National Anti-Corruption Commission

Integrity Outlook

2022/23

This brief provides an overview of the corruption risks and vulnerabilities identified between July 2020 and June 2023 from finalised investigations under the *Law Enforcement Integrity Commissioner Act 2006* and related prosecutions.

Enquiries about this report can be directed to the
National Anti-Corruption Commission
GPO Box 605, Canberra, ACT, 2601
or by email to contact@nacc.gov.au

This publication should be attributed as:

Integrity Outlook 2022-23

National Anti-Corruption Commission, Canberra.

The terms under which the coat of arms may be used can be found on the Digital Transformation Agency website.

Contents

Summary

The Integrity Outlook 2022/2023 presents important trends relating to corruption and integrity risks and vulnerabilities for Commonwealth agencies. It uses evidence collected from investigations conducted by the Australian Commission for Law Enforcement Integrity (ACLEI) under the *Law Enforcement Integrity Commissioner Act 2006* (the LEIC Act) over the last three financial years (2020-2023) to identify these risks.

This report provides stakeholders, government agencies and the general public with information on the main corruption and integrity risks identified. This is intended to inform corruption prevention strategies and otherwise assist policymakers. It also provides the basis for future iterations of the Integrity Outlook, as part of the National Anti-Corruption Commission's (the Commission) mandate to report on risks and vulnerabilities.[1]

The available evidence indicates that **misuse of information** is the most widespread form of corrupt conduct, presenting a ubiquitous integrity risk. This category includes unauthorised access to or modification of restricted data, and unauthorised disclosure of information. In many cases, unlawful access to government information is a precursor to subsequent disclosure to unauthorised third parties. This highlights the risks associated with unlawful access, and the scope for reducing risk by vigilance in this area.

[1] See s 271(2)(c) and s 164(2) of *the National Anti-Corruption Commission Act 2022* (the NACC Act).

Conflicts of interest are also a prevalent source of corruption issues. Many types of corrupt conduct – such as breaches of public trust, abuse of office and misuse of information – originate from conflicts of interest. Such conflicts therefore pose a substantial risk for government agencies, parliamentarians, and public officials. This is why identifying, disclosing and managing potential conflicts of interest is a critical pillar in integrity architectures.

Another key vulnerability is **fraud**, which includes misuse of credit cards, forging official documents, theft, and mis-using intellectual property.[2] Fraud is widespread. It detracts from the resources available and can be very costly. It can also be associated with the involvement of organised crime which exacerbates the integrity risks.

Abuse of office is yet another significant risk, which can be mitigated by prevention strategies. Examples of abuse of office include soliciting or receiving a bribe, perpetrating visa fraud, and exploiting public resources for personal gain.

Finally, it is important to be alert to **grooming**, which is the practice of building personal relationships and influence with officials, with a view to then exploiting them for private gain or access to information. Grooming can be attempted by diverse individuals and groups, including organised crime, foreign actors, commercial enterprises, and others who wish to influence decision-making or access confidential information. Grooming is an illustration of how different integrity risks and vulnerabilities can overlap, creating complex challenges for policymakers and prevention practitioners.

---

[2] Explore the fraud problem | Commonwealth Fraud Prevention Centre (counterfraud.gov.au).

The Commonwealth Integrity Maturity Framework (CIMF)[3] is a tool, for agencies of all sizes and levels of exposure, to assist in creating and maturing their integrity mechanisms. Such tools enhance the integrity ecosystem in the Commonwealth public sector by providing agencies with support to prevent, report and address integrity issues within their jurisdictions.

[3] Commonwealth Integrity Maturity Framework | National Anti-Corruption Commission (NACC).

Methodology

The corruption vulnerabilities identified in this report are drawn from investigations of alleged or suspected corrupt conduct by staff members of agencies within the former ACLEI jurisdiction.

The information contained in this report is based on an analysis of:

- ACLEI investigation reports resulting in findings of corrupt conduct
- Agency final investigation reports resulting in findings of misconduct[4]
- ACLEI investigations resulting in criminal convictions of Commonwealth officials.

