Australian Government
Australian Commission for Law Enforcement Integrity

Corruption Vulnerabilities Brief 2020-21

This brief provides an overview of the corruption vulnerabilities identified between July 2020 and June 2021 from finalised investigations under the *Law Enforcement Integrity Commissioner Act 2006* and related prosecutions.

Enquiries about this report can be directed to the
Australian Commission for Law Enforcement Integrity
GPO Box 605, Canberra, ACT, 2601
or by email to contact@aclei.gov.au

Reports published by the Integrity Commissioner
and summaries of reports which have not been made public
can be found on the ACLEI website: aclei.gov.au

This publication should be attributed as:

Corruption Vulnerabilities Brief 2020/21

Australian Commission for Law Enforcement Integrity, Canberra.

Contents

Summary

The 33 scenarios analysed in this Corruption Vulnerabilities Brief highlight the vulnerability of Commonwealth officials to attempted corruption by others who seek to obtain sensitive information to which they have access. Official information is a valuable commodity for individuals seeking to enter Australia, bring goods into Australia, access or obtain government services, or find out information about law enforcement operations.

The vulnerabilities identified in this report may be relevant to non-law enforcement Australian Government agencies.

Agencies are invited to consider how these vulnerabilities are relevant to their staff and functions and put in place proactive strategies to mitigate corruption risk.

The Australian Commission for Law Enforcement Integrity (ACLEI) provides tailored corruption prevention advice and has a range of resources to assist agencies to strengthen their integrity frameworks.

Methodology

The corruption vulnerabilities identified in this report are limited to investigations which fall within the Integrity Commissioner's jurisdiction under the *Law Enforcement Integrity Commissioner Act 2006 (Cth)* (LEIC Act). That is, investigations of alleged corrupt conduct by staff members of agencies within the Integrity Commissioner's jurisdiction.

The information contained in this report is the result of an analysis of:

- 9 ACLEI investigation reports resulting in findings of corrupt conduct and/or corruption prevention observations.[1]
- 21 agency final investigation reports resulting in findings of misconduct.[2]
- 5 final criminal convictions of Commonwealth officials arising from issues brought to ACLEI's attention, including 2 which were the subject of ACLEI investigation reports.[3]

The 33 scenarios analysed for this report involved corrupt conduct and misconduct by staff members from 4 agencies within the Integrity Commissioner's jurisdiction. The matters analysed in this brief were initially reported to ACLEI between 2013 and 2019 and involved conduct that occurred across various timeframes ranging from 2000 to 2019.

Table 1 depicts the date the corrupt conduct or misconduct commenced, by number of matters. As this Vulnerabilities Brief is based on the outcomes of investigations of past conduct, the vulnerabilities that are described below may not represent the full range of current corruption risks faced by these agencies. Equally, the analysis may not take into

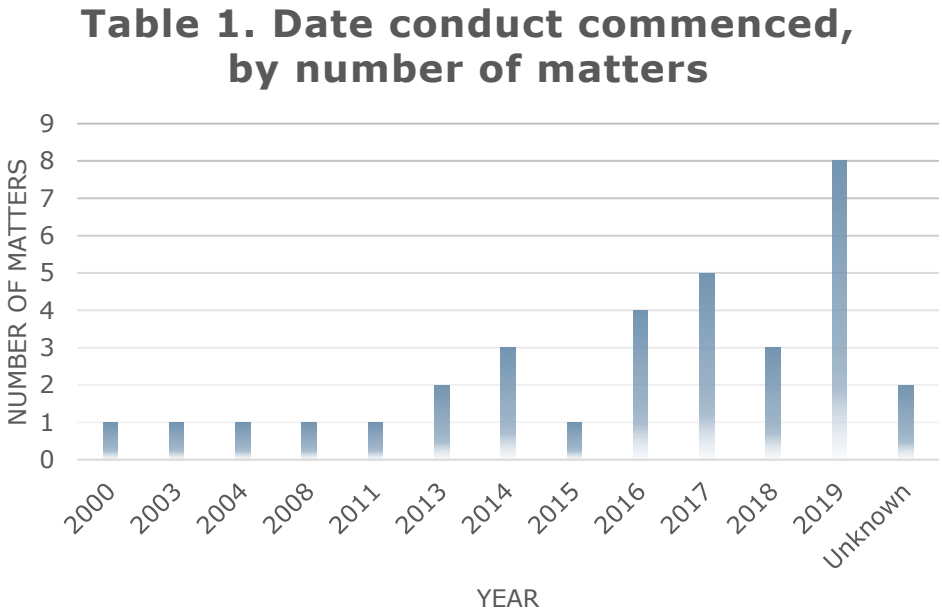
---

[1] See ACLEI investigation reports: https://www.aclei.gov.au/reports/investigation-reports.

