



# Organised crime group cultivation of Victorian public sector employees

INFORMATION FOR PUBLIC SECTOR AGENCIES

[www.ibac.vic.gov.au](http://www.ibac.vic.gov.au)

Did you know your employees could be targeted by organised crime groups to access information, influence decisions and manipulate systems?

Criminal groups have been identified targeting all levels of government including council workers, departmental officers and law enforcement employees.

## Your agency could be at risk

If your agency is not aware of the risks presented by organised criminal groups or lacks the basic protections against organised crime cultivation, you increase the likelihood that you could be targeted.

This document outlines some of the key risks and mitigation strategies to guard against organised crime group cultivation.

---

**Organised crime** means activities involving two or more offenders and an offence against the law of Victoria that is punishable by 10 or more years imprisonment, where:

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

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.

---

## Why do criminal groups target public sector employees?

Organised crime groups can target public bodies to access:

- databases, particularly those with personal identification information that could facilitate identity theft, debt collection, witness intimidation, extortion, or that could be sold to other criminal groups
- decision-making processes, including contracting and tendering and the regulation of particular industries
- property and goods with high resale value or that facilitate criminal activity.

The cultivation of public sector employees is an attractive way for organised crime groups to facilitate their criminal activities. Where a public sector employee can be persuaded to cooperate with a criminal group, they offer the group ongoing access to information or assets while using their inside knowledge of that public body's systems to avoid detection. Manipulating public sector employees is an efficient and cost-effective means of facilitating major criminal enterprises.

## Agency vulnerabilities

The most vulnerable agencies will be those with:

- **large identity data holdings**, particularly where those systems can be accessed by a large number of employees
- **decision-making and regulatory powers**, including those agencies overseeing the security, construction, planning, development, prostitution, gaming and liquor industries
- **access to sensitive information**, including law enforcement information.

## Vulnerabilities for agencies

The following table outlines data holdings, potentially at-risk sectors, and practices that could be targeted by organised crime groups.

<b>Data holdings</b>	<b>Sectors with decision-making and regulatory processes</b>	<b>Work and security practices</b>
<ul style="list-style-type: none"> <li>• law enforcement information</li> <li>• identity information</li> <li>• financial information including credit card and billing details</li> </ul>	<ul style="list-style-type: none"> <li>• security</li> <li>• construction</li> <li>• planning</li> <li>• development</li> <li>• prostitution</li> <li>• gaming and liquor</li> <li>• licensing</li> </ul>	<ul style="list-style-type: none"> <li>• poor security culture</li> <li>• poor proactive use of auditing functions</li> <li>• lack of adequate, role-based, personnel security risk assessment</li> <li>• poor pre-employment screening</li> <li>• poor communication between business areas</li> <li>• lack of awareness of people risks at a senior level</li> <li>• inadequate corporate governance</li> </ul>

## Consequences of criminal cultivation

The following table outlines potential consequences of successful criminal cultivation by organised crime groups.

<b>Employee</b>	<b>Agency</b>	<b>Societal</b>
<ul style="list-style-type: none"> <li>• embarrassment</li> <li>• physical harm</li> <li>• threats to themselves, family and friends</li> <li>• loss of employment</li> <li>• reputational damage</li> <li>• identity theft</li> <li>• investigations or penalties associated with criminal activity</li> </ul>	<ul style="list-style-type: none"> <li>• reputational damage</li> <li>• financial loss</li> <li>• loss of intellectual property</li> <li>• breaches of physical security around buildings and infrastructure</li> <li>• intimidation, violence and threats to employees</li> <li>• legal consequences associated with criminal investigations</li> </ul>	<ul style="list-style-type: none"> <li>• threats to the physical safety of community members</li> <li>• loss of services or provision of inadequate services</li> <li>• unfair tendering conditions for public sector contracts</li> <li>• loss of confidence in public organisations</li> <li>• increased risk of identity theft</li> </ul>

## How your employees could be targeted

### RISK-TAKING BEHAVIOURS

### SOCIAL MEDIA

### PRE-EXISTING RELATIONSHIPS

### INCIDENTAL ASSOCIATIONS

Organised crime groups are becoming more sophisticated in their approaches to public servants. In many cases it may be difficult to identify cultivation attempts by organised crime group members. Organised crime groups may try to develop relationships with public sector employees using some of these tactics:

