



MEDIA RELEASE

23 April 2020

Serious misconduct in leading integrity agency has lessons for all

The Corruption and Crime Commission has tabled its [Report into misconduct risks with access to confidential information in the Office of the Auditor General](#) in State Parliament today, with startling revelations of serious misconduct and corruption risks within one of the State's major integrity agencies.

The Commission's report details how two auditors, each a certified practising accountant, had regularly accessed sensitive and confidential information within OAG systems that were not properly protected.

One of the auditors obtained access to the names and addresses of every serving police officer in WA while completing an audit and then retained them – 8,800 officers, employees and contractors stored in a spreadsheet on a laptop computer, unbeknown to the OAG.

There is no evidence the police data was shared, however the misconduct risk is real and its value to organised crime could be immense. This risk is obvious and must continue to be addressed by the OAG.

The report also outlines how both auditors routinely accessed confidential information about other OAG colleagues, including their payroll details and other personal information. This is private information that must be secure and available only to those who have a legitimate need for it.

The Commission formed an opinion of serious misconduct in relation to an auditor's deliberate destruction of an encrypted IronKey USB. Perhaps because he was angry, as he claimed, or possibly because he didn't want an examination of what had been stored on it, or what had been done with data from it.

Specific misconduct risks revealed in this report include:

- the easy transfer of data, despite being securely stored on an IronKey USB, which could potentially be misused;
- identity theft, facilitated by access to payroll systems;
- access to home addresses (of serving police officers) which may be used for intimidation or other serious criminal offences against individual officers, or may lead to the exposure of officers working in covert or other high-risk areas;
- access to confidential information which could be used to blackmail or manipulated for personal gain; and
- the risk of organised crime targeting public servants for information.

"Although the OAG was the centre of this investigation, all public sector agencies should immediately evaluate their data management risks and, where necessary, take action to mitigate them," said Corruption and Crime Commissioner the Hon. John McKechnie QC.

[Report into misconduct risks with access to confidential information in the Office of the Auditor General](#) is the final report presented to State Parliament by Corruption and Crime Commissioner the Hon. John McKechnie QC before his term concludes on 27 April 2020.

ENDS

Read the report

[Report into misconduct risks with access to confidential information in the Office of the Auditor General](#)

Media contacts

Marie Mills: 0418 918 202 or mariem@millswilson.com.au

Louisa Mitchell: 0434 308 208 or louisam@millswilson.com.au