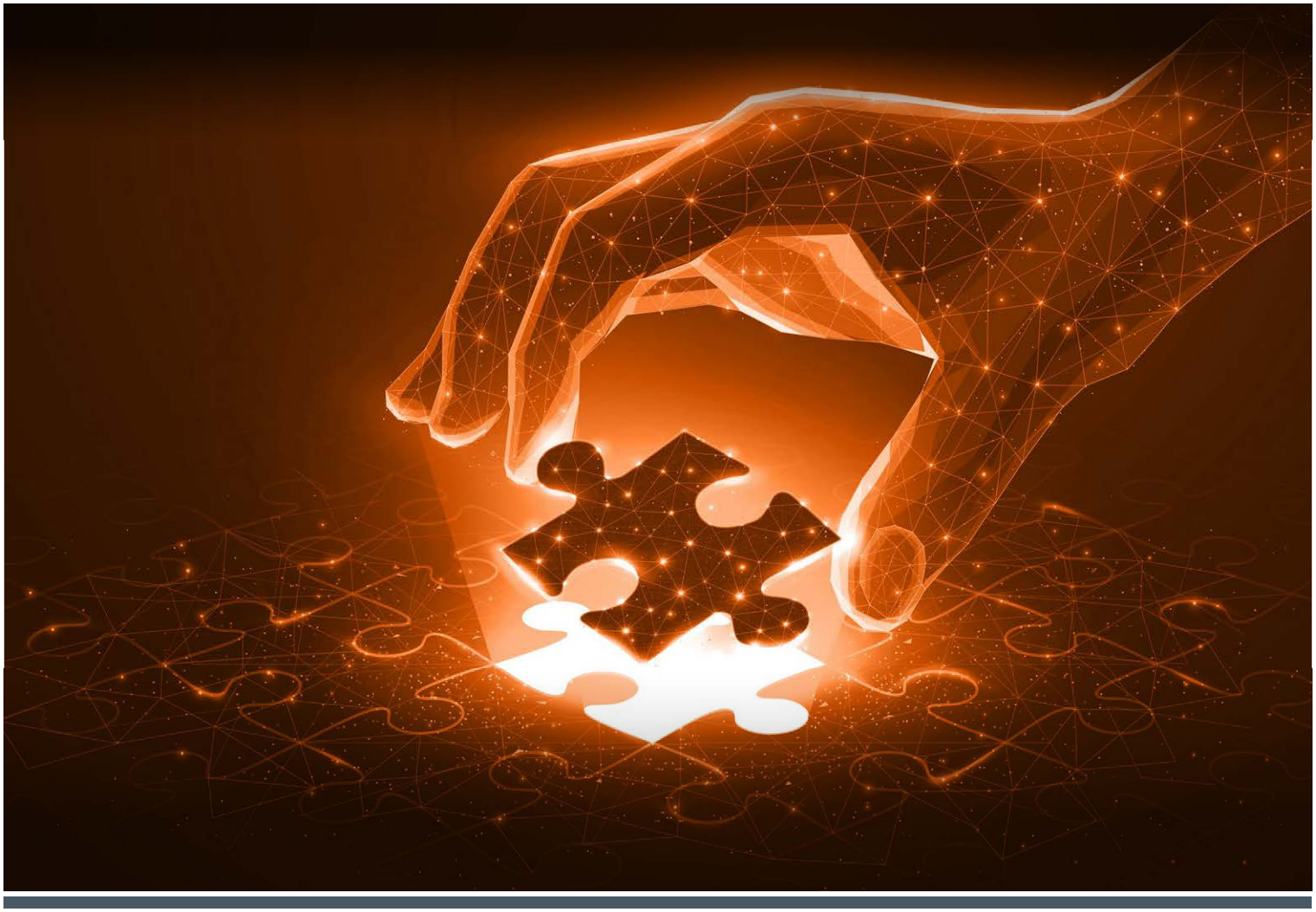
Australian Government
Defence

DEFENCE FRAUD AND CORRUPTION CONTROL PLAN 2022



ONE DEFENCE
WITH INTEGRITY

Defending Australia and its National Interests
www.defence.gov.au

SECRETARY AND CHIEF OF THE DEFENCE FORCE STATEMENT

Public confidence in the integrity of Defence and its personnel is vital to the proper operation of government, the defence of Australia and its national interests.

The Defence Transformation Strategy, together with the 2020 Defence Strategic Update and the 2020 Force Structure Plan, outline an unprecedented program of investment in Defence capability; Australian taxpayers are investing approximately $270 billion in Defence capability over the next decade. This investment increases the obligation on Defence to return public trust and confidence by delivering on this commitment with a strong basis of integrity, in the most efficient, effective and ethical means possible.