[2] Pursuant to s.66 of the *Law Enforcement Integrity Commissioner Act 2006 (Cth)*, agencies are required to report on their investigations into corruption issues.

[3] Prosecutions in relation to Operation Fortescue and Operation Zelinsky were finalised within the same period as the corresponding ACLEI investigation reports – the information relating to these matters has only been counted once, under ACLEI investigations.

account measures that agencies have since taken to mitigate the corruption risks that these investigations identified.

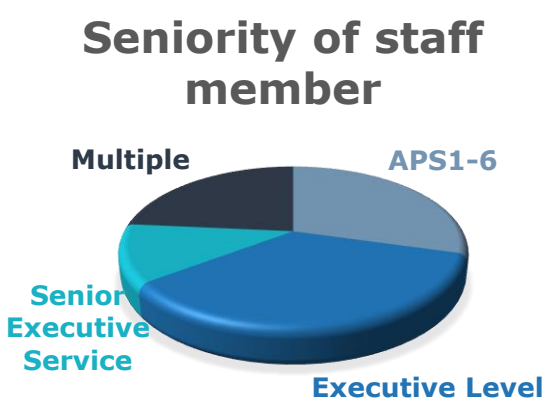


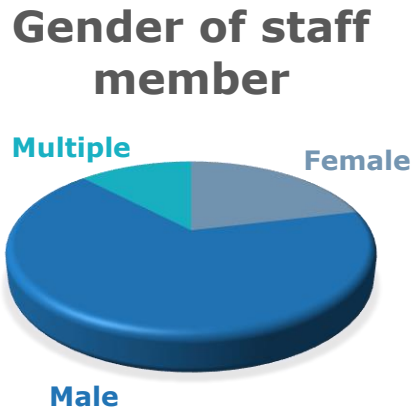
Overview

The location where the conduct took place was identified in 18 scenarios: 7 matters occurred in the ACT, 6 occurred in NSW, one in Victoria, one in Western Australia, one in Queensland and 2 in offshore locations (i.e. Australian overseas embassies or territories).

The staff member's seniority was identified in 17 scenarios:[4] 2 involved Senior Executive Service staff, 6 involved staff in managerial positions, 5 involved staff in more junior roles, and 4 involved multiple individuals.

In 7 of the 33 scenarios (21%) the staff member was female, in 22 matters (66%) the staff member was male. The remaining 4 scenarios involved multiple staff members.





[4] Equivalent seniority between agencies has been determined based on the APS Integrated Leadership System.

Misuse of information

Official information is a valuable commodity. As a result, unauthorised access to, disclosure and modification of information is a key enabler of corrupt conduct. This corruption vulnerability was the most prevalent of the matters brought to ACLEI's attention through investigations during the reporting period.

Corruption prevention observation: practices to protect sensitive information

It is important that agencies that have access to sensitive and/or valuable information have in place policies and procedures that support the operational security of that information. Such practices can include, but are not limited to, regular auditing of accesses to those systems or databases to identify any instances of access that is not for a legitimate purpose.

(Source: ACLEI Operation Zelinsky Investigation Report)

Typology 1: Unauthorised access

Of the 33 scenarios analysed, 15 (48%) involved unauthorised access to information systems. The kinds of information accessed included: personnel files, import/export information, immigration information and information pertaining to the operational activities of law enforcement agencies. In one instance, a staff member accessed records of associates out of curiosity (sometimes referred to as 'browsing'). However, in the majority of cases staff members accessed information either to pursue or advance their own interests, or to assist others.

