WESTERN AUSTRALIA

CCC | Corruption and Crime Commission

Report into misconduct risks with access to confidential information in the Office of the Auditor General

Version 2
August 2020

ISBN: 978-0-6485674-7-9

This report and further information about the Commission can be found on the Commission website at www.ccc.wa.gov.au.

Corruption and Crime Commission

Postal Address PO Box 330
Northbridge Post Shop
WA 6865

Telephone (08) 9215 4888
1800 809 000
(toll free for callers outside the Perth metropolitan area)

Facsimile (08) 9215 4884

Email info@ccc.wa.gov.au

Website www.ccc.wa.gov.au

Twitter @CCCWestAus

Office Hours 8.30 am to 5.00 pm, Monday to Friday

Special Needs Services

If you have a speech or hearing difficulty, contact the Commission via the National Relay Service (NRS) on 133 677 for assistance or visit the NRS website, www.relayservice.com.au. NRS is an Australia-wide telephone service available at no additional charge. The Commission's toll-free number is 1800 809 000.

If your preferred language is a language other than English, contact the Translating and Interpreting Service (TIS) for assistance on 13 14 50. TIS provides a free, national, 24 hours a day, seven days a week telephone interpreting service. TIS also provide on-site interpreters for face-to-face interviews by contacting 1300 655 082.

TABLE OF CONTENTS

CHAPTER ONE

Overview

[1] The Auditor General is an independent officer of Parliament and the *Auditor General Act 2006* gives the Auditor General independence in decision-making. The Office of the Auditor General (OAG) is a major integrity agency.

[2] In carrying out its functions, necessarily the OAG must examine material within public authorities that is confidential and sensitive. For this reason, officers of the OAG are required to keep material they uncover during the course of their work as auditors confidential on pain of penalty.[1]

[3] On 27 February 2019, as required by law,[2] OAG notified allegations of serious misconduct to the Commission. The misconduct risk in relation to data and information is one of the Commission's strategic themes informing its decisions on possible investigations. In view of the potential misconduct risk in the exposure of confidential information, the Commission commenced an investigation code named Operation Phoenix.

[4] Although OAG had conducted a preliminary investigation, the seriousness of the allegations were best suited to a Commission investigation which could utilise digital forensic expertise and hold private examinations.

[5] The outcome is startling. Two auditors, each a certified practicing accountant (CPA), had routinely accessed confidential information about other OAG officers, including payroll details and other private and confidential information.

[6] They were able to access confidential information within OAG because it was not properly protected. Once an officer in OAG logged on using a password, that officer had access to all of the OAG systems, including access to TRIM, a record management system. Each primary file on TRIM had its own access controls set by OAG staff. The primary file was a dataset in that it contained numerous individual documents relating to that subject. If the officer's staff profile had access to a particular file, that access allowed the officer not only to browse or read the documents contained within that file, but to download the document or migrate it to a private device.

---

[1] *Auditor General Act 2006* s 46.

[2] *Corruption, Crime and Misconduct Act 2003* (CCM Act) s 28.

[7] In its response to a draft of this report, OAG detailed the security requirements and the defect that enabled the breach:

> *OAG's systems and datasets have additional security requirements on a role-based or need-to-access basis.*
>
> *The payroll system and the finance system for example have strong access controls that limit access only to specifically identified staff. These are not open to all staff.*
>
> *Audit files are only accessible by audit staff in the relevant division, with sensitive audit files having restrictive access to only the relevant audit team.*
>
> *Some (but not all) sensitive/confidential files in TRIM had lost their tight security when new versions were created and the new files did not inherit the access restrictions of the parent folder. This was subsequently addressed with enduring monitoring controls in place.*[3]

[8] The officers' conduct described in this report demonstrates that information on the systems such as payroll reports and credit card statements were open to all staff, albeit due to inadequate access controls on TRIM.