The nature of Defence business, and the scale of this investment expose the department to some significant and unique fraud and corruption risks which can:

- reduce the resources available for delivering priority Defence capabilities in fulfilling their intended purpose;
- place the safety of our personnel and assets at risk; and
- undermine public confidence in Defence and the Australian Government's stewardship of public resources.

The Defence Fraud and Corruption Control Plan (DFCCP) documents the department's approach to the identification and management of fraud and corruption risks. Consistent with Commonwealth compliance requirements and current best practice, this plan gives rise to a live and dynamic fraud and corruption prevention, detection and response system, reflecting Defence's need to adapt fraud and corruption control activities to address the constantly changing strategic environment.

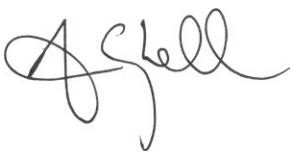
All Defence personnel and contractors play a critical role in our anti-fraud and corruption control strategies and are expected to act with the highest integrity, in a manner that is ethical, transparent and promotes accountability.

This plan provides the means for all Defence personnel and those who undertake business with Defence to recognise current fraud and corruption risks and vulnerabilities and how they can integrate control strategies in their everyday business.

Greg Moriarty

Secretary

26th May 2022



Angus J Campbell AO, DSC

General

Chief of the Defence Force

26th May 2022

DEFENCE FRAUD AND CORRUPTION POLICY STATEMENT

The Australian Government expects all Commonwealth officials or persons otherwise engaged through contract by the Commonwealth to collectively prevent, detect and deal with fraud and corruption. All personnel are expected to behave with integrity, at all times. Defence will take action to deal with fraudulent and corrupt behaviour.

DEFENCE INTEGRITY FRAMEWORK

This plan is a key component of the Defence Integrity Framework. Built on the three pillars of '*People, Processes and Technology',* the Defence Integrity Framework supports a range of prevention, detection and response measures to ensure a systemic and integrated approach to integrity across Defence.

DEFINITIONS

Fraud

Fraud is defined in the *Commonwealth Fraud Control Framework*, as:

"dishonestly obtaining a benefit or causing a loss by deception or other means."

Fraud can be committed by personnel (internal fraud) or by persons external to Defence (external fraud). It may also be committed jointly between an employee and an outside party. Fraud offences against the Commonwealth may be prosecuted under a number of Commonwealth laws.

Examples of the type of conduct by personnel, contractors or third party providers that fall within Defence's definition of fraud include (but is not limited to):

- theft or misuse of Commonwealth information, intellectual property or confidential information (including funding proposals, procurement information, personal records)
- misuse of Commonwealth program funding and grants
- misuse of Commonwealth resources, including unlawful use of, or unlawful obtaining of, property, equipment, material or services
- abuse of official position in order to obtain a benefit for oneself or another
- misuse of entitlements (e.g. expenses, leave, travel allowances or attendance records, including abuse of time off in lieu)
- misuse of facilities (e.g. unauthorised use of Defence Estate, information technology, mobile devices, and telecommunication systems)
- financial fraud (e.g. unauthorised use of credit cards, false invoices, misappropriation)
- causing a loss, or avoiding and/or creating a liability
- providing false or misleading information and/or documents to the Commonwealth, or failing to provide information (when an obligation exists)
- making, or using forged or falsified documents; and
- release, or use of misleading information for the purposes of deceiving, misleading or to hide wrongdoing.

Corruption

Corruption can be defined as:

"Dishonest activity in which a director, executive, manager, employee, member or contractor of an entity acts contrary to the interests of the entity and abuses their position of trust in order to achieve some personal gain or advantage for themselves or for another person or organisation.[1]"

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

- collusion between a Commonwealth official and a contractor
- bribery (domestic or foreign)
- 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; and
- insider trading – misusing official information to gain an unfair private, commercial or market advantage for self or others.

NON-COMPLIANCE AND UNETHICAL BEHAVIOUR

Non-compliance is a broad term for any failure to comply with legal requirements. These requirements may be in the form of legislation, regulation, funding agreements, administrative rules, and licensing conditions. Examples include the requirement for all APS personnel to act in accordance with the APS Code of Conduct, which is set out in section 13 of the *Public Service Act 1999* (PS Act); and the requirement for all Australian Defence Force (ADF) members to act in accordance with the *Defence Force Discipline Act 1982* (DFDA).