It is a criminal offence to access or modify restricted data without authorisation.[5] The Protective Security Policy Framework (PSPF) requires all non-corporate Commonwealth entities to implement information security measures. This includes maintaining the confidentiality, integrity and availability of all official information and assets owned by the Australian Government, or those entrusted to the Australian Government by third parties or through international agreements within Australia. The PSPF 2019-20 Consolidated Maturity Report confirms that '[i]nformation security remains the most challenging outcome for agencies.'[6]

The joint ACLEI, Australian Federal Police (AFP) and Home Affairs investigation in **Operation Zeus** revealed that officers were able to obtain information which was not required for the execution of their duties and went unnoticed by fellow employees or supervisors.[7] **Operation Zelinsky** identified unauthorised accesses to systems which the staff member had no legitimate reason to access.[8]

The risk of unauthorised access is heightened in a COVID-19 context with the majority of the workforce working remotely on personal or portable devices. Access to information systems may not be able to be audited in the same way on portable devices and individuals are not subject to the usual in-person oversight that occurs in the workplace.

---

[5] Section 478.1 *Criminal Code Act 1995 (Cth)*.

[6] PSPF Whole-of-Government Maturity Report 2019-20.

[7] ACLEI Investigation Report: Operation Zeus.

[8] ACLEI Investigation Report: Operation Zelinsky.

Corruption prevention case study: Home Affairs' active detection program

In November 2020, Home Affairs notified ACLEI that it had initiated an active detection campaign focusing on unauthorised access to one of its key systems. The campaign resulted in 172 notifications of corruption issues to ACLEI in 2020–21 that were identified by Home Affairs as 'non-significant corruption issues'. The allegations related to staff members who had accessed their own record or that of a family member [on a very small number of occasions], and where there was no evidence of unauthorised disclosure of restricted information or any other inappropriate action.

(Source: ACLEI Annual Report 2019-20)

Typology 2: Unauthorised disclosure

Thirteen of the 33 scenarios analysed (39%) involved unauthorised disclosure of restricted information.

It is an offence for a Commonwealth officer (or persons performing services for or on behalf of the Commonwealth) to communicate information made or obtained by reason of their being or having been a Commonwealth officer, when they are under a duty not to disclose the information.[9] 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.[10]

Corruption prevention observation: Understanding the value of official information

It is essential that staff members understand the value of the information they have access to, and if approached by someone in their social network for favours or information, act early and report it to their agency. There is never any justification for disclosing official information to family, friends or social contacts.

(Source: ACLEI Operation Adder Investigation Report)

In 3 ACLEI investigations, staff members disclosed sensitive law enforcement information to individuals associated with organised crime. The staff members in question were prosecuted and sentenced to prison terms.[11]

In 2 of those investigations, disclosures were made in return for a financial benefit. The greatest monetary benefit a staff member obtained in return for the information disclosed was a bribe of $100,000 in **Operation Zeus**. The staff member was convicted of receiving a bribe and aiding and abetting the illicit importation of tobacco products and sentenced on appeal to a 3.5 year jail term with a 2 year non-parole period. In related civil proceedings, $1.8m of the staff member's assets were forfeited to the Commonwealth.[12] In joint ACLEI and AFP investigation **Operation Ruby**, the staff member's employment was terminated following the disclosure of sensitive information

[9] Section 122.4 of the Criminal Code.

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

[11] Operations Dreadnought, Ruby and Zeus.

[12] For more information on identifying and addressing vulnerabilities, see ACLEI Factsheet: Corruption Prevention Concepts – Unauthorised Disclosure of Information.

to a drug syndicate, they were sentenced to a 22 month prison term (suspended after 11 months) and forfeited $306,643 of their superannuation to the Commonwealth.

In another 7 cases, disclosures were made in return for 'social capital'. Motivations included assisting family or associates and community affiliates.[13] In the context of corruption, ACLEI defines social capital as the non-monetary benefit and/or improved social standing that can be gained through corrupt conduct.[14]

In 3 agency investigations, the employment of the relevant staff member was terminated following the unauthorised disclosures.

Typology 3: Modifying information

In addition to the offence of accessing or modifying restricted data without authorisation mentioned above, it is also an offence to knowingly modify any data held in a computer without authorisation and being reckless as to whether the modification impairs access to or the reliability, security or operation of the data.[15]

Staff members deliberately accessed and modified official information in three scenarios. In **Operation Zelinsky**, the staff member modified comments on a consignment to obfuscate his illegitimate instructions to release it from biosecurity inspection. One agency investigation identified a senior staff member accessing, altering and deleting comments on the performance records of a junior colleague. In another agency investigation completed during the reporting period, a staff member accessed their own personnel record on numerous occasions and modified the details to 'ensure they were correct'.

