency operating domestically and internationally, and faces its most challenging strategic environment since the Second World War. In response, the 2024 National Defence Strategy and the 2024 Integrated Investment Program have fundamentally shifted Defence's approach to the defence of Australia. These two documents guide significant and urgent changes required to transform Defence's capability, force posture, force structure, acquisition, recruitment and international engagement.

To meet our new strategic objectives, the Government is funding $330 billion through to 2033-34 on capability investment priorities which present new and challenging risks that must be assessed and adequately addressed. This includes the risk of fraudulent and corrupt behaviour.

To be effective in preventing, detecting and responding to fraud and corruption, Defence requires a control Plan that is agile and responsive to this complex environment.

People

Defence people are dispersed throughout Australia and the world.

57,226
Australian Defence Force members

19,465
Australian Public Service personnel

32,000+
Australian Defence Force reservists

Assets

Defence has $145.9 billion of total assets including:

$89.5b
of specialist military equipment

$36.0b
of buildings and infrastructure, including training areas, ranges and major bases

Projects

As at 30 June 2024, Defence managed projects included:

568
major acquisition projects

99
minor acquisition projects

with total acquisition costs of
$245b

Source: Defence Annual Report 2023-24.

What is Fraud and Corruption?

Defence uses fraud and corruption definitions prescribed by the Commonwealth Fraud and Corruption Control Framework.

Fraud

Fraud is defined as "*dishonestly obtaining (including attempting to obtain) a gain or benefit, or causing a loss or risk of loss, by deception or other means*."

Fraud requires intent. It requires more than carelessness, accident or error. When intent cannot be shown, an incident may be noncompliance rather than fraud. A benefit is not restricted to a material benefit, and may be tangible or intangible, including information. A benefit may also be obtained by a third party.

Examples of fraud include::

- theft or misuse of Defence assets, equipment or facilities
- accounting fraud (for example false invoices, misappropriation of funds, vendor management)
- misuse of Defence expense or travel cards
- dishonestly obtaining allowances and benefits
- theft or misuse of Defence information or intellectual property
- providing false or misleading information to Defence, or failing to provide information when there is an obligation to do so.

Corruption

Corruption is defined as "*any conduct that does or could compromise the integrity, accountability or probity of public administration*."

This includes any conduct of any person (whether or not a staff member of a Commonwealth agency) that adversely affects, or that could adversely affect, either directly or indirectly:

- the honest or impartial exercise of any staff member's powers as a staff member of a Commonwealth agency
- the honest or impartial performance of any public official's functions or duties as a public official
- any conduct of a staff member of a Commonwealth agency that constitutes or involves a breach of public trust
- any conduct of a staff member of a Commonwealth agency that constitutes, involves or is engaged in for the purpose of abuse of the person's office
- any conduct of a staff member of a Commonwealth agency, or former staff member of a Commonwealth agency, that constitutes or involves the misuse of information or documents acquired in the person's capacity as a staff member of a Commonwealth agency.

Put simply, 'corruption' is the misuse of entrusted power or authority for personal gain. The following list provides examples of types of behaviours that may amount to corruption in Defence:

- collusion between Defence personnel and a contractor, consultant or outsourced service provider
- bribery
- obtaining, offering or soliciting secret commissions, kickbacks or gratuities
- one or more individuals manipulating a procurement process for personal gain
- nepotism - preferential treatment of family members
- cronyism - preferential treatment of friends and associates
- acting or failing to act on a conflict of interest
- unlawful disclosure of official or commercially sensitive information
- insider trading - misusing official information to gain an unfair private, commercial or market advantage for self or others.

Leadership and Culture

Leadership and culture are the cornerstones of effective fraud and corruption prevention. Defence is committed to fostering a culture where fraud and corruption is not tolerated, transparency and accountability is expected, and the workplace supports and empowers individuals to speak up when suspected fraud or corruption occurs.

Defence Values and Behaviours are at the core of the Defence Culture Blueprint. Defence Values and Behaviours guide Defence personnel on what is and is not acceptable in our workplaces. The Defence Culture Blueprint Program and Defence Culture Strategy will embed an organisational culture where leadership, professionalism, integrity and positive corporate behaviour are valued and rewarded.