This includes where parties try to comply but make mistakes (accidental non-compliance), or where parties exploit ambiguities or opportunities that are non-compliant (opportunistic non-compliance).

1 Australian Standard (AS) 8001-2021: Fraud and Corruption Control

GOVERNANCE

KEY RESPONSIBILITIES

All Defence personnel should understand what constitutes fraud and what to do if they suspect fraudulent activity. All personnel are expected to comply with legislative requirements and internal policies, behave in accordance with the above integrity requirements, and identify and report fraud and corruption risks.

Certain positions and committees have additional responsibilities, including:

- The **Secretary** is the accountable authority responsible, under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), for governing the department in a way that promotes the proper use of public resources. This includes taking all reasonable measures to prevent, detect and respond to fraud and corruption relating to Defence personnel, services or third parties who interact with the department. The Secretary and the **Chief of the Defence Force** (CDF) have approved this plan, demonstrating their combined commitment to the control of fraud and corruption.

  The Secretary and CDF have delegated some authority to other accountable officers and committees.
- The **Associate Secretary** has the corporate responsibility for overseeing the implementation of fraud prevention and control for Defence, in line with Section 10 of the PGPA Rule.
- The **Chief Finance Officer** has accountability for setting Defence's financial framework and ensuring that risks associated with the department's appropriations and expenditure are addressed.
- The **Chief Information Officer** facilitates the protection of Defence information security and access control.
- The **Chief Security Officer** has accountability for implementing the requirements of the Protective Security Policy Framework and the Defence Security Principles Framework across Defence.
- The **Principal Integrity Officer (PIO)** maintains enterprise accountability and responsibility for the provision of independent and objective assurance on the fit-for-purpose nature and quality of the Defence Integrity Framework. The PIO is also responsible for promoting an ethical culture throughout Defence to complement governance arrangements and increase the department's capacity to prevent, detect and deter fraud and corruption.
- The **Defence Integrity Division** is responsible for designing, implementing and evaluating fraud strategies and countermeasures in line with the various risk exposure levels.
- The **Enterprise Business Committee** considers current and emerging risks, which may include fraud and corruption, in the context of Defence's strategic objectives.
- **Group Heads and Service Chiefs** are responsible for leading the establishment and maintenance of an ethical culture within their organisations together with the implementation and operation of governance arrangements. This includes:
  - appointing a suitably resourced and qualified Group Fraud Control Coordinator;
  - ensuring that the risk of fraud and corruption is considered in the planning and development of programs and the conduct of activities under their control;

- ensuring that Defence personnel in their Group participate in mandatory fraud and integrity awareness training at least every two years;
- responding to requests from the Principal Integrity Officer to conduct fraud control activities including the conduct of a Group Fraud Risk Assessment; and
- ensuring their organisations understand and comply with relevant legislation, regulations, procedures and policies.

In addition to the above, the **Defence Audit and Risk Committee** oversees Defence's system of risk management, internal controls, including fraud and corruption risk, and provides independent advice to the Secretary and CDF on their appropriateness.

DEFENCE FRAUD AND CORRUPTION RISKS

Defence-wide fraud and corruption risk assessments are conducted and reviewed every two years.

The fraud and corruption risks identified below are the result of a Defence-wide fraud risk assessment conducted in accordance with AS/NZ ISO standards, in 2021.

Defence Fraud and Corruption Risks	Examples
Theft misuse and/or unauthorised disclosure of Defence information	• Unauthorised release of commercially sensitive information, often as a result of an existing conflict of interest which may or may not have been declared
Fraudulent or corrupt procurement and contract management practices by domestic and / or overseas staff	• Suppliers offering or providing gifts, benefits or other incentives to Defence personnel • Undeclared conflicts of interest
Theft of Defence assets	• Theft of Defence assets including: – Mobile devices – Commonwealth vehicles – Specialised military equipment – Weapons and ammunition – Consumables – Fuel and lubricants
Collusion between supplier organisations during bidding	• Preferential treatment of suppliers • Collusion between suppliers to manage pricing and control the market
Fraudulent/corrupt behaviour by staff involved in accounts payable	• Undeclared conflicts of interest • Supplier paid for goods or services not rendered

To reduce enterprise-wide fraud and corruption risks in areas with higher levels of exposure, Defence continues to strengthen systems and countermeasures for conflicts of interest, post separation employment and unauthorised access to sensitive information.

CONFLICTS OF INTEREST

A conflict of interest refers to any situation where there is, or may appear to be, conflict between a person's personal interests and their public duties and responsibilities. Undeclared or poorly managed conflicts of interest are enablers of fraud and corruption in Defence.