Data

The data used for this report is for the period FY 2020-2023. This enables identification of recurrent risks and vulnerabilities over that period, and to some extent of trends. As the work of the Commission progresses, the addition of data for longer periods may permit more rigorous analysis.

[4] Section 66 of the *Law Enforcement Integrity Commissioner Act 2006* (Cth) required agencies to report to ACLEI on their internal investigations into corruption issues.

Key risks and vulnerabilities

Misuse of information

The most prevalent form of corrupt conduct is misuse of information, comprising unauthorised access to, disclosure and modification of information.

Government information is a valuable and coveted commodity. Possession of such information can give its holders significant power, economic advantage, and capacity to exploit government policy. As a result, its misuse is a high-risk vulnerability, which is reinforced by its prevalence. It is an offence for a Commonwealth officer (or persons performing services for or on behalf of the Commonwealth) to disclose information made or obtained while being, or having been in the past, a Commonwealth officer.[5] The Australian Public Service (APS) Code of Conduct provides that APS employees 'must not improperly use inside information or the employee's duties, status, power or authority to gain a benefit or cause a detriment'.[6]

Misuse of information can be seen in two categories, namely, unauthorised *access* and unauthorised *disclosure*, though both can be involved in the same corrupt activity.

Unauthorised access

This refers to an official accessing information without authority, or without a lawful business purpose, or outside their security clearance. The

---

[5] *Criminal Code Act 1995* (Cth), s 122.4.

[6] *Public Service Act 1999* (Cth), s 13 APS Code of Conduct.

reasons for these types of unlawful accesses can range from ignorance of current regulations, to curiosity, to criminal motivation.

Unauthorised disclosure

This involves the illegal provision of official information to third parties. The motives may be associated with conflicts of interest, grooming (both addressed later in this report), and the involvement of third parties such as organised criminal groups, foreign actors, or commercial interests.

The Commonwealth's Protective Security Policy Framework (PSPF) sets out the requirements for agencies to safeguard official information and communication technology systems to maintain the confidentiality, integrity, and availability of all official information. These include the implementation of operational controls proportionate to the value, importance, and sensitivity of the information.

The use of information technology and information security infrastructure that allows for timely auditing and reporting is a key measure in the effective deterrence, detection and investigation of issues relating to unauthorised access and disclosure of information.

In this context, it is important that agencies which hold sensitive information have in place policies and procedures that support the security of that information. These can include proactive, regular, and targeted auditing of access to information systems and databases. This helps identify any instances of access to information that is not for a legitimate purpose, and operates as a deterrent to unauthorised access. As information can be misused after the official has ceased to be employed, there is a requirement for post-employment restraints, management and controls.

Conflicts of interest

Conflicts of Interest (COI) are also a prevalent source of integrity issues in government agencies. For example, in 2021, 18.7% of APS employees who reported witnessing corruption said they had witnessed individuals acting (or failing to act) in the presence of an undisclosed conflict of interest.[7] Over the same period, 50 APS employees were found to have breached the APS Code of Conduct requirement to disclose any material personal interests and take steps to avoid real or apparent conflicts of interest.[8] Moreover, conflicts tend to be the origin of many other forms of corrupt conduct, including breach of public trust, abuse of office, and misuse of information.

COI can be actual, potential, or perceived. COIs arise when an official's interests, affiliations, or relationships impact, can potentially impact or can be perceived to impact their impartiality in the discharge of their official duties. It is important to note that all three can be damaging to an official or agency's reputation, if not managed properly. Conflicts undermine confidence in public decision-making.

---

[7] Australian Public Service Commission, *APS Employee Census Overall Results 2021*, APSC website (accessed 03/10/22).

[8] Australian Public Service Commission, 2021, *APSC State of the Service Report 2020-21, 'Reform in the shadow of COVID-19'*, APSC website (accessed 03/10/22).

Conflicts of interest typology

Type	Description
Actual	A direct conflict which impacts an official's impartiality.
Perceived	When members of the public may reasonably assume a COI is present.
Potential	A COI is not present but may appear in the future if not managed.