Integrity

Defence personnel must act transparently when making work-related decisions, reflecting the probity and ethical standards of the Commonwealth and Defence, including adherence to Defence Values and Behaviours.

Defence requires contractors, consultants and outsourced service providers to demonstrate the same ethical standards by complying with the principles set out in this Plan and *Defence and the Private Sector: Working with Integrity.*

Fraud and Corruption Tolerance

Defence does not tolerate fraudulent or corrupt behaviour. Defence acknowledges that it cannot avoid or prevent all fraud and corruption risks, which is why Defence is committed to implementing a contemporary control framework to prevent, detect and respond to fraudulent and corrupt behaviour.

In practice this means that Defence:

- expects all Defence personnel including contractors, consultants and outsourced service providers engaged through contract with Defence to behave with integrity at all times
- expects all Defence personnel including contractors, consultants and outsourced service providers engaged through contract with Defence to report all suspected fraud and corruption immediately, in accordance with the details outlined in this Plan and other related Defence instructions, polices and guidance
- will assess all allegations of fraud or corruption and respond as appropriate
- where appropriate, will take action to have any fraudulent or corrupt behaviour dealt with through criminal, civil, disciplinary or administrative processes
- where appropriate, will apply administrative or contractual penalties, including termination of engagement and will take all reasonable measures to recover misappropriated funds and assets.

Roles and Responsibilities

The Secretary and the Chief of the Defence Force (CDF) approve this Plan demonstrating their combined commitment to the prevention, detection and response to fraud and corruption.

Pursuant to the PGPA Act, the **Secretary** is the Accountable Authority and is responsible for governing Defence in a way that promotes the proper use of public resources.

In that context, the Secretary is the **Risk Owner** for fraud and corruption, and must take all reasonable measures to prevent, detect and respond to fraud and corruption that could arise in relation to activities undertaken for, or on behalf of, Defence, including work undertaken by contractors, consultants and outsourced service providers. The Secretary has delegated some authority to other accountable officers within Defence as listed on the following pages.

The Secretary is also the Agency Head under the *National Anti-Corruption Commission Act 2022* (NACC Act) and has obligations to refer corruption to the National Anti-Corruption Commission (NACC).

Associate Secretary (Chief Risk Officer) is the fraud and corruption **Risk Steward** and has the responsibility for overseeing the implementation of fraud and corruption control within Defence, in line with Section 10 of the PGPA Rule.

Chief Finance Officer has accountability for setting Defence's financial framework and ensuring that risks associated with Defence's appropriations and expenditure are addressed.

Chief Information Officer facilitates the protection of Defence information system security and Information and Communication Technology (ICT) access control. The Chief Information Officer is supported by the Chief Security Officer to ensure integrity and application of information security principles and practices for Defence ICT.

Chief of Joint Capabilities facilitates the protection of Defence data, information and systems through layered cyber security and access control arrangements.

First Assistant Secretary Defence Integrity (Principal Integrity Officer (PIO)) maintains enterprise accountability for the Defence Integrity Framework, and is responsible for Defence's fraud and corruption control arrangements. This responsibility includes promoting a culture of integrity through training and awareness throughout Defence, and increasing Defence's capacity to prevent, detect and respond to fraud and corruption. Additionally, they are the Value Chain Leader for the Defence business process Incident Event to Outcome in the Defence Enterprise Resource Planning (ERP) Program Case Management Solution. The Secretary has delegated their obligations as Defence's Agency Head for the purposes of the NACC Act to the Principal Integrity Officer.

First Assistant Secretary Defence Security (Chief Security Officer) has accountability for implementing the requirements of the Protective Security Policy Framework and the Defence Security Principles Framework across Defence.

Group Heads and Service Chiefs play a critical role in supporting fraud and corruption control arrangements. In addition to assigned responsibilities for specific control arrangements, they are responsible for leading the establishment and maintenance of an ethical culture within their Group or Service, together with the implementation and operation of governance arrangements.