[9] In most organisations, an officer is given access only to those matters required for their role. Access to payroll and personal details of staff is generally confined to members of human resources and finance teams.

[10] The potential for others to acquire this information is a serious misconduct risk. It can be used for personal gain. It can be sold to criminals.

[11] In the course of Operation Phoenix, the Commission uncovered a further misconduct risk.

[12] Auditors from OAG working in teams routinely make site visits to public authorities to conduct audits.

[13] Security of data provided by the public authority for the purpose of an audit is controlled by use of an encrypted USB flash drive, known as an IronKey. The IronKey is used with a laptop computer provided to each auditor by OAG.

[14] OAG's policies require information received on an IronKey to be deleted after it is uploaded to the OAG audit program. OAG provides periodic reminders regarding the obligation for staff when information is particularly sensitive. However, if these policies are not followed,

[3] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 2.

information may remain on a laptop for years, able to be copied and shared.

[15] OAG, in its response to this paragraph said:

> *OAG has a policy that requires that information received from client agencies is deleted from the IronKey after it is loaded into the OAG's protected audit workpaper system.*
>
> *Further, for the audit in question the Assistant Auditor General gave written instructions to all auditors, reminding them of this and other security requirements around data handling. This was supplemented by verbal advice. The officer in question was one of those given these reminder instructions …*
>
> *We have also undertaken periodic checks that staff do not retain copies of audited entity information on their laptops and IronKeys.*[4]

[16] Clearly, whatever policies and instructions were in place, did not work. This remains a serious misconduct risk.

[17] An auditor obtained and retained access to the names and addresses of every serving police officer in WA, some years after completing an audit of the WA Police Force. The names of 8,800 officers, employees and contractors were stored on a spreadsheet on a laptop computer. OAG was unaware until the laptop was forensically examined as part of Operation Phoenix. There is no evidence the police data was shared with others. However, the misconduct risk is obvious. The information was less than five years old. Its value to criminal elements could be immense.

[18] OAG has independence of action and is responsible for auditing the finances and actions of all departments of government, State and local. It should be trusted to keep information confidential. The misconduct risk exposed in this report shows, unless OAG has taken action to tighten its controls, that trust may be misplaced.

[19] OAG, in its response said 'OAG took remedial action immediately following the incident. It is of high priority to the Office that audited entities can place trust in the OAG. Strong information security and continuous improvement is of upmost importance to the OAG'.[5]

[4] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 3.
[5] Ibid.

Why make this report public

[20] An aspect of the serious misconduct function of the Commission is to help public authorities to prevent serious misconduct.[6]

[21] OAG has made representations that this report be not made public:

> *In relation to the matter of a staff member not following instructions, we have concerns that publication of the matter would impact the Office's ability to fulfil its purpose. Despite the Auditor General's clear mandate to access records, OAG teams already experience reluctance and obstruction in getting access to data. The attention of senior, experienced staff is often diverted to liaising with agency management to obtain access to data. We believe making public the matter of the Police spreadsheet will not only cause undue angst among current and serving police officers, and potentially raise the profile of its existence amongst criminal elements, it will make agencies more reluctant to provide access, thereby further diverting the time of our experienced management staff.*
>
> *As this instance, serious as it is, relates to one officer disobeying policy and instructions, we suggest the report, or that particular finding not be made public. The Office has already taken prompt action to address this matter, and will maintain increased ongoing vigilance in this regard. To reiterate, making an example of one person by publication of the report, will impact audit staff's ability to do their job for years to come when the lesson has clearly been learned.*[7]

[22] These are matters of substance and the Commission has considered them. It notes that the WA Police Force is less concerned that the publication of the facts surrounding the retention of the police database will have an adverse impact on its operations.

[23] The Commission has decided that the public interest is best served by publication.

[24] Parliament, of which the Auditor General is an independent officer, is entitled to know there is a misconduct risk in that office.