Conflicts of interests are not inherently negative and can occur without anyone being at fault. However, it is vital they are disclosed and managed effectively so that Defence personnel perform their duties in a fair and unbiased way.

The need to manage conflicts of interest are based on two expectations:

- That people in public positions must avoid situations in which private interests can affect their public duties – an actual conflict of interest.
- That people in public positions should avoid the perception or potential for a conflict of interest to arise. In Defence, we refer to these types of conflicts of interest as potential or perceived.

Defence has a mature and comprehensive system of controls to mitigate and/or manage the risks posed by the realisation of conflicts of interest, including comprehensive policies mandating the declaration and management of conflicts of interest by Defence personnel, Defence tenderers and Defence contractors.

POST SEPARATION EMPLOYMENT CONFLICTS OF INTEREST

Conflicts of interest can arise between a Defence official's current duties and proposed future employment.

Defence personnel are required to inform the department in writing if they are approached with a formal offer of employment or if they apply for employment, where an actual, potential or perceived conflict of interest between their current official duties and the proposed future employment could arise. Where a decision maker determines that an actual, potential or perceived conflict of interest exists or is likely to exist, appropriate management strategies must be put in place.

Similarly, former Defence personnel (ADF or APS) may be restricted from performing or contributing to the performance of a contract (as an employee of the contractor) for a period of time following their separation. This may apply where a person was involved in the preparation or management of the contract, the assessment or selection of the contractor, or the planning or performance of the procurement or activity relevant to the contract.

THEFT, MISUSE AND UNAUTHORISED DISCLOSURE OF DEFENCE INFORMATION

The security of information is critical to the integrity of Defence's mission. If Defence does not protect its own information and information received from external parties from unauthorised access, its ability to function in support of the Government will be undermined.

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.

DEFENCE FRAUD AND CORRUPTION CONTROLS

Defence's approach to fraud and corruption control is consistent with Commonwealth legislative requirements. The Defence Fraud Control Framework operates to prevent, detect and respond to fraud and corruption.

PREVENTION

Fraud and corruption prevention strategies establish the 'first line of defence', focussing on the establishment and maintenance of sound governance systems, systems of control and an ethical organisational culture. Key components of Defence's fraud and corruption prevention strategy are:

- **Fraud and Integrity Awareness:** ADF members and APS personnel are required to complete Fraud and Integrity Awareness training within the first six months of commencement and at least once every two years, thereafter. Contractors and External Service Providers may be required to complete this training if the Commonwealth deems it relevant or applicable to a contract or deed. This mandatory training is supplemented by periodic campaigns to raise awareness of integrity-related matters within Defence.
- **Procurement and Contracting:** Appropriate levels of due diligence and probity are required at all stages of the procurement and contract life cycle to ensure adherence to procurement rules and policy, and the integrity expectations of the department. All suppliers, including contractors, consultants and external service providers are subject to appropriate due diligence and probity processes.
- **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 and accountability and early identification of loss or theft.
- **Information Controls:** In line with the Commonwealth's protective security measures, Defence, in partnership with the Australian Signals Directorate takes a systematic approach to ICT security risk management, network usage and detection capabilities.
- **Financial Controls:** Defence Finance Group 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 *Public Governance, Performance and Accountability Act 2013*. A range of assurance initiatives are also in place to help ensure the integrity of financial data and management across Defence.
- **Personnel Controls:** Defence maintains a range of personnel controls, including:
  - **Australian Defence Force Personnel** – The *Defence Act 1903* governs the appointment to, or enlisting of, persons in the ADF. All Royal Australian Navy, Australian Army and Royal Australian Air Force personnel must complete an Acknowledgement of the Requirements of Service. This acknowledgement clearly outlines that fraud and related offences will not be tolerated in the ADF and may constitute grounds for termination of service.
  - **Australian Public Service Personnel** – The employment of APS personnel within Defence is guided by the relevant provisions of the *Public Service Act 1999* and accompanying regulations and directions.

All Defence personnel are required to hold a recognised Australian Government Security Vetting Agency security clearance, and to maintain this clearance throughout the duration of their employment with Defence.

Defence personnel and external service providers are to be security-cleared to the level commensurate with the level of classified information or assets they are required to access, or the responsibilities they hold.