Group Heads and Service Chiefs must:

- ensure that the risk of fraud and corruption is considered in the planning and development of programs and the conduct of activities under their control
- advise Integrity Division, as soon as reasonably practicable, of any substantial change in structure, functions or activities to enable an assessment of fraud and corruption risk
- ensure that Defence personnel in their Group or Service participate in mandatory Fraud and Integrity Awareness training
- respond to requests from the Integrity Division to conduct fraud and corruption control activities including conducting fraud and corruption risk assessments, the development and implementation of treatments and the conduct of control assurance activities
- appoint an appropriately qualified and resourced Group Fraud Control Coordinator.

Group Heads and Service Chiefs may be specifically delegated responsibility by Control Owners to ensure the implementation and/or reporting against specific controls to mitigate or manage a risk.

Group Fraud Control Coordinators are appointed by their respective Group Head or Service Chief to form a Defence wide fraud and corruption control network. They inform and support the Risk Steward and Control Owners by regularly liaising with Integrity Division and coordinating Group or Service specific fraud and corruption control activities.

Commanders and Managers at all levels have a critical role in supporting fraud and corruption control within Defence. In addition to the expectations of all Defence personnel, Commanders and Managers are expected to:

- ensure subordinate Defence personnel complete mandatory Fraud and Integrity Awareness training
- take action to appropriately manage any actual, potential or perceived conflicts of interests in relation to subordinate Defence personnel
- take appropriate action on any reports of suspected fraud, corruption or unethical behaviour, including matters which may constitute a Public Interest Disclosure
- provide resources and support to ensure that the risk assessment process accurately reflects each Group and Service, and that the controls imposed are reviewed on a regular basis to maintain and mitigate current and emerging risks.

Control Owners are responsible for managing the implementation and assessment of controls for specified fraud and corruption risks. Control Owners must ensure performance of their control(s), including the effectiveness of the controls, against their objectives and for reporting on control performance.

Joint Military Police Unit is responsible for investigating routine and minor offences of fraud committed by serving Australian Defence Force members under the *Defence Force Discipline Act 1982*. The Unit performs a key fraud and corruption response capability, working in close partnership with Integrity Division.

All Defence personnel, contractors, consultants and outsourced service providers are expected to act with integrity and comply with relevant legislation, Defence Instructions, policies, manuals and guidance in:

- promoting ethical behaviour
- assisting with the implementation of fraud and corruption control risk management strategies and cooperatively participating in activities designed to prevent, detect and respond to fraud and corruption
- completing mandatory Fraud and Integrity Awareness training[1]
- reporting any incidents of fraudulent or corrupt behaviour, or conflicts of interests that come to their attention
- not acting in a retaliatory, discriminatory or otherwise adverse manner towards any individual, on account of that individual making a genuine report of fraud or corruption
- not hindering, obstructing or impeding any investigation into suspected fraud or corruption
- providing every courtesy and reasonable assistance to any person authorised to conduct an investigation into suspected fraud or corruption.

1 Contractors, consultants and outsourced service providers must complete training as specified under the terms of their engagement with Defence.

Key Fraud and Corruption Risks to Defence

Defence undertakes an Enterprise level fraud and corruption risk assessment every two years, or when there are substantial changes in structure or functions. The risk assessment identifies and analyses existing, new and emerging fraud and corruption risks to Defence. Defence monitors these risks and, where appropriate, implements targeted control programs.

The key fraud and corruption risks to Defence are summarised below

Human Resources

- Fraudulent or corrupt behaviour during recruitment activities
- Theft, misuse and/or unauthorised access to information and assets post separation

Corporate Information

- Theft, misuse and/or unauthorised disclosure of information

Assets

- Theft, misuse and/or misappropriation of:
  - ICT assets
  - Medical equipment, supplies or pharmaceuticals
  - Stores, equipment and clothing
  - Petroleum, oils and lubricants
  - Specialist military equipment
  - Weapons and ammunition

Procurement and Contract Management

- Fraudulent or corrupt behaviour during procurement and contracting activities

Corporate Funds

- Fraudulent use of Defence allocated expense cards
- Fraudulent claim of entitlements or allowances
- Fraudulent or corrupt behaviour in the management of Defence grants
- Defence personnel use their position for financial or personal benefit
- Fraudulent or corrupt behaviour by Defence personnel or contractors involved in accounts management
- Fraudulent behaviour by external party during accounts payable transactions impacting Defence

Details of these risks and controls are documented in the 2024 Defence Fraud and Corruption Risk Register. Fraud and corruption risks not identified as key risks to the Enterprise are managed by the relevant Group and/or Service.