Abuse of office

Abuse of office can take several forms, but generally involves using public office and the various duties, benefits and resources that accompany that office, to dishonestly benefit oneself or another, or to dishonestly cause detriment to another. Abuse of office can occur both during and after the staff member's employment, if the former staff member uses information obtained during their employment to dishonestly obtain a benefit or cause a detriment following their departure. Many other forms of corruption can also fall under the broader category of abuse of office, for example unauthorised access to and disclosure of information, bribery, insider trading or misuse of Commonwealth resources. Some examples from the investigations under the LEIC Act are described below.

Seven ACLEI investigations and 3 prosecutions concluded with findings of abuse of office under the LEIC Act or a conviction for abuse of public office under subs 142.2(1) of the Criminal Code, constituting 30% of all scenarios analysed for this report. The 3 prosecutions resulted in convictions for abuse of office and sentences ranged from prison terms between 6 months (suspended) and 3 years, to a fine of $10,000. Seven additional agency investigations involved conduct that could amount to an abuse of office.

[13] For more information, see ACLEI Factsheet: Corruption Prevention Concepts – Social Capital.

[14] For more information, see ACLEI Glossary – Social Capital.

[15] Section 477.2 Criminal Code.

Typology 1: Misuse of position

The APS Code of Conduct provides that APS employees should not use their duties, status, power or authority to gain or seek to gain a benefit for themselves or any other person, to cause or seek to cause a detriment to their agency, the Commonwealth or any other person.

Five of the ACLEI investigations resulting in findings of abuse of office during the reporting period involved the misuse of staff members' positions to access and disclose information without authorisation.

In one agency investigation a staff member used information obtained in the course of their role as a biosecurity officer inspecting cargo, to illegally import and sell prohibited fish species for financial gain. The agency referred the matter to the AFP and the staff member was convicted of abuse of public office, possessing illegally imported specimens and dealing in the proceeds of crime and sentenced to 3 years' imprisonment. The sentence was confirmed on appeal in November 2020.[16]

Another agency investigation identified that a staff member misused their position to sign blank statutory declarations for associates who then used them to claim sick leave with their employer. The staff member also accepted benefits including complimentary access to corporate services from these associates. The agency considered that this investigation revealed broader practice issues at that particular location and undertook training and awareness measures to mitigate ongoing vulnerabilities.

An additional agency investigation found that a staff member failed to take the necessary actions to preserve and analyse evidence and prepare for a prosecution, resulting in the withdrawal of the prosecution. The agency identified that the misconduct was the result of inadequate training and poor management. This investigation illustrates the distinction between abuse of office and broader failures to uphold due care and diligence, in that the misuse of position requires an element of dishonesty and the causing of a benefit/detriment.

Typology 2: Misuse of Commonwealth property

The APS Code of Conduct requires APS employees to use Commonwealth resources in a proper manner and for a proper purpose.

Operation Swan was a joint investigation with the then Department of Agriculture, the Australian Border Force (ABF), AFP and Victoria Police and identified that a staff member had stolen a large volume of office supplies. The Integrity Commissioner determined that this constituted an abuse of office under the LEIC Act because a public officer had misappropriated public goods for private purposes.

Corruption prevention observation: Abuse of office

That employment granted the staff member access to the workplace and the goods, which were obtained with public funds for public purposes. The staff member took the goods for their private use contrary to duties owed to their employer and to the public with respect to the use of public resources.

(Source: ACLEI Operation Swan Investigation Report)

[16] AFP Media Release, Biosecurity officer sentenced after importing exotic fish (19/12/2019).

In one agency investigation, an officer used a Commonwealth vehicle for private purposes, failed to record the use of the vehicle and falsified a statutory declaration in relation to the personal use of the vehicle. Another agency investigation found that a staff member had misused Commonwealth equipment for personal purposes. In both instances, the staff member's employment was terminated following the investigation.

Typology 3: Misuse of benefits

The APS Code of Conduct states that APS employees should not provide 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. Failure to correctly record leave or fraudulently claiming personal leave can lead to undue benefits for staff members.

Corruption prevention observation: Management responsibility

Agencies should ensure appropriate supervisor vigilance and adherence to policy in areas of ostensibly 'routine' administration that may be open to corrupt exploitation. Managers can drive positive attendance by setting early, clear and realistic expectations in line with organisational culture and individual requirements.