DETECTION

No system of preventative controls can provide absolute assurance that fraud or corruption is not occurring. It is therefore critical that effective systems for detecting fraud and corruption as early as possible are in place to enable an effective response and minimise the impact on Defence. Measures to detect internal and external fraud, as well as corruption within Defence include:

- **Mandatory Reporting:** An instance of fraud or corruption is considered a Notifiable Incident, and must be reported to the chain of command/management and a Defence Investigative Authority. Where there is a requirement to report suspected fraud and corruption externally, a relevant Defence Investigative Authority will consult with the appropriate law enforcement agency or other agency undertaking law enforcement activities.
- **Public Interest Disclosure (PID) Scheme:** This scheme provides a legislative framework for the protected disclosure and investigation of serious wrongdoing within the Commonwealth public sector. All Defence personnel and contractors are encouraged to report suspected wrongdoing within the workplace using existing mechanisms and engage the PID scheme, where appropriate.
- **Business intelligence:** Defence has in place a comprehensive, data-driven program targeting key fraud and corruption risks across the Defence enterprise.
- **Financial Management Compliance:** Defence conducts a range of activities to monitor financial compliance across the department. Fraudulent transactions are assessed and, where appropriate, referred for investigation.
- **Internal Audit and Independent Reviews:** Internal audit activity and independent reviews play an important role in the detection of fraud and corruption, and ensures key internal control mechanisms are effective and support compliance measures.
- **Defence Procurement Complaints Scheme:** This scheme provides a mechanism for the reporting and management of complaints about Defence procurements.

RESPONSE

Fraud and corruption response is a key element of the overall fraud control framework in Defence. The nature of the response will be dependent on the individual circumstances of a case. The primary objective of a response to an event is to ensure that perpetrators of fraud are identified and appropriate remedies applied in order to achieve a deterrent effect.

Defence has a measured response to each reported case of fraud.

- **Investigation:** Suspected instances of fraud that are considered routine in nature are undertaken by Defence in accordance with the Australian Government Investigation Standards. The Principal Integrity Officer is the lead authority within Defence for the investigation of fraud and corruption impacting on the department.

In practice, Defence has established shared arrangements between the Defence Integrity Division, the Joint Military Police Unit and the Directorate of Conduct and Performance (for APS matters) for the investigation of allegations of fraud and corruption, which recognise the existence of competent investigative capabilities and appropriate legislative regimes. Where appropriate, Defence will refer a matter for investigation by an external law enforcement authority. Depending on the circumstances of the case, administrative or disciplinary action will be considered in parallel, or as an alternative, to a criminal prosecution.

- **Recovery:** Defence takes reasonable measures for recovery of fraud losses, including formal proceeds of crime action, civil recovery processes and administrative action.

REPORTING AND MONITORING

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 internal and external reporting:

- In accordance with the *Commonwealth Fraud Control Framework*, the Principal Integrity Officer reports to the Minister for Defence on significant fraud and corruption incidents, their management and the outcomes of criminal prosecutions.
- To further assist Defence to meet its reporting obligations under the *Public Governance, Performance and Accountability Act 2013*, the Principal Integrity Officer supports the Chief Finance Officer with details on fraud cases to enable annual reporting to the Minister for Defence and the Minister for Finance on significant non-compliance with finance law.
- Annual reporting to the Enterprise Business Committee within the context of the Defence's current and emerging strategic business risks.
- Biannual reporting to the Defence Audit and Risk Committee which provides oversight and advice to the Accountable Authority in accordance with section 45 of the *Public Governance, Performance and Accountability Act 2013*.
- Annual and biennial reporting to the Australian Institute of Criminology (AIC). All non-corporate Commonwealth entities are required to collect information on fraud and complete an annual fraud questionnaire to the AIC in accordance with the Commonwealth Fraud Control Policy.
- Annual reporting to the Commonwealth Ombudsman in relation to public interest disclosures.
- Annually, Defence certifies in the Defence Annual Report that the department has prepared fraud risk assessments and a Fraud and Corruption Control Plan, and has in place appropriate fraud prevention, detection, investigation, reporting and data collection processes.

FURTHER INFORMATION

Queries about the Defence Fraud and Corruption Control Plan can be forwarded to fraud.risk@defence.gov.au

Related Information:

Commonwealth Fraud Control Framework 2017

Defence Instruction (Administration Policy)

Australian Government Investigations Standards

APS Values and Code of Conduct

One Defence Leadership Behaviours

Defence Act 1903

Defence Force Discipline Act 1982

Defence Integrity Policy Manual

Defence Incident Reporting and Management Manual

Defence Commercial Policy Framework

Defence Security Principles Framework

Defence Public Interest Disclosure Scheme

Defence Procurement Complaints Scheme

Public Governance, Performance and Accountability Act 2013

Public Interest Disclosure Act 2013

Public Service Act 1999

ONE DEFENCE
WITH INTEGRITY

Developed by Defence Integrity Division, Department of Defence