[25] Moreover, this report is a misconduct risk report for the benefit of all public authorities so that their individual data management risks may be evaluated and, where necessary, mitigated.

[26] OAG, as part of its response, refers to policies and instructions, some of which were breached by the two auditors.

[27] If there is one defining message from their conduct, it is that policies, procedures and instructions are not enough. There must be technological security built into the system and periodically reviewed.

---

[6] CCM Act s 18.

[7] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 1.

CHAPTER TWO

Access to confidential information

[28] On 24 January 2019, senior officers at OAG became aware that a staff member had been accessing a payroll file containing a range of personal information about all staff members. Access had been made regularly, each fortnight, since July 2018.

[29] The officer was an auditor and had been involved in financial audits, amongst others, of the WA Police Force, Department of Justice and Corruption and Crime Commission. In these audits, he may have been entrusted with access to some of the most confidential and sensitive information held by a public authority. He will be referred to as officer one.

[30] On further review, it became apparent that an auditor had accessed three of the same payroll files. He first denied accessing any information, but later claimed he may have accessed the files in error. In private examination before the Commission, the officer was frank in admitting his access to a number of files. He will be referred to as officer two.

[31] The information stored in the TRIM payroll folder includes:

Detailed Costings Report - for each individual on payroll:

- *Name*
- *Salary*
- *Age*
- *Allowances*
- *Deductions - not identified*

Pay Summary Report for each individual:

- *Name*
- *Net salary*
- *Tax*
- *YTD totals*

Creditor Payments Detail Report – Names and details of employees who have deductions made for the following, and amounts deducted:

- *Child support*

- *Tax paid*
- *Tax debts*
- *Maxxia deductions*
- *Social Club*

GESB Files - Names of all staff and their:

- *Contact details*
- *Date of birth*
- *Home address*
- *Superannuation account details*
- *Tax file number*

Payrun report:

- *Name*
- *Title*
- *Hours worked*
- *BSB and bank account number*
- *Gross salary*
- *Net salary*
- *Leave taken*
- *Employee's level and increment*
- *Child support paid*
- *Superannuation paid*
- *Allowances*

[32] In addition to the data contained in the payroll reports, other HR files were accessed, including files that contained birth certificates, details of professional and academic qualifications and relocation support arrangements.

[33] OAG, in its response to this paragraph said: 'In our view, details of staff professional and academic qualifications are not confidential, as we need that information to allocate staff to audits. As such, it is widely used information in the OAG'.[8]

[8] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 4.

[34] The TRIM documentation viewed or downloaded by both officers separately included:

- Incidents when additional payroll information was viewed or extracted, including officer one accessing the payroll transaction file shortly after its creation every fortnight from July 2018.
- Incidents of access to other officers' personal information, including details of salary recoups for secondment arrangements, with officer one accessing some documents dating back to 2012 and officer two dating back to 2018.
- Incidents of access to documents of reimbursements to other officers. Most of these were dated between 2011 and 2015, accessed on an ad hoc basis by officer one between August and December 2018 and by officer two between September and December 2018.
- Incidents where evaluation and career progression memos were accessed for other officers.
- Incidents of access to documents which were internal memos to and from members of the executive management group (EMG).

[35] In addition, an auditor viewed at least one monthly credit card statement for the Auditor General and officer two accessed the server room logs.

Code of Conduct

[36] In common with all organisations, OAG has a Code of Conduct and affirms it is committed to the highest standards of corporate governance. The Code of Conduct was acknowledged by both officers. The Code of Conduct provides:

> *Professional ethics and the law dictate that OAG employees respect the confidentiality of information acquired during the course of their work, using it only for work related purposes. As a condition of employment with the Office, section 46 of the Auditor General Act 2006 requires the preservation of secrecy of all matters known as a result of work under this Act. This prevents communication of any such matters to any person except as may be required in connection with the administration of this Act.*
>
> *Confidentiality of information remains in place after cessation of the employment contract. Unjustified and unauthorised release of audit information could compromise the public interest and possibly jeopardise an audited entity's ability to perform its functions. Confidentiality of working papers is a professional as well as statutory issue. Penalties of up to $50,000 can be enforced for disclosure of*

information. Under no circumstances should information be used for personal gain.