(Source: ACLEI Operation Ajax Investigation Report)

ACLEI **Operation Ajax** resulted in the prosecution of a staff member in relation to falsifying medical certificates for the purposes of fraudulently claiming sick leave. The staff member was convicted of offences relating to the use of forged documents (ss 11.1(1) and 145.1(1) of the Criminal Code) and sentenced to a 12 month good behaviour order and 200 hours of community service and ordered to pay reparation in the sum of $4,564.12. This investigation highlighted the need to be alert to potential behavioural changes, such as repeated absenteeism, that could be indicative of underlying integrity issues.

The joint ACLEI and Home Affairs investigation in **Operation Fortescue** identified that 4 ABF officers had separately submitted and processed fraudulent Tourist Refund Scheme claims and directed refunds amounting to $139,480.56 to bank accounts held in their names or the names of their family members. All officers were prosecuted for offences of obtaining a financial benefit by deception.

One agency investigation analysed found that a staff member failed to correctly record leave.

Grooming

Four ACLEI investigations finalised during the reporting period highlighted the ongoing vulnerability of law enforcement officials to grooming. Law enforcement officials were deliberately targeted by commercial and criminal entities, as well as former colleagues, with a view to corrupting them to secure undue advantages.[17]

It is likely that grooming is also a potential corruption vulnerability in other public sector contexts where officials have access to sensitive information and insider knowledge of regulatory or other processes which is of value to commercial and criminal entities.

[17] See ACLEI Factsheet: Corruption Prevention Concepts – Grooming.

Officials can unwittingly fall victim to grooming when personal and professional relationships evolve in ways that compromise their integrity and might only realise they have been exploited after having engaged in corrupt conduct.

Typology 1: Grooming by organised crime

In **Operation Ruby**, an AFP officer was introduced by a former mentor and colleague to an associate who was an amateur boxer and involved in organised crime. The officer trained regularly with this individual who, at the same time, was grooming him to obtain access to information relating to law enforcement investigations of drug importations.

In return for the information, the trainer gifted $7,000 to the AFP officer who retained the money and did not declare it. The officer was prosecuted and sentenced to 22 months' imprisonment and forfeiture of $306,643 of his superannuation to the Commonwealth. His employment with the AFP was terminated.

In **Operation Zeus**, a former ABF officer acted as go-between for an organised crime syndicate and a (then) serving ABF officer. Both the (then) serving and the former ABF officer were groomed by the syndicate to provide them with official information and insider knowledge in furtherance of their illegal drug importation activities.

Typology 2: Grooming by commercial entities

The joint ACLEI, AFP and Department of Agriculture, Water and Environment (DAWE) investigation in **Operation Voss** identified that a staff member was befriended and groomed by a business owner over a number of years, until the officer ultimately felt a strong personal allegiance to the business owner and, as a result, disclosed a range of sensitive and commercially valuable information to him. The officer conducted lenient inspections of plants imported by the business owner and over the course of their relationship received cash, overseas travel, and part-time employment.

Corruption prevention observation: Grooming methodologies

Once officers are targeted, groomers establish trust by building relationships over time. During this period, officers may become dependent on any benefits they receive from the groomer (such as money, social capital or gifts). Groomers then begin to request the targeted officers undertake actions or provide information to them, and officers comply. Over time, groomers then capitalise on the relationship and due to the fear or threat of their complicity being exposed, officers continue to fulfil subsequent requests.

(Source: ACLEI Operation Voss Investigation Report)

Typology 3: Reach back by former colleagues

'Reach back' involves former staff members seeking out and/or using their relationships with current staff members to acquire favours, access and information.

Operation Zeus also involved reach back by a former ABF officer, to provide information and instructions to a (then) serving ABF officer so that he could perform unauthorised searches on ABF systems to identify a suitable company to facilitate an undetected importation of illicit drugs.

Operation Ruby provides another illustration of 'reach back.' In this investigation, two former colleagues exploited their relationship with the AFP officer to gain access to sensitive information for themselves or others.

Corruption prevention observation: Loyalty to former colleagues

The nature of law enforcement work can create an intense group loyalty that can extend even after staff leave law enforcement employment, allowing them inappropriate access to information or law enforcement decision-making.

(Source: ACLEI Operation Ruby Investigation Report)

Integrity in high-volume processes

Two ACLEI investigations and 4 agency investigations analysed identified corruption vulnerabilities in immigration decision-making processes and access to related information systems, representing 18% of the total number of scenarios analysed. The vulnerabilities identified in these matters may also apply to other decision-making processes, particularly high volume processes that involve discretion or where decision makers can choose to access individual cases to make decisions.

