Organised crime group cultivation of public sector employees

Intelligence report 1

September 2015
Organised crime groups are grooming Victorian public sector employees to access information, influence decisions and manipulate systems.

This issue has been identified across public bodies ranging from law enforcement agencies to departments to councils. Some agencies with access to sensitive information are not aware of the risks presented by organised criminal groups and lack basic protections against organised crime cultivation.

This assessment aims to increase awareness of this issue across the Victorian public sector. It also seeks to highlight mitigation strategies that could be adopted by public bodies, while noting that these strategies will vary between bodies based on associated risks.

Most public sector bodies hold information or commodities that are attractive to organised crime groups. However, the bodies most likely to be targeted are those with access to law enforcement information or large volumes of identity and credit card information. Some public sector regulatory bodies – such as those overseeing the construction, planning, development, prostitution, gaming and liquor industries – may also face increased risks.

The full extent to which organised crime groups target Victorian public sector bodies remains unknown. The lack of awareness of the threat posed by organised crime groups and the lack of prevention and detection measures in place across the public sector mean that it is likely that most organised crime cultivation activities against public sector employees go undetected.
2 Introduction

2.1 Background

Organised crime groups are targeting Victorian public sector employees to gain access to information, systems or commodities. Crime groups are attempting to facilitate this access by cultivating relationships with public sector employees.

From consulting across the public sector, IBAC identified that many public sector bodies were unaware of this threat. These bodies did not address the risks posed by organised crime in their organisational risk assessments and often lacked appropriate prevention and detection measures tailored to this threat.

This assessment seeks to increase awareness of this issue across the Victorian public sector. In doing so, it highlights:

• background on the nature of organised crime activities in Victoria
• likely targets of organised crime cultivation attempts
• strategies used by organised crime groups to cultivate relationships with public sector employees
• prevention, mitigation and detection strategies that can assist in addressing the threat.

This assessment highlights that public bodies need to consider the threats presented by organised crime groups when undertaking their risk assessments. Where appropriate, public bodies should introduce proactive prevention, mitigation and detection strategies addressing the identified risks.

2.2 Definitions

Within this assessment, the following definitions are used:

**Organised crime** means activities involving two or more offenders and a serious offence where there is:

• substantial planning and organisation
• systemic and continuing criminal activity
• a purpose of obtaining profit, gain, power or influence or of sexual gratification where the victim is a child or
• where two or more of the offenders involved in the offence are, at any time, either declared individuals or declared organisation members.¹

**Public sector employee** means all Victorian state and local council employees, contractors and consultants.

2.3 Methodology

This assessment draws upon IBAC complaint data and investigations, consultations with a range of Victorian, interstate and Commonwealth agencies, and open source research.
3 Organised crime groups

3.1 Overview

Organised crime operates on a continuum of seriousness and complexity of activity. The lower end includes small-scale crime committed by small groups of individuals such as low-level property crime. More sophisticated criminal networks are involved in cybercrime, intellectual property infringement and financial crime. The most serious activities include large-scale organised criminal groups engaged in corporate fraud and trafficking and distributing illicit drugs.

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

3.2 The Victorian organised crime environment

Organised crime groups operating in Victoria are constantly evolving in response to targeting by law enforcement agencies. As authorities close loopholes and improve targeting, crime groups adapt and develop alternative ways of operating. Improved targeting by law enforcement is one of the most significant drivers of organised crime efforts to develop new ways to access commodities, identify criminal opportunities and avoid detection. One way in which organised crime groups can achieve these ends is by targeting public servants and using them to access information, systems, decision making processes or commodities.

The extent of organised crime involvement in public sector corruption in Victoria (and across Australia) is not well understood. This is because of the difficulties in identifying corrupt conduct, a lack of awareness around the issue, increasingly sophisticated behaviour by organised crime groups, and because corruption allows groups to anticipate and avoid detection efforts.

3.3 Why organised crime groups target public bodies

Organised crime groups target public bodies to access:

- sensitive information or systems
- decision-making processes
- property and goods with high resale value or that facilitate criminal activity.

The cultivation of public servants represents an attractive avenue by which organised crime can access information, systems, decision-making processes or commodities held by public bodies. When a public servant can be persuaded to cooperate with a criminal group, they offer 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 study – IBAC Operation Toucan: alleged supply of information to outlaw motorcycle gang members

Early in 2013, IBAC received information that several Victorian public sector employees, working at different statutory bodies based in Shepparton, were providing confidential information to members of an OMCG. While IBAC was unable to establish direct evidence of employees passing information to OMCG members, IBAC was able to establish one employee’s:

- proven links to one or more OMCG members
- proven unauthorised or otherwise inappropriate access to some agency-held information
- failure to disclose declarable associations
- suspicious conduct regarding other issues in connection with the person’s employment.