[37] The Code of Conduct further provides that officers of the OAG must respect confidentiality of information at all times. Information and material collected while performing duties of the office is the property of the OAG. It should be kept securely and only used for its intended purpose.

[38] Both officers breached the Code of Conduct but nearly six months passed before their accesses were detected.

CHAPTER THREE

Serious misconduct risks surrounding confidential personal information within the Office of the Auditor General

[39] Serious misconduct occurs if:

(a) a public officer corruptly acts or corruptly fails to act in the performance of the functions of the public officer's office or employment; or

(b) a public officer corruptly takes advantage of the public officer's office or employment as a public officer to obtain a benefit for himself or herself or for another person or to cause a detriment to any person; or

(c) a public officer whilst acting or purporting to act in his or her official capacity, commits an offence punishable by 2 or more years' imprisonment.[9]

[40] The Commission may report on ways to prevent and combat serious misconduct in public authorities.

[41] Public authorities hold a great deal of information about citizens and their own officers. That information can be valuable to others and may be used for personal gain.

[42] When a public authority lacks or does not enforce sufficiently robust information controls, there is a serious misconduct risk that information will fall into the wrong hands.

[43] In what follows, the Commission stresses there is no evidence that sensitive or confidential information was shared or distributed, so no opinion of serious misconduct has been formed in respect of the significant data breaches. However, the misconduct risk is real and should continue to be addressed by OAG.

[44] OAG in its response to this paragraph said 'Immediately following the incident, the OAG took multiple actions to address the risk'.[10]

[45] Other public authorities should examine their systems to ensure compliance with current policies on privacy and information sharing.

[46] The risks can be illustrated by the actions of each of the two officers.

[9] CCM Act s 4(a)-(c).

[10] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 5.

Officer one

[47] Officer one has a Bachelor's Degree in Accounting and is a CPA. Officer one was employed as an auditor at OAG.

[48] Officer one conceded that he had accessed personal information of other officers. He attempted to pass responsibility to the system:

> *I didn't think it was confidential in nature given everyone in the whole organisation had access to that information. There wasn't any, I guess, preface to the information saying it was confidential; alerts, warnings, headings or anything like that. I'd like I said if it was known and made aware and I knew that it was confidential, I wouldn't have accessed that information.*[11]

[49] If this is a commonly held view in public authorities, it needs to be swiftly corrected. Some material is self-evidently confidential.

[50] In examination, officer one admitted to accessing about six months' of payroll data, which included fortnightly certifications and payroll verification reports for other divisions within OAG. He also accessed commencement information for new officers.

[51] Officer one accessed monthly credit card statements and acquittals. Various officers within OAG, including the Auditor General herself, have business credit cards. His explanation as to why he accessed credit card information was implausible. He said "I guess curious".[12]

[52] OAG in its response to this paragraph said 'The type of expenditure by the [Auditor General] (parking etc) is not generally more confidential than that of any other cardholder'.[13]

[53] It appears from this response that OAG does not see an issue with an officer having access to credit card expenditure without any good reason. The serious misconduct risk should be obvious and is explained in this report.

[54] Officer one agreed there was no reason for him to access the credit card information but tried to explain his actions:

> *Like I said, it might have been within other documents I wanted to check, and when I pressed the document that I want, it went to her document instead. Because when you access TRIM remotely, it is quite slow. If you press on a document by one document that you wanted, and because if it's refreshing or whatever, it would open up another document by mistake.*[14]

---

[11] Officer one transcript, private examination, 7 February 2020, p 15.
[12] Ibid 25.
[13] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 5.
[14] Officer one transcript, private examination, 7 February 2020, p 27.

Well