Defence consults with other entities where fraud and corruption risks impact on the responsibilities of the other entity in accordance with legislative obligations or powers relating to information sharing.

Preventing Fraud and Corruption

Fraud and corruption prevention strategies are the ‘first line of defence’, focusing on the establishment and maintenance of sound governance systems and an ethical organisational culture. Prevention activities provide the most cost-effective method of controlling fraud and corruption.

Key elements of Defence's fraud and corruption prevention strategy

Mandatory Fraud and Integrity Awareness training

Governance, accountability and oversight

Policies, procedures and guidance documents

A program of regular risk assessments and reviews to ensure controls remain effective

System and physical access controls

Periodic communications to raise awareness of fraud, corruption and integrity related matters

Personnel Controls

SECURITY CLEARANCE

All Defence personnel, including contractors, consultants and outsourced service providers, are required to hold a Commonwealth security clearance and to maintain this clearance for the duration of their engagement with Defence. Security clearances reduce the likelihood that the organisation will employ or engage personnel who are predisposed to fraudulent or corrupt behaviour. The Defence Security Principles Framework provides instruction to determine the level of security clearance required.

FRAUD AND INTEGRITY AWARENESS

Defence personnel must complete mandatory Fraud and Integrity Awareness training. This online training meets the Australian Public Service Commissioner's Directive for integrity training for Australian Public Service employees.

Face-to-face and virtual Fraud and Integrity Awareness training, as well as Conflict of Interest Masterclasses, are also delivered nationally. These sessions are designed to ensure that all Defence personnel understand their integrity obligations, are equipped to identify integrity risks, including fraud and corruption, and understand when and how to report suspected fraud, corruption or integrity incidents. Defence also runs periodic integrity communication campaigns that are themed and focused on key integrity risks, including fraud and corruption.

ENGAGEMENT AND SEPARATION OF PERSONNEL

All Defence personnel, contractors, consultants and outsourced service providers are subject to on-boarding and off-boarding processes which are supported by preventative controls such as education, policies and system level controls.

CONFLICTS OF INTEREST

All Defence personnel must regularly assess whether they have an actual, potential or perceived conflict of interest and take reasonable steps to avoid situations where their private interests conflict with their official duties. Where an actual, potential or perceived conflict of interest is identified, Defence personnel must submit a *Conflict of Interest Declaration Form* (AF220) via ServiceConnect.

All tender evaluation and recruitment panel members must submit a positive affirmation of no conflict, via submission of an AF220 where no actual, potential or perceived conflict of interest exists.

Members of the Senior Leadership Group and the Defence Audit and Risk Committee must provide an annual declaration of interest.

Contractors, consultants and outsourced service providers must adhere to the conflict of interest obligations as outlined in their contract.

Defence personnel, contractors, consultants and outsourced service providers can seek advice on conflict of interests via *defence.integrity@defence.gov.au*.

POST SEPARATION EMPLOYMENT CONFLICT OF INTEREST

All Defence personnel must report any offer of post-separation employment that could lead to an actual, potential or perceived conflict of interest, as soon as practicable and before accepting the offer. All post-separation employment declarations must be made by submitting a *Conflict of Interest Declaration Form* (AF220) via ServiceConnect.

Defence personnel may also need to apply for a foreign work authorisation when working for, or on behalf of, a foreign military or government body post-separation, as required under the *Defence Amendment (Safeguarding Australia's Military Secrets) Act 2024*. The requirement for a foreign work authorisation strengthens Australia's security by preventing individuals from disclosing or exploiting classified information.

To find out more information on who is required to submit a foreign work authorisation request, see the *Authorisation requirements* page.

Financial Controls

Defence maintains a set of financial controls to ensure a true and fair view of Defence's financial performance, position and proper use and management of public resources, consistent with the PGPA Act.