It remains possible that a detailed newspaper article about a connected police investigation may have compromised IBAC’s investigation, by putting persons of interest to IBAC on alert.
3.4 Consequences of organised crime cultivation

When organised criminal groups cultivate public sector employees to access information, decision-making processes or commodities, there are consequences for the individual, their public body and society more broadly.

For the employee these consequences can include:
- embarrassment
- physical harm
- threats to themselves, family, and friends
- loss of employment
- penalties associated with criminal activity.

For the agency, harms can include:
- reputational damage
- financial loss
- loss of intellectual property
- breaches of physical security around buildings and infrastructure
- intimidation, violence and threats to employees
- legal consequences associated with criminal investigations.

Broader societal harms can include:
- threats to the physical safety of community members
- increased uncertainty about the reliability of personal information
- loss of services or provision of inadequate services from public sector bodies
- unfair tendering conditions for public sector contracts
- loss of confidence in public organisations.

Where agencies lack prevention and detection measures to address the threats presented by organised crime, significant damage can be done over a long period of time.

4 Targets of organised crime groups

4.1 Information targeted by organised crime

Public servants can have access to information critical to the commission of serious crimes. This information assists organised crime groups to identify criminal opportunities, facilitate criminal activity, undermine competitors or avoid detection. Identity information is particularly valuable, as it facilitates identity fraud, debt collection, witness intimidation, extortion, or can be sold to other criminal groups.

The most vulnerable agencies will be those with significant data holdings, particularly those that have access to law enforcement information or large volumes of identity and credit card information. An increasing number of public sector bodies, large and small, collect identity information and could potentially be targeted. Data systems that can be accessed by a large number of employees are particularly attractive to organised crime groups as there are more potential cultivation targets through which to seek access to a system.

Risk assessments undertaken by these public bodies should demonstrate an awareness of the threat posed by organised crime and, where appropriate, respond with proportionate prevention and detection measures.

4.2 Decision-making processes targeted by organised crime

Decision-making and regulatory processes undertaken by Victorian public servants could be targeted by organised crime groups. In particular, investigations in Victoria and other jurisdictions have shown the security, construction, prostitution, gaming and liquor industries present attractive opportunities for organised crime groups to generate income or to launder the proceeds of crime. Regulators overseeing these industries are attractive targets for organised crime groups seeking to increase their profits or avoid detection. Despite this, some regulatory bodies are unaware of the threat posed by organised crime groups and do not identify that they could be targeted.
4.3 Work areas likely to be targeted

It is not only sensitive operational areas within public sector bodies that are likely to be targeted. Although integrity measures have traditionally focused on ‘front-line’ operational staff, support officers in administrative and information technology areas may also access sensitive information or conceal improper actions.

In determining which work areas face the highest risk of organised crime cultivation, public bodies should consider for each work area:

- the information, decision-making powers and commodities that are accessible
- vulnerabilities associated with the employees within that work area (such as likelihood to come into contact with organised crime group members)
- work and security practices.

Poor protective security and management processes have been consistently identified in cases where government insiders have worked with organised criminal groups. Factors that have been associated with exploited work areas include:

- poor security culture
- poor proactive use of auditing functions
- lack of adequate, role-based, personnel security risk assessments
- poor pre-employment screening
- poor communication between business areas
- lack of awareness of people risk at a senior level
- inadequate corporate governance
- general workplace dysfunction.

In addition to these internal factors, public bodies must also consider how they share their information and systems. Although a public body may have identified internal high-risk work areas, they may remain vulnerable where information and systems are shared with other bodies or where functions are outsourced to private providers.

4.4 Vulnerable individuals

It is difficult to profile those public sector employees who will be the most vulnerable to cultivation by organised crime groups. However, certain personal and environmental characteristics are more commonly associated with those who are targeted by criminal groups.

The presence of one or all of these indicators does not necessarily mean an individual will be vulnerable to an approach by organised crime – however they are the most common risk indicators of which supervisors, security managers and human resources personnel should be aware.

Case study – Prison officer cultivated by inmates at Port Phillip Prison

A prison officer who was targeted by imprisoned organised crime figures subsequently smuggled mobile phones, takeaway food and other items into Port Phillip Prison. A Victoria Police investigation identified that the officer was paid cash to smuggle the prohibited materials into the prison and was promised further inducements that did not eventuate.

