Australian Government
Australian Commission for Law Enforcement Integrity

CORRUPTION CONCEPTS: GROOMING

Grooming of public officials by corrupt actors is an ongoing integrity risk. The Australian Commission for Law Enforcement Integrity (ACLEI) has observed grooming in the course of its investigations into serious and systemic corruption. This guide describes the perpetrators, targets and methodologies of grooming identified through ACLEI investigations, and outlines strategies to prevent, detect and address grooming as a facilitator of corrupt conduct.

What is grooming?

In the context of corrupt conduct in public office, grooming is broadly defined as the deliberate targeting of public officials, and intentional manipulation by people within or outside of an agency, with a view to gain an illegitimate or illegal advantage, by:

- gaining unauthorised access to and/or disclosure of official information
- influencing official decisions for an illegitimate advantage
- obtaining preferential treatment and undermining the integrity of agency protocols
- facilitating the importation or exportation of illicit or prohibited goods
- obtaining property and goods with high resale value or that facilitate criminal activity.

Stages of grooming

Grooming tends to follow an identifiable pattern:

Stage 1: Targeting

Typically, perpetrators of grooming spend time identifying officials who are willing and able to assist them in their illicit aims. In this phase, perpetrators may or may not engage directly with their targets. If they do it may present as innocuous and therefore not raise any suspicions.

Stage 2: Relationship building

During this phase, the perpetrator takes a more overt interest in the targeted official, seeking to establish trust by building rapport over time. This may develop into a friendship or relationship outside of the work environment.

In this context, perpetrators may offer apparently unconditional gifts to the official to make them feel valued and to establish an increasing sense of loyalty or obligation towards the perpetrator. Alternatively, perpetrators may seek time alone with the official to identify opportunities to exploit and manipulate their weaknesses. In this context, perpetrators actively seek more personal information about the official, to utilise as potential blackmail in a later stage of the grooming process.

Perpetrators will ask more probing questions about the official's duties and may seek assistance consistent with what the official would expect in genuine circumstances.

Stage 3: Coercion and corrupt conduct

In this stage, the relationship is leveraged by the perpetrator to illegally:

- obtain official information
- influence official decisions and protocols for an illegitimate advantage and/or
- facilitate a crime.

Bribes may be explicitly offered or given by the perpetrators during this phase. Officials may also be blackmailed, suffer threats to their physical safety or the safety of their associates.

Perpetrators may also extort the official's continued assistance by using the personal or sensitive information they have acquired about them or by threatening to expose them. As a result, officials often find it difficult to refuse unreasonable requests from the perpetrators. Over time, officials may fear their corrupt conduct will be exposed.

Targets of grooming

All government officials are vulnerable to grooming. Perpetrators of grooming invest considerable time in understanding, manipulating, coercing, or even threatening potential targets.

Perpetrators will leverage some of the most fundamental human needs and/or circumstances, including:

- the need to feel seen, understood, valued and/or recognised
- frustration in the workplace
- financial hardship
- health or relationship concerns.

Trusted insiders are trusted employees and contractors who deliberately and wilfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises. These may be recruited or placed in a trusted role by a criminal enterprise or private entity.

All government officials should be aware that they are at an increased risk of being targeted due to their privileged access to information, decision-making powers and commodities. Common targets of grooming are individuals who are:

- Vulnerable due to their private and personal circumstances – these staff members may be more likely to trust easily and can be groomed to gain insights into their professional work.
- Responsible for decision-making in their agencies - corruptors actively seek relationships with individuals who do not require oversight of their actions or decisions as it allows for the corruption to be undetected.
- Information technology and administration staff – particularly those with privileged access to information systems who may be missed through unauthorised access detection processes or be able to obfuscate their access to information.

- Warehouse personnel, supply chain employees and companies and individuals employed at airports and seaports have access to commercially valuable goods and are likely to come in contact with public and privately-employed (including self-employed) individuals who could have a vested interest in corrupting officials.