Procurement and Contracting Controls

Defence applies due diligence and probity controls to all stages of the procurement and contracting life cycle. Controls are tailored according to the scope, scale and risk of activities and align to the Commonwealth Procurement Rules, Defence procurement and contracting policies and the Defence Commercial Framework. This is supported by the development of system controls within the My Procurements application to reduce instances of non-compliance, and deter fraud and corruption, through the systemised capture and reporting of procurement decisions and approvals.

Defence undertakes a range of audit and assurance activities to ensure all Defence personnel, suppliers, including contractors, consultants and outsourced service providers undertake procurement and contracting activities in accordance with these policies and frameworks, and *Defence and the Private Sector: Working with Integrity*.

Information Controls

In line with the Australian Government Protective Security Policy Framework, Defence takes a systematic approach to ICT security risk management, network usage and detection capabilities.

The Defence Security Principles Framework and the security classification system contained within, allows Defence to share and exchange information with confidence by ensuring a common recognition of confidentiality requirements and the consistent application of protective security measures. A range of assurance initiatives help ensure the integrity of data and information management across Defence.

Asset Controls

Defence maintains comprehensive asset registers and inventory management systems. To govern these systems, Defence undertakes regular stocktakes in relation to both assets and inventory to ensure appropriate maintenance, accountability and early identification of loss or theft.

Detecting Fraud and Corruption

No system of preventative controls can provide absolute assurance that fraud or corruption will not occur. It is therefore critical that preventative measures are supplemented with detective controls to support early detection and enable a timely and effective response.

Measures to detect internal and external fraud and corruption within Defence include:

- system monitoring and scanning, including proactive detection analytics
- data modelling and intelligence analysis to identify potential fraudulent and corrupt behaviour
- post-transactional reviews to identify altered or missing documentation, or falsified authorisation, that may identify fraud or corruption in high risk activities
- internal and external audits
- mandatory reporting of suspected and/or actual fraud and corruption
- reporting mechanisms to receive confidential internal and external fraud and corruption tip-offs
- monitoring conflict of interest disclosures
- intelligence sharing with, and collaborating across, law enforcement, integrity agencies and international jurisdictions.

Intelligence and Data Analytics

Defence has a rolling program of data analytics projects that focus on areas of fraud and corruption risk. The program is informed by intelligence activities, which include post-case analysis of reported fraud and corruption incidents, risks outlined in this Plan, and topics arising from engagement with the Senior Leadership Group, Groups and Services and external partners.

Audit and Assurance Activities

COMPLIANCE ACTIVITIES

Defence undertakes a broad range of activities and employs system and manual controls to detect financial and legislative non-compliance. Where fraudulent transactions and/or expenditure claims are identified they are referred for investigation. Where fraud and corruption risks have been identified in a specific project or area of operations, Defence undertakes targeted compliance activities to identify deficiencies, and to reinforce best practice.

The Defence Procurement and Contracting Assurance Framework is an example of this. It provides centralised assurance monitoring and reporting on procurement practices and compliance with Commonwealth Procurement Rules, Defence Procurement and Contracting Policy, and the Defence Commercial Framework across Defence.

CONTROL TESTING

Defence undertakes a range of assurance activities to detect fraud and corruption, and test control effectiveness to ensure countermeasures are appropriate and working effectively. In addition to existing assurance activities undertaken by Groups and Services, Defence will develop and implement a targeted risk-based program of control testing.

AUDITS

Internal and external audits play an important role in the prevention and detection of potential and actual fraud and corruption risks. When developing the Defence Strategic Internal Audit Plan, Defence considers fraud and corruption risks to enable targeted testing of controls to identify improvement opportunities.

How to Report Allegations of Fraud and Corruption

Defence classifies fraudulent or corrupt behaviour, actual or suspected, as a Notifiable Incident under Defence Instruction - Administration and Governance Provision 4: Incident Reporting and Management.

All Defence personnel, contractors, consultants and outsourced service providers must report suspected fraud and corruption.

Defence Incident Reporting Hub

Defence personnel can report suspected fraud and corruption through the *Defence Incident Reporting Hub* intranet page.

Anyone, including Defence personnel families and the public, can report suspected fraud or corruption in Defence through the *Complaints and Incident Reporting* page on the Australian Government Defence website.