Commonwealth officials have an obligation to disclose relevant interests under s 29 of the *Public Governance, Performance and Accountability Act 2013* (Ch) (PGPA Act). In addition, the APS Code of Conduct requires APS employees to take reasonable steps to avoid any conflict of interest (real or apparent) and to disclose details of any material personal interest in connection with the employee's APS employment.[9] Material personal interests can relate directly to an official's role, or more broadly to the overall purpose of the entity. The *Public Governance, Performance and Accountability Rule 2014* (Cth) details how and when officials need to disclose material personal interests, and the circumstances when the duty to disclose does not apply.[10]

---

[9] *Public Service Act 1999* (Cth), Section 13(7).

[10] *Public Governance, Performance and Accountability Rule 2014* (Cth), Sections 12-16D.

An employee holding a security clearance is subject to a separate requirement under the PSPF to notify their agency or the Australian Government Security Vetting Agency (AGSVA) of any changes to financial circumstances or associations that may give rise to actual or perceived conflicts of interest. The purpose of this notification is to determine the employee's ongoing suitability to hold a security clearance.

Potential conflicts are inescapable: it will be commonplace for officials occasionally to know or have an interest in individuals or entities that might be affected by a decision. The key point is the management of such potential conflicts, typically on a case-by-case basis, by disclosure and recusal. Risks associated with COI can be reduced through several mechanisms. These include training for officials on the identification and disclosure of conflicts of interest, the implementation of routine requirements for disclosure of conflicts, and the regular analysis, reporting and review of conflict-of-interest issues.

Fraud

Fraud is defined as "dishonestly obtaining a benefit, or causing a loss, by deception or other means".[11] It has a close correlation with corruption. The magnitude of the issue is illustrated by:

The Australian Institute of Criminology found that the cost of fraud against the Commonwealth in 2020-21 was $265.9 million.

[11] Commonwealth Fraud Control Framework | Attorney-General's Department (ag.gov.au).

In the same period, 80,184 allegations of fraud against the Commonwealth were received or detected by government entities.[12]

Moreover, there is reason to suppose that fraud is significantly more prevalent than official figures suggest.

For analytical purposes, fraud can be categorised as internal or external. Internal fraud refers to fraud perpetrated by an entity's official or a contractor, while external fraud refers to fraud perpetrated on the agency by an external actor.

Types of internal fraud

Type	Description
Credit card fraud	When employees use their Commonwealth credit cards for personal expenses unrelated to official duties, and without explicit authorisation from the relevant financial delegates.
Misuse of resources	When an official uses government resources for purposes other than those specified by the entity or relevant regulations.

[12] Fraud against the Commonwealth 2021–22 (aic.gov.au).

Type	Description
Timesheets and medical certificates	When an official provides false or misleading information in response to a request for information that is made for official purposes in connection with the employee's APS employment.

The Commonwealth Fraud Control Framework (Framework) under the PGPA Act outlines the Australian Government's requirements for fraud control. It requires Commonwealth entities to put in place a comprehensive fraud control program that covers prevention, detection, investigation, and reporting strategies.

Minimising the incidence of internal fraud through the identification and management of fraud risks should continue to be an ongoing focus of agencies. This can be achieved through the development, implementation and regular review of fraud prevention and detection strategies.

Abuse of office

Examples of conduct which can fall under the abuse of office label:

- unauthorised access to and disclosure of information
- receiving bribes
- misuse of Commonwealth resources

The concept of abuse of office involves an official using their official capacity improperly to obtain a benefit for themselves or another person,

or to cause a detriment to another person. This type of misconduct is sometimes described as abuse of power or authority.[13]

Many categories and instances of corrupt or improper conduct involve at some point an official abusing their position. An abuse of office can be committed through the exercise of influence arising from the person's public office, or the use of information obtained in their capacity as a public official, or any other conduct in that capacity. An official can also abuse their office if they use their position to force or persuade a third party into actions in which they would otherwise not engage.

Abuse of office is not only corrupt conduct, but also a criminal offence in its own right.