> The border and drug law enforcement occupations—irrespective of the agency concerned—are especially prone to corrupt temptation and are working environments that are notoriously difficult to supervise. No agency with such responsibilities is immune from these risks and vulnerabilities.
>
> *(Source: ACLEI Operation Heritage Investigation Report)*

Bribery

Bribery is an all-encompassing term to cover any undue advantage offered, promised or given to an official for himself or herself or for a third party in order that an official act or refrain from acting in the exercise of his or her duties. Bribery in the context of grooming is wide-ranging and is not limited to monetary benefits. It can include, for example:

- favours or non-financial assistance
- emotional / familial support
- secondary employment
- promotion
- holidays, expensive jewellery or alcohol
- social benefits or increased status.

Government officials should never expect to receive additional benefits for doing what they are paid to do. The acceptance of gifts, benefits or hospitality can result in an actual, potential or perceived conflict of interest that can undermine the legitimacy of an official's actions and their impartiality.

For this reason, the acceptance and declaration of gifts and benefits must be considered in the context of the Australian Public Service (APS) Values and Employment Principles and be consistent with the APS Code of Conduct and any agency-specific guidance.

Gifts are not always offered in a transactional manner, or explicitly in connection with the illegal assistance being provided by the official. In some circumstances, they may appear to the official as being given only in the context of what they believe is a genuine and meaningful relationship with the perpetrator.

In the following case study, the official felt a strong personal obligation to the business owner who groomed him and with whom he had built (what he believed) was a genuine friendship over many years.

Case study: Operation Voss

Operation Voss was a joint ACLEI and Australian Federal Police (AFP) investigation into an allegation that an employee of the Department of Agriculture, Fisheries and Forestry (former Department of Agriculture, Water and Environment (DAWE)) was assisting the owners of a business to import plants into Australia and bypass biosecurity controls.

During the course of the investigation, it was identified that the official was groomed and apparently befriended by the business owners over many years, until they ultimately felt a strong personal allegiance to the business owners. As a result, the official disclosed a range of sensitive and commercially valuable information and conducted lenient inspections of plants imported by the business owners.

It was only when interviewed by investigators, that the official began to recognise that the benefits they had been given by the business owner (including emotional support, cash, overseas travel, and part-time employment) were likely to have been given in order to illicit their subsequent assistance and corrupt conduct.

Perpetrators of grooming

Organised crime groups (OCGs)

Organised criminal activities range from small groups of individuals cooperating to conduct low-level property crime, through to larger, more

sophisticated criminal networks involved in cybercrime, intellectual property infringement and financial crime.

The most serious activities include large-scale OCGs engaging in the distribution of illicit drugs and drug-fuelled volume crime, money laundering, cybercrime and child sexual exploitation.

OCGs display a capacity to expand into new illicit markets and infiltrate legitimate industries, and are structured to operate across borders. Although outlaw motorcycle gangs (OMCGs) attract significant attention, OCGs vary greatly in size and structure and can include networks based on family ties, social links, ethnicity, language or shared criminal purpose.

The cultivation of public servants represents an attractive avenue by which OCGs can access information, systems, decision-making processes or commodities held by public bodies. An official who can be compelled or persuaded to cooperate with a criminal group offers the group ongoing access while employing inside knowledge of the public bodies' systems to avoid detection. Obtaining information and access from insiders is an efficient and cost-effective means of facilitating major criminal enterprises.

Case studies: Operation Ruby and Operation Zeus

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

In Ruby, a (then) serving AFP officer was introduced by his former colleague to an amateur boxer involved in organised crime. The officer trained regularly with this individual, who was grooming him to obtain access to information relating to law enforcement investigations of drug importations.

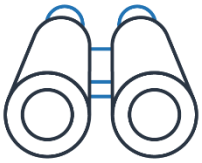
In return for the information, the trainer gifted $7,000 to the officer, who kept the money and did not declare it. The officer was prosecuted and sentenced to 22 months' imprisonment and forfeited $306,643 of his superannuation to the Commonwealth. His employment with the AFP was terminated.

Extremist groups

Extremist groups can target public officials and actively seek to forge relationships with like-minded 'insiders' in the public service. Individuals employed by law enforcement agencies who hold ties, strong political, religious or otherwise 'extremist' ideologies may sympathise with criminal sentiments reflected by similar groups.

Both known and unknown links to extremist groups pose a significant risk for law enforcement and other government agencies, with an increased possibility for sensitive information being disclosed to criminal entities.