It was assessed that a combination of personal and environmental factors contributed to making the officer vulnerable to cultivation. These included greed, emotional instability, a lack of confidence in social situations and upheaval caused by health and relationship issues.
Personality factors are those innate characteristics relating to how an individual responds to situations and interacts with others. The factors most commonly associated with a public sector employee’s susceptibility to organised crime cultivation include:

- immaturity (including a lack of life experience and naiveté)
- low self-esteem (extremely dependent on recognition, struggles to cope with adversity)
- amorality and unethical behaviour (lacks moral values or personal integrity, shows no remorse)
- prone to fantasising (believes they are engaged in activities that have no basis in reality)
- impulsiveness (seeks instant gratification and does whatever feels good in the moment)
- lacking conscientiousness (ignores rules, duties and obligations, shows a lack of focus)
- manipulativeness (uses others to serve their own self-interest).

Environmental factors include negative life events or lifestyle factors that increase individuals’ vulnerabilities. These can include serious financial, alcohol, gambling or drug problems, loss of status at work, significant personal injury, death of a family member or close friend, relationship break-ups or loneliness.

5 Organised crime cultivation strategies

5.1 Pre-existing relationships

Organised crime groups will exploit family relationships, intimate partnerships, pre-existing friendships and cultural links to gain access to public bodies’ information and systems. Such group loyalties and social bonds can be enduring and powerful motivations for corruption.

Pre-existing relationships present a particularly powerful opportunity for crime groups in regional areas. The greater levels of social connectivity that exist in smaller regional areas increase the likelihood of organised crime group members knowing public body employees.

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

Case study – Australian Customs Service officers at Sydney International Airport

An investigation into drug trafficking at Sydney International Airport highlighted how long-term friendships can lead to corruption. The joint investigation by the Australian Commission for Law Enforcement Integrity, Customs and Border Protection, and the Australian Federal Police identified a network of airport workers including Australian Customs Service employees and baggage handlers who shared common links, including school and community ties. These same links extended to friends who were active members in organised crime groups, including outlaw motorcycle gangs.

These shared backgrounds led to the airport workers becoming involved in the drug trafficking activities of their organised crime associates. The strength of the bonds between group members also allowed the corrupt group to expand with a level of confidence and provided additional protection against detection by authorities.
Within such a relationship, a corrupt official can justify their actions by arguing that ‘helping a friend’ is the ‘right’ thing to do, even where it involves a betrayal of the public trust. On this basis, organised crime groups have sought to target not only those public sector employees who can provide immediate assistance but also those who may be of use in the future.

5.2 Social media

Social media provides an additional environment in which organised criminals can engage with public sector employees. However unlike traditional ‘real world’ forums, social media allows crime groups to search for employment details, personal interests and characteristics that could allow the identification of personal vulnerabilities. Criminals use these details to initiate contact, which at first may appear to be innocent, but which may escalate as the target’s potential criminal use is assessed.

Social media allows large numbers of public sector employees to be identified. Some applications, such as LinkedIn, may also identify work units and position responsibilities. When combined with information from other social media platforms, it may be possible to identify a target’s name, date of birth, photographs, details of their friends and families, personal interests, where they spend their spare time, gambling behaviour, relationship status and emotional vulnerabilities.14

Organised crime groups across Australia are already using social media platforms in innovative ways such as to recruit individuals to serve as couriers for illicit drugs and precursor chemicals.15 It is highly likely that Victorian crime groups will increasingly use social media to identify public sector employees and to cultivate relationships that facilitate corruption.

5.3 Interest in tattoos, fitness culture, bodybuilding and martial arts

Evolving interests associated with organised crime group members and the broader community have created new areas where criminals and public sector employees regularly interact. The demography of OMCGs has shifted toward younger individuals who are more likely to be involved in fitness culture, bodybuilding and mixed martial arts. This coincides with broader community engagement in these activities and greater community participation in tattoo culture – an area where OMCGs have maintained a long-standing presence.

These environments provide an opportunity for organised criminals and public sector employees to develop incidental associations. They also present opportunities for organised crime groups to actively screen members of the public for capabilities that could assist their criminal activities.

5.4 Illicit drug use and the misuse of prescription medication

Risk-taking behaviour among some public sector employees exposes them to compromise. Long-term drug use surveys indicate that illicit drug use and the misuse of prescription medications have become more common across the community over recent decades.

One area of significant change has been the supply and use of performance and image enhancing drugs (PIEDs) which has increased significantly over the past five years.16 This has been fuelled by the growth in interest in fitness culture and bodybuilding. 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.17
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
- it is potentially addictive behaviour that can leave the user susceptible to manipulation
- it demonstrates an adherence to values at odds with expected public sector standards
- it 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\textsuperscript{18}
- it 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 – Victoria Police detective exchanging police information for testosterone**

In May 2012, following an internal investigation, a Victoria Police detective was sentenced to a suspended jail sentence and fined $10,500 after pleading guilty to disclosing Victoria Police information and possessing testosterone. The detective had a strong interest in body building and developed a relationship with a body builder who had a criminal history and links to OMCGs.