In one agency investigation, a locally-engaged staff member at an Australian overseas embassy abused their official position to grant themselves and their family member tourist visas to visit Australia. In another agency investigation, a staff member in a managerial position directed officers to disregard agency protocols regarding investigation of incoming passengers subject to alerts. Another investigation involved a staff member accessing immigration records of close associates who were unlawfully in Australia and failing to disclose the nature of their relationship.

ACLEI **Operation Angove** did not identify any corrupt conduct by serving or former ABF staff members, but did identify a number of issues with the administration of the visa support arrangement between Home Affairs and Crown and off-terminal clearances by the ABF. These issues included lack of documentation about the visa support arrangement, poor record keeping, including gaps in recorded reasons for decisions, and a lack of understanding of national policies and procedures for front line staff. Home Affairs made a range of changes to its operating frameworks to address issues observed in this investigation.

Corruption prevention observation: Good record keeping is vital

A systematic approach to good record keeping can significantly reduce vulnerability to corruption, by recording decision making and authorisations, by detailing access to information and providing evidence of any manipulation or deletion of documentation.

(Source: ACLEI Operation Angove Investigation Report)

ACLEI **Operation Swordfish** formed part of the Visa Integrity Taskforce which investigated corrupt conduct in the context of offshore immigration decision-making. An important outcome of the VITF was the dissemination of corruption prevention products, which enable the corruption issues and vulnerabilities discovered through these investigations to be learnt from and mitigated in the future.

Home Affairs also implemented a number of corruption mitigation strategies, including:

- revision of the Department's Fraud and Corruption Risk Assessment to include offshore specific controls
- updates to mandatory training to include specific fraud and corruption content
- development and implementation of an Offshore Network Security and Integrity Checklist, and
- deployment of Caseload Risk and Integrity Teams in visa processing hubs to review and analyse caseload risk indicators.

Corruption prevention observation: Oversight of offshore processes

Vulnerabilities included record keeping practices offshore, the amount of information recorded in electronic systems from offshore paper based visa applications, audit capability of some of Home Affairs' electronic systems, the ability to process applications outside of an assigned caseload and the documentation of escalated decisions.

(Source: ACLEI Operation Swordfish Investigation Report)

Employment suitability

Employment suitability refers to the policies and processes that agencies implement to assess and mitigate integrity or security risks associated with an individual prior to, during and upon termination of employment. The PSPF sets out the core requirements for employment suitability.[18]

One agency investigation analysed identified that the staff member the subject of the investigation had not undergone pre-employment screening and did not hold the relevant clearance for their role.

Typology 1: Declaring material personal interests

Commonwealth officials are subject to a general duty to disclose interests under s 29 of the *Public Governance, Performance and Accountability Act 2013 (Cth)* (PGPA Act). The APS Code of Conduct requires APS employees to take reasonable steps to avoid any conflict of interest (real or apparent) and disclose details of any material personal interest of the employee in connection with the employee's APS employment. Material personal interests could directly relate to an official's personal 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.[19]

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 of any change in personal circumstances. The purpose of this notification is to determine the employee's ongoing suitability to hold a security clearance.

[18] PSPF Policy 12: Eligibility and suitability of personnel; Policy 13: Ongoing assessment of personnel; Policy 14: Separating personnel.

[19] Sections 12-16D of the PGPA Rule.

An important element of any agency's employment suitability framework is a clear process for staff members to declare changes to financial circumstances or associations that may give rise to real, apparent or potential conflicts of interest.

In 2 separate agency investigations analysed, staff members failed to declare associations which gave rise to conflicts of interest or presented integrity risks and disclosed official information to those individuals. Another agency investigation found that a staff member had failed to declare an association with a defendant to proceedings in which the staff member had appeared as a witness for the prosecution.

Typology 2: Secondary employment

Secondary employment, including volunteer work, may create real, apparent or potential conflicts of interest with a staff member's public service employment. Integrity frameworks should include a process for employees to seek and obtain permission for secondary, or outside, employment.

Three agency investigations analysed identified that the officers in question had engaged in undeclared outside employment. In the course of another agency investigation, it came to the agency's attention that a secondary employment approval had expired and the staff member had not sought to renew it. The investigation also found that the nature of the secondary employment created a conflict of interest and as a result, the secondary employment was suspended for the staff member.