Foreign intelligence services



Espionage refers to the theft of Australian information by someone either acting on behalf of a foreign power, or intending to provide information to a foreign power which is seeking advantage.

Individuals employed by government agencies have access to sensitive information as part of their official duties, and are at increased risk of being targeted and groomed by foreign actors to provide this information for clandestine activities. Employees having suspicious, unusual and frequent communication with foreign entities pose an inherent risk of espionage to organisations that deal with sensitive government information.

Commercial entities

Operation Voss illustrates that perpetrators of grooming are not limited to organised criminals. They can include individuals seeking to advance their own personal or professional interests and who might not initially raise the suspicions of government officials.

All of the agencies in ACLEI's jurisdiction officially engage with commercial entities as part of their function - for example, in a regulatory or procurement capacity. Professional relationships can morph into friendships that can be leveraged in exchange for preferential treatment or to obtain official information that provides a commercial advantage.

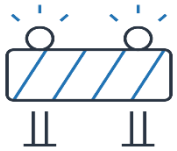
Existing Colleagues

Strong group loyalties have been observed in the law enforcement context, arising from the expectations of the role – unsociable hours and shift work, occupational hazards and violence, high officer discretion and isolation from the general public. It is likely similar group cultures could arise in other public sector contexts.

The early years of employment are a particularly vulnerable time, as a new officer is learning the realities of 'how we do things', which can be markedly different to what they were taught in a training environment.

This can create a culture of favours or 'debt' repayment, which can be maintained even in the face of corruption by colleagues and at the expense of the expectations of the agency.

Reach-back



'Reach-back' refers to former staff members or known professional connections seeking out and/or using their relationships with current staff members to acquire favours, access and information.

Operation Zeus 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 involved reach-back by two former colleagues exploiting their relationship with a former AFP officer to gain access to sensitive information.

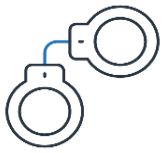
> The nature of law enforcement work can create an intense group loyalty that can extend even after staff leave law enforcement employment, allowing them inappropriate access to information or law enforcement decision-making.
>
> (Source: *ACLEI Operation Ruby Investigation Report*)

Reach-back is also a risk for agencies with regulatory powers. It is common for former officials of these agencies to subsequently gain employment with

the entities they previously regulated. In this context, officials need to be mindful of the relationships they maintain with former colleagues and the risk that professional and personal boundaries will be blurred. These relationships are likely to present a declarable conflict of interest that requires ongoing management.

Grooming vulnerabilities

Private investigations



The relationship between former law enforcement officers and the private investigations industry creates a potential vulnerability that sensitive information may be improperly disclosed to private investigators. This risk is also heightened where Australian law enforcement agencies enforce a mandatory retirement age (for example, the Queensland Police Service enforces a mandatory retirement age of 60) and experienced officers may elect to continue their careers in the private investigations industry.

Long-term relationships, particularly those based on bonds of family, friendship or culture enable organised crime groups to shift employees' loyalties away from their employer.

> A law enforcement employee's professional relationships may evolve in ways that compromise the integrity of a workplace and facilitate inappropriate and illegal behaviour. Officers can obtain information which is not in accordance with the execution of their duties and without being noticed by fellow employees or supervisors.
>
> *(Source: ACLEI Operation Zeus Investigation Report, 2020)*

Former law enforcement officers working in the private investigations industry may use their personal networks and relationships to reach-back into their former colleagues, who may feel pressured to provide information due to misplaced loyalty, or the repayment of a debt or favour.

Security industry

Criminal groups have been known to infiltrate the security industry to commit a variety of crimes that have been deemed as high profit, at a low risk - including money laundering, fraud, extortion, illicit drug and firearm supply. Security consultancy and businesses supplying security contractors are also popular as post-law enforcement employment.

Former law enforcement officers may seek to access training materials and/or law enforcement methodology, or approach trusted former colleagues to undertake secondary employment. Law enforcement agencies generally do not support secondary employment for their officers in regulated industries, because of the conflict it creates with their primary employment and the risk of contact with individuals who may seek to gain access to law enforcement information.