The detective began to illegally source testosterone — a prescription-only drug sold widely on the black market in gymnasiums and body building circles — from the bodybuilder. In response, the bodybuilder requested the detective source confidential police information. The detective subsequently accessed police databases and on several occasions passed on sensitive classified information about police investigations and other criminal entities.\textsuperscript{19}

## 6 Prevention and detection strategies

Some Victorian public bodies are not aware of the threats posed by organised crime groups. Limited understanding of the threat means that instances of organised crime cultivation are more likely to result in widespread and long-term damage to the public sector. This lack of awareness is reflected in the lack of prevention and detection measures in place to mitigate this threat.

Prevention and detection measures must be proportionate to the threat faced by different public sector bodies. Bodies facing the highest risk include those with access to law enforcement information, large volumes of identity information or credit card details, along with those regulatory bodies overseeing industries attractive to organised crime. Public bodies must examine how vulnerable their employees are to organised crime cultivation and consider the costs and benefits of the prevention and detection measures that can mitigate the threat.

### 6.1 Security culture within public sector agencies

The most effective protection against criminal cultivation attempts is a robust security culture.\textsuperscript{20} When employees and management understand the threat, have received appropriate training and are kept up to date on emerging security issues, they are better equipped to detect and repel approaches from organised crime and to identify warning signs in others’ behaviour. Promoting professional and corruption-resistant cultures within agencies helps address the threat from organised crime and encourages resistance to a range of corruption vulnerabilities.
6.2 Risk assessments and mitigations

The risks associated with organised crime groups should be addressed in organisational risk assessments. When framing their risk assessments, public bodies might consider:

• Current security environment: Are there frequent and serious security incidents? Are there good levels of detection or self-reporting? How are incidents dealt with?

• High-value information and systems: What information or systems controlled by a public body would be valuable to an organised crime group? Who has access?

• Precedence: Has a public body or similar bodies been targeted by organised crime?

The areas of greatest risk will be different across different bodies, meaning there is not a uniform set of mitigation strategies that should be applied to all public bodies. Furthermore, organisational risk assessments should acknowledge that some work areas or positions are at higher risk and should be subject to additional security measures.

6.3 Vetting and revalidation of employees

Screening employees for security risks serves as a risk mitigation strategy against organised crime cultivation. Vetting involves a series of checks to ensure individuals entrusted with access to information or resources are suitable and can be relied upon to safeguard them. Vetting employees when they are recruited serves as a protective layer that can discourage organised crime groups. It can identify employees with risk factors that might make them vulnerable to targeting by crime groups in the future, providing public bodies with an opportunity to put risk mitigation strategies in place.

Levels of vetting will vary depending on the risks associated with different public bodies. Even within a public body, different vetting standards may be applied to address the range of risks presented by different work areas or positions.

For those in low-risk positions, appropriate vetting practices might include checking police records and referees.

As risks increase, additional vetting enquiries may be applied, including checks of employment histories, finances, relationships, and use of alcohol and illicit drugs. Public bodies could consult the Australian Government personnel security guidelines—Vetting practices when designing vetting measures tailored to the risks they face.

Inconsistent vetting standards across the Victorian public sector create vulnerabilities that can be targeted by organised crime groups. Victorian public bodies with access to similarly valuable assets, information and systems can have different approaches to recruitment checks and revalidation. Inconsistent standards are also applied to contractors or external bodies that have access to public sector information and systems.

The introduction of the Victorian Protective Data Security Framework (VPDSF) seeks to address these inconsistencies by making certain security standards mandatory across the public service. The Commissioner for Privacy and Data Protection is working with public sector bodies to encourage consistent application of the VPDSF’s personnel security standards.

Although pre-employment screening is important, it will not identify all individuals who present a security risk. Vulnerabilities such as personality factors, lifestyle changes or workplace behaviours are not always observable at recruitment or may arise following recruitment. Revalidation of employees’ clearances at regular or random intervals during their employment ensures that public bodies can respond to changes in employees’ risk factors.