The use of information technology can be a key tool for the prevention of abuses of office, particularly as they relate to access to information. Clear record-keeping of access can serve as a deterrent for this misconduct. Education and awareness programs focussing attention on the risks associated with attempts to obtain personal benefits from office can also be useful.

People

Ultimately, it is individuals who engage in corrupt conduct.

The personal circumstances of employees, such as relationship breakdowns, financial pressures, and illness, are associated with corruption risk. Agencies should consider *early intervention systems*, which are evidence-led strategies to analyse and identify corruption

[13] In this report, abuse of office and abuse of power/authority are addressed together.

patterns and trends. This helps identify opportunities to act and disrupt behaviours which might lead to corrupt conduct.[14] Benefits of early intervention include:

- the support of staff facing adverse circumstances
- the prevention of serious misconduct through early identification of at-risk behaviour
- empowering frontline supervisors to engage with staff on wellbeing and performance issues.

Grooming

Grooming (in the integrity context) is the process by which public officials are deliberately targeted, either through the intentional building of trust or by deliberate coercion and threats, with a view to gaining access to confidential information, influencing government outcomes and processes, or gaining commercial advantages.

The ideal target for grooming is an official who may be experiencing financial difficulties, is unhappy or frustrated in the workplace, is isolated, or is experiencing domestic or other personal challenges. These factors make them vulnerable to the advances of people offering support, gifts, and other benefits.

[14] Macintyre S, Prenzler T, Chapman J, International Journal of Police Science & Management (2008-10:2), *Early Intervention to Reduce Complaints: An Australian Victoria Police Initiative*.

The process of grooming typically involves three stages:

1. **Targeting**. The official is identified by the potential corrupter as a vulnerable individual.

2. **Relationship building**. The corrupter builds a relationship with the official. Typically, this is done deceptively through strategies such as friendship, gifts, offers of support etc. This generates in the victim a sense of reciprocal obligation and loyalty. However, in some cases it may be by threats, extortion, and violence.

3. **Coercion and corrupt conduct.** Once the relationship has been established, the corrupter then asks or demands the official to engage in corrupt or unethical conduct. This can involve both actions and omissions by the government official, such as unlawful access to information, disclosure of protected information, taking of bribes, and overlooking unlawful conduct.

There are many actors who may have an interest in gaining personal access to government officials. The diversity of these groups and individuals signals the challenge that corruption prevention practitioners face when designing policies to address grooming. They include:

- **organised criminal groups** will look for access to sensitive information, particularly law enforcement information including in relation to investigations or border control activity, which helps them avoid detection.

- **individuals and businesses** may seek to groom officials for information or to exercise their regulatory powers to provide them with a commercial or private advantage.

- **former colleagues** now working in the private sector may use their personal networks and relationships to 'reach-back' into contacts and colleagues in government agencies to obtain insider information.
- **foreign entities** pose an inherent risk of espionage and foreign interference to organisations that deal with sensitive government information.
- **extremist groups** can target public officials and actively seek to forge relationships with like-minded 'insiders' in the public service in pursuit of politically motivated objectives.

Conclusion

The Integrity Outlook presents the most frequently occurring integrity risks and vulnerabilities for Commonwealth entities found in ACLEI investigations for the period FY 2020-2023. **Misuse of information** stands out as the most common form of misconduct, followed by **abuse of office (**including of power or authority) and **fraud** against the Commonwealth, which is costly and probably more common than assumed. **Conflicts of interest**, whether real, potential, or perceived are a risk not only in practical financial terms but are also a significant reputational risk to Commonwealth agencies, and lie at the heart of many forms of corrupt conduct. Employees who are under financial or personal stress are vulnerable to **grooming** and are more likely to engage in corrupt conduct. Early intervention programs for such employees are indicated as a means of addressing this risk.

The integrity issues discussed in this report indicate the need for agencies to implement targeted prevention work in the areas of access to information, through the use of information technology to monitor and audit access, clear rules governing access to information, and clear procedures requiring the disclosure of conflicts of interest.

The Commission's corruption prevention function will continue to develop and deliver research, policies and outreach to aid in managing and reducing integrity risks and vulnerabilities in Commonwealth agencies.