Criminal compromise

Relationships with individuals associated with or involved in organised crime have the potential to compromise law enforcement integrity and support criminal activity through the unauthorised access, modification and/or disclosure of classified information.

Grooming by criminal entities can be enabled by junior or inexperienced officers with a lack of proper training. This risk can be further amplified if comprehensive and ongoing background checks, thorough supervision and robust auditing practices are not appropriately adopted by law enforcement agencies.

Selective dissemination of information to criminal groups is often characterised as a primary behaviour of corrupt conduct. The realisation of this risk could potentially mean that handlers do not have the capability to manage experienced criminals as informants — instead they may become managed and manipulated by the criminals. To reduce corruption vulnerability, human source handling should be managed with adequate safeguards, such as intrusive oversight and a requirement for all sources to be formally registered with law enforcement.

Criminal entities will look for access to law enforcement through intimate relationships, family connections, or cultural and social links. Existing

relationships with criminal actors may represent a significant corruption vulnerability. Organised crime will attempt to compromise a law enforcement employee's loyalty to their employer by exploiting their relationship and creating a conflict of interest. While officers may not always be aware that their associates are involved in organised crime, failure to declare a known association will ultimately increase the likelihood of misconduct and corruption risk to an agency.

Supply chain vulnerabilities

Individuals employed in international supply chains are particularly vulnerable to grooming. A wide range of official duties at Australia's border can be exploited to facilitate illicit or expedite legitimate imports and exports.

These may include customs brokers, freight forwarders, truck drivers, stevedores, provedores, contracted workers (security, cleaning, unpackers etc.), depot and warehouse employees, caterers, baggage handlers, airline and shipping crews.

These individuals work closely with government officers at the border and have access to commercially valuable goods and information. The integrated working environment of the supply chain subsequently increases the risk of grooming.

Use of illicit substances and misuse of prescription medication

Risk-taking behaviour by government officials can expose them to compromise. While not corrupt conduct in itself, the use of illicit substances creates a fundamental conflict with an official's duty to behave lawfully or uphold the law. Access to illicit substances necessarily involves contact with those supplying drugs and potentially organised networks of crime, creating opportunities for compromise and coercion.

The growth in fitness culture and bodybuilding has fuelled a significant increase in the supply and use of performance and image enhancing drugs (PIEDs). Investigations by Australian integrity and law enforcement agencies have identified multiple cases where the corruption of public officials by organised crime groups has been linked to gymnasiums, PIEDs and body image.

Illicit drug use and the misuse of prescription medications by public sector employees make those employees attractive targets for organised crime group cultivation because it:

- is illegal behaviour that makes the user vulnerable to blackmail and extortion
- is potentially addictive behaviour that can leave the user susceptible to manipulation
- demonstrates an adherence to values at odds with expected public sector standards
- shows an appetite for personal risk-taking, which may be an indication that an individual is susceptible to other high-risk behaviours, including engaging in corrupt conduct
- shows naïve or dismissive attitudes towards the corruption risks inherent in associations with criminal elements including those who supply recreational drugs or PIEDs.

Case study: Operation Heritage

Operation Heritage investigated several former Australian Border Force (formerly Australian Customs and Border Protection) officers who were actively involved in the importation into Australia of border-controlled substances, including the precursor drug pseudoephedrine. They abused their positions to arrange and effect the importations, and to attempt to frustrate detection of their activities. They gave and received bribes to achieve their objectives.

The investigation resulted in prosecutions of eight former Commonwealth officials and resulted in seven convictions and one prosecution where the charge was proven and the defendant discharged without conviction. The sentences imposed ranged from release without passing sentence to imprisonment for a period of 14 years.

Social Media

Information shared through social media platforms can provide a large amount of personal, sensitive information. ASIO has highlighted the risk of social media being leveraged for the purposes of espionage and encourages officials to be discreet about their access to sensitive information, to be responsible and to report suspicious activity.

Further Reading

For more information on preventing grooming in your workplace, take a look at the following:

- Grooming Prevention: Officials
- Grooming Prevention: Managers and SES
- Grooming Prevention: Integrity Teams
- Corruption Conversations Starters: Grooming
- Corruption Concepts: Grooming (Op Voss video)
- Corruption Case Studies: Operation Voss

References

ACIC (Australian Criminal Intelligence Commission) (2017) *Organised Crime in Australia 2017* , ACIC, Australian Government, accessed 16 June 2022.