Revalidation is particularly important as organised crime groups appear more likely to target existing employees rather than to infiltrate agencies by putting forward a member and associate for recruitment. A system of revalidation also acknowledges that employees’ access and influence within a public body will generally increase the longer they have been employed, increasing their potential value to organised crime groups. Long-term employees may also develop risk factors such as disenchantment with their employer or a desire for revenge. Robust and ongoing security screening assists in identifying and reducing these vulnerabilities.
6.4 Auditing

One of the most effective means of identifying incidents of organised crime cultivation of public sector employees is proactive and random auditing of information and financial systems. Routine auditing can identify where there has been inappropriate access, use or sharing of information, systems or property.

Many Victorian public sector bodies have auditable systems housing sensitive data. However, proactive auditing of these systems is generally not routinely undertaken. Instead, the auditing function is most commonly utilised after an incident has been identified as part of the investigative process. Auditing is used to determine the extent of a particular data breach, rather than to proactively identify data breaches or suspicious activity.

Case study – Victoria Police’s Taskforce Keel

Victoria Police’s Taskforce Keel examined the activities of a senior constable at a suburban station who accessed and printed sensitive information and shared it with individuals engaged in the trafficking of illicit drugs. The senior constable used colleagues’ passwords to access classified information systems and traded this information in exchange for illicit drugs. Although auditing of Victoria Police’s systems assisted in the investigation of the senior constable, proactive auditing may have led to earlier detection of the unauthorised activities.

6.5 Declarable associations

Personal relationships between public sector employees and criminal entities have long been identified as a cultivation risk. These relationships have the potential to facilitate the inappropriate release of information, compromise law enforcement activities or facilitate organised criminal activity. Such associations could be perceived as influencing public sector employees’ capacity to perform their role.

It is inevitable that associations will occur between public sector employees and individuals engaged in criminal activities. These associations might arise through family links, clubs, societies, secondary employment or social activities and may, in many cases, be unavoidable. Consequently, they should be addressed by being declared to an employer so that any actual or potential risk can be appropriately managed.

Declarable associations should not be viewed negatively by either employees or by public sector bodies. It is important to note that having a declarable association is not misconduct. The improper act stems from a failure to declare or properly manage the association. It is for this reason that such associations are best referred to as ‘declarable’ rather than ‘inappropriate’ associations.

Declaring associations helps maintain the credibility of an employee and the public body as a whole and reduces risks to a public body’s operations.
Agencies should have clear policies in place around the identification and reporting of declarable associations. Where employees do not have a clear understanding of what constitutes a declarable association or how they should declare that association, compliance with the policy is likely to be poor. Best practice policies integrate mandatory reporting of declarable associations into the recruitment process and during periodic checks on employees’ personal particulars.

Public bodies should also ensure there are systems in place to record declarable associations. Much of the preventative value of a declaration is lost if it is not accurately recorded in a way that can support decision making in the future. For example, if an organised crime figure is befriending multiple employees across different areas of an organisation, this might not be identified if declarable associations are not centrally recorded.

6.6 Staff welfare

Many of the issues that heighten employees’ susceptibility to organised crime cultivation can also have adverse impacts upon their welfare. Organisational responses to illicit drug use, problem gambling and relationship breakdowns must account for the welfare of the individual as well as any impact upon the security of the public body. Relationships should be established between the welfare areas of public bodies such as human resources and the areas responsible for security. This should ensure sensitive and effective arrangements are in place to address the sharing of information related to employee activities that could increase their susceptibility to cultivation.

7 Conclusions

The full extent of organised crime involvement in public sector corruption in Australia remains unknown.

Many Victorian public sector bodies lack an awareness of the threat posed by organised crime groups and do not have prevention and detection measures to address the threat. This limits the likelihood of employees being equipped to identify and repel targeting by organised crime groups and the likelihood that public bodies will proactively detect and report corrupt approaches.

A significant number of public sector bodies hold information or commodities of value to organised crime groups and could be targeted.

Despite the limited information relating to organised crime approaches to Victorian public servants, it is likely that crime groups will continue to target public sector bodies to access these information systems and commodities.

Consequently, risk assessments undertaken by Victorian public sector bodies should reflect an awareness of the threat. Agencies can respond by adopting measures proportionate to the risk they face, such as by changing recruitment practices, vetting, revalidation, auditing, conflicts of interest, declarable associations and training.

Raising awareness of the threat and of the appropriate protective measures will better equip public sector bodies to identify and repel cultivation attempts by organised crime groups.
8 References

1 This definition is based on the definition of an ‘organised crime offence’ in section 3AA of the Major Crime (Investigative Powers) Act 2004 (Victoria) which is similar to the definition of ‘serious and organised crime’ in section 4 of the Australian Crime Commission Act 2002 (Commonwealth) and the definition of an ‘organised criminal group’ in Article 2 of the United Nations Convention Against Transnational Organised Crime.