- targeting risk-taking behaviour by public sector employees such as illicit drug use or problem gambling. These activities can leave public sector employees vulnerable to being coerced or manipulated by organised crime groups
- utilising social media in innovative ways, such as using Facebook to target individuals who can be identified as public sector employees
- using pre-existing relationships to shift public sector employees' loyalties away from their employer. Members of the crime groups might develop these relationships and seek to persuade the targeted employee that helping a friend is the right thing to do
- through shared interest. Evolving interests associated with organised crime group members and the broader community have created new areas where organised criminals and public sector employees can interact. Organised crime groups members now increasingly mix with broader community groups at fitness clubs, tattoo parlours, and body building and martial arts venues.

## Prevention and detection strategies

Some public sector bodies are not aware of the threats posed by organised crime groups and lack appropriate prevention and detection measures to mitigate these risks.

The following strategies can assist public sector agencies to prevent and detect organised crime cultivation.

### Security culture within public bodies

- Risk assessments undertaken by public bodies should address the threats presented by organised crime groups.
- Clear security and integrity standards should be established that are tailored to the types of risk faced by different public bodies.
- There should be engagement with staff around the development, implementation and monitoring of prevention and detection strategies.
- Identifying high-value information and systems ensures bodies can apply appropriate protections to the areas that are most likely to be targeted.

### Declarable associations

- Personal relationships between public sector employees and criminal entities have long been identified by law enforcement and anti-corruption agencies as a risk.
- Declaring associations helps maintain the credibility of an employee and the public body.
- Agencies should have policies around the identification and reporting of declarable associations and there should be clear consequences for failing to do so.
- Best practice policies integrate mandatory reporting of declarable associations into the recruitment process and during periodic checks on employees' personal particulars.

## Pre-employment checks and revalidating employees

- Vetting during recruitment serves as an important strategy to detect and prevent organised crime cultivation.
- Revalidation of employees' security clearances at regular and or random intervals during their employment ensures public bodies can respond to changes in employees' risk factors.
- The introduction of the Victorian Protective Data Security Framework seeks to address these inconsistencies by making certain security standards mandatory across the public sector.

## Auditing

- Routine auditing of information and financial systems can identify where there has been inappropriate access to, or use or sharing of, information, systems or property.
- Public agencies could do more to proactively audit their information and financial systems housing sensitive data.
- Auditing should be used to proactively identify suspicious activity and not only to determine the extent of a breach after it has been detected.

If your public sector body has access to information or commodities of value to organised crime groups then you could be targeted.

Organisational risk assessments should include an assessment of the risks presented by crime groups. Responses to address these risks may include proactive random auditing of identified risk areas, regularly checking for conflicts of interest and declarable associations.

## More information

For more detail about the mandatory security standards required of Victorian government agencies, visit the website of the Victorian Commissioner for Privacy and Data Protection at [www.cdpd.vic.gov.au](http://www.cdpd.vic.gov.au)

The Victoria Public Sector Commission produces guides for recommended recruitment practices, codes of conduct and organisational culture that are available at [www.vpsc.vic.gov.au](http://www.vpsc.vic.gov.au)

If you would like further information about the material provided in this fact sheet, download the related report *Organised crime group cultivation of public sector employees* from the IBAC website [www.ibac.vic.gov.au](http://www.ibac.vic.gov.au)

Level 1, North Tower  
459 Collins Street,  
Melbourne VIC 3000  
GPO Box 24234,  
Melbourne, VIC 3001

T 1300 735 135  
F (03) 8635 6444

September 2015

IBAC is Victoria's anti-corruption agency responsible for identifying and preventing serious corrupt conduct across the whole public sector, including members of Parliament, the judiciary and state and local government.

IBAC also has a broad oversight role in relation to police personnel misconduct and an important education function to proactively assist public sector agencies to improve their systems and processes to prevent corrupt conduct.

**To report corruption phone 1300 735 135 or visit [www.ibac.vic.gov.au](http://www.ibac.vic.gov.au)**