ANAO (Australian National Audit Office) (2018) *ANAO Report No.38. Performance Audit: Mitigating Insider Threats through Personnel Security Across Entities*, ANAO, Australian Government, accessed 16 June 2022.

APSC (Australian Public Service Commission) (2021) *Guidance for Agency Heads – Gifts and Benefits,* APSC, Australian Government, accessed 16 June 2022.

ASIO (Australian Security Intelligence Organisation) (2021) *Counter Espionage and Foreign Interference*, ASIO, Australian Government, accessed 16 June 2022.

ASIO (Australian Security Intelligence Organisation) (n.d.) 'Think Before You Link', ASIO, Australian Government, accessed 16 June 2022.

Australian Government (2018) *National Strategy to Fight Transnational, Serious and Organised Crime*, Australian Government, accessed 16 June 2022.

Coady T and James S (2013) *Violence and Police Culture*, Melbourne University Publishing, Melbourne.

Crous C (2009) 'Human intelligence sources: Challenges in policy development.' *Security Challenges*, 5(3):117-127, http://www.jstor.org/stable/26460096

David C (2008) *Conflict of interest in policing: problems, practices and principles*, Institute of Criminology Press, Sydney.

Department of Home Affairs (2022) *Countering foreign interference*, Department of Home Affairs, Australian Government, accessed 16 June 2022.

Europol (European Union Agency for Law Enforcement Cooperation) (2021) *Europol Spotlight - The use of violence by organised crime groups*, Europol, EU Justice and Home Affairs Council, accessed 16 June 2022.

Hope Sr KR (2016) 'Training to curb police corruption in developing countries: A suggested framework.' *International Journal of Police Science and Management*, 19(1):3-10, doi.org/10.1177/1461355716674371.

IBAC (Independent Broad-based Anti-corruption Commission) (2015) *Organised crime group cultivation of public sector employees*, IBAC, Parliament of Victoria, accessed 16 June 2022.

ICAC (Independent Commission Against Corruption) (2019) *Gifts and benefits*, ICAC, Government of New South Wales, accessed 16 June 2022.

McCafferty F, Souryal, S, McCafferty, M (1998) 'The corruption process of a law enforcement officer: A paradigm of occupational stress and deviancy.' *Journal of the American Academy of Psychiatry and the Law*, 26(3):433 – 458, https://pubmed.ncbi.nlm.nih.gov/9785287/

NSW Police Integrity Commission (1997) *Operation Saigon: Royal Commission into the NSW Police Service, Final Report Volume II: Reform*, NSW Police Integrity Commission, Government of New South Wales, accessed 16 June 2022.

Prenzler, T (1997) 'Is there a police culture?' *Australian Journal of Public Administration* 56(4):47-56, doi.org/10.1111/j.1467-8500.1997.tb02488.x.

Prenzler, T and Milroy, A (2012). *Recent inquiries into the private security industry in Australia: Implications for regulation.* *Security Journal* 25(4):1-16, doi.org/10.1057/sj.2012.2.

Rowe, E, Akman, T, Smith, R, Tomison, A (2013) *Organised crime and public sector corruption: A crime scripts analysis of tactical displacement risks.* Australian Institute of Criminology, ACIC, Australian Government, accessed 16 June 2022.

Strategic Centre for Organised Crime Office for Security and Counter-Terrorism (2015) *Individuals at risk of being drawn into Serious and Organised Crime*, Home Office, Government of the United Kingdom, accessed 16 June 2022.

U4 Anti-Corruption Resource Centre (2010) U4 Helpdesk Answer: Anticorruption and police reform, Chr. Michelsen Institute, accessed 16 June 2022.

United Nations Office on Drugs and Crime (2004) United Nations Convention Against Corruption, United Nations Office on Drugs and Crime, accessed 16 June 2022.

White V and Robinson S (2014) 'Leading change in policing: Police culture and the psychological contract', *The Police Journal*, 87(4):258 – 269, doi.org/10.1350/pojo.2014.87.4.675.

Workman-Stark, A L (2017) *Inclusive policing from the inside out*, Springer.