Public Interest Disclosures (PID)

A PID is a mechanism for public officials to disclose suspected wrongdoing, including fraud or corruption. The *Public Interest Disclosure Act 2013* (PID Act) provides protections for disclosers and legal remedies to address reprisal action taken against them as a result of making a disclosure. The PID Act also requires supervisors to give information to a Defence Authorised Officer if they receive information about disclosable conduct.

In Defence, public officials include current and former:

- Defence Australian Public Service employees
- Australian Defence Force permanent and Reserve members
- Cadets, Officers and Instructors of the Australian Defence Force Cadets
- contracted service providers that are, or have been, engaged under contract with Defence.

You can make a disclosure to a Defence Authorised Officer by telephone, in writing, including email, or in person. All reasonable efforts are made to protect a discloser's identity. With limited exceptions, it is an offence for a person to use or disclose the identifying information of a discloser.

CONTACT DETAILS

Email: *defence.pid@defence.gov.au*
Domestic Phone: 1800 673 502
International Phone: +61 2 6266 2433

If you would like further information, please visit *Defence PID* or the Australian Government Defence website – *Public Interest Disclosures*.

National Anti-Corruption Commission (NACC)

The NACC operates independently of government and has broad jurisdiction to investigate suspected serious or systemic corrupt conduct across the Commonwealth public sector.

Any person (including members of the public and public officials) can report corruption to the NACC, and there are protections provided for whistle-blowers and witnesses who provide information to the Commission. Please see the NACC website for further details.

Foreign Bribery

The Australian Government has a zero tolerance approach to foreign bribery and other forms of corruption and strongly discourages companies from making facilitation payments. Foreign bribery is bribery of a foreign public official. It is a serious criminal offence that carries heavy penalties. If Defence personnel suspect bribery of a foreign public official may have occurred, they must report the matter through the *Defence Incident Reporting Hub*. Defence refers suspected foreign bribery matters to the Australian Federal Police.

Responding to Fraud and Corruption

Any alleged fraudulent or corrupt behaviour that is reported or detected by Defence will be handled appropriately with consideration to the nature and seriousness of the allegation.

Investigating Fraud and Corruption

The Principal Integrity Officer is the lead authority within Defence for the investigation of fraud and corruption. In practice, Defence has established shared arrangements between Defence Integrity Division, the Joint Military Police Unit (for Australian Defence Force matters) and the Directorate of Conduct and Performance (for Australian Public Service matters) for the assessment and/or investigation of allegations of fraud and corruption within Defence's scope of responsibility.

Reported cases of fraud and corruption are assessed, and where appropriate, investigated by the relevant Defence Investigative Authority[2] in accordance with the Australian Government Investigation Standards and the Commonwealth Fraud and Corruption Control Framework 2024. Where matters involve potentially serious or complex offences, they may also be referred to the Australian Federal Police or to the NACC. Depending on the nature and seriousness of the allegation, investigations may be undertaken to an administrative, civil, and/or criminal standard of proof.

Investigation Outcomes

There are a number of outcomes that may result from a fraud or corruption investigation. Depending on the circumstances of the case, Defence may take administrative or disciplinary action in parallel, or as an alternative, to a criminal prosecution. Decisions are guided by a range of legislative requirements and Defence and Commonwealth policy such as the *Prosecution Policy of the Commonwealth*.

Defence takes all reasonable measures to recover fraud and corruption losses, including formal proceeds of crime action, civil recovery processes and administrative action.

Where fraud has been committed by a contractor, consultant or outsourced service provider, Defence will consider contractual actions such as financial penalties, contract renegotiation or termination. Administrative actions, such as declining future engagements will also be considered.

In cases where an investigation has identified control gaps, opportunistic non-compliance or opportunities for improvement, Defence will review and update the relevant controls where appropriate.

2 Defence Investigative Authority means any/all of the following: the Commander Joint Military Police Unit; Assistant Secretary Investigations and Public Interest Disclosures, Defence Integrity Division; Assistant Secretary Security Threat and Assurance, Defence Security Division; Director Conduct and Performance, Defence People Group.

Recording and Reporting Requirements

All reports of fraud and corruption, together with details on the management of those matters, including activities, critical decisions and outcomes, are recorded in the Defence ERP Case Management Solution (DECMS).

Regular reporting is an important part of effective governance and provides assurance over the appropriateness of Defence's control arrangements to prevent, detect and respond to fraud and corruption.

Defence undertakes the following fraud and corruption reporting

Internal

Enterprise Business Committee

Annual

Provide oversight of Defence's current and emerging key fraud and corruption risks.

Defence Audit and Risk Committee

Annual

Provide written advice to the Secretary and CDF on the appropriateness of:

- Defence's fraud control arrangements to detect, capture and effectively respond to fraud risks consistent with the Commonwealth Fraud and Corruption Control Framework; and
- Defence's system of risk oversight and management as a whole, with reference to the Commonwealth Risk Management Policy and Commonwealth Fraud and Corruption Control Framework, referring to any specific areas of concern or suggestions for improvement.

Defence Annual Report

Annual

The Secretary, as the Accountable Authority, provides:

- certification of compliance with section 10 of the PGPA Rule which deals with preventing, detecting and dealing with fraud and corruption; and
- a statement of any significant fraud and corruption issue reported to the Minister for Defence and Minister for Finance in accordance with section 17AG of the PGPA Rule.

External

Minister for Defence

Annual or as required

Minister for Finance

Annual or as required

The Accountable Authority reports significant fraud and corruption incidents, their management and the outcomes of criminal prosecutions in accordance with section 19 of the PGPA Act.

Australian Institute of Criminology

Annual

Provision of information on fraud and corruption metrics to inform the Australian Institute of Criminology annual Fraud against the Commonwealth census in accordance with the Commonwealth Fraud and Corruption Control Policy.

Commonwealth Ombudsman

Biannual

Provision of PID metrics in accordance with the PID Act.

Legislation and Policy

Legislation

- *Public Governance, Performance and Accountability Act 2013*
- *National Anti-Corruption Commission Act 2022*
- *Public Interest Disclosure Act 2013*
- *Defence Force Discipline Act 1982*
- *Public Service Act 1999*
- *Criminal Code Act 1995*
- *Defence Amendment (Safeguarding Australia's Military Secrets) Act 2024*

Commonwealth Fraud and Corruption Control Framework

The Commonwealth Fraud and Corruption Control Framework supports Defence to effectively manage the risks of fraud and corruption. The Framework is comprised of:

- **Section 10 of the PGPA Rule 2014** sets out the minimum standards in relation to managing the risk and incidents of fraud and corruption.
- **Commonwealth Fraud and Corruption Policy** sets out the procedural requirements that must be implemented in relation to specific areas of fraud and corruption controls such as investigations and reporting.
- **Resource Management Guide 201: Preventing, detecting and dealing with fraud and corruption** provides practical guidance on fraud and corruption control arrangements.

Accountable Authority Instructions

Accountable Authority Instructions are issued under the authority of section 20A of the PGPA Act to supplement the application of the PGPA framework (PGPA Act and the PGPA Rule 2014) within Defence.

Accountable Authority Instruction 1 - Managing Risk and Accountability

outlines arrangements for risk management and fraud and corruption control in Defence including key accountabilities.

Resources

- *Defence Values and Behaviours*
- *Australian Public Service Values, Code of Conduct and Employment Principles*
- *Defence and the Private Sector: Working with Integrity*
- *Defence Procurement*
- *Defence Procurement Complaints Scheme*
- *Defence Security Principles Framework*
- *Defence Public Interest Disclosure Scheme*
- *Incident Reporting Hub*

Contact us

Defence personnel, contractors, consultants and outsourced service providers must report suspected fraud and corruption.

If you suspect fraud or corruption

Defence personnel can report through the Defence *Incident Reporting Hub* intranet page.

The public can report through the *Complaints and Incident Reporting* page on the Australian Government Defence website.

Public Interest Disclosure Scheme

You can also make a disclosure to a Defence Authorised Officer by telephone, in writing, including email, or in person. All reasonable efforts are made to protect a discloser's identity.

Contact details

Email: *defence.pid@defence.gov.au*
Domestic Phone: 1800 673 502
International Phone: +61 2 6266 2433

For further information on the Defence Fraud and Corruption Control Plan, please contact *fraud.risk@defence.gov.au*.


207037

Australian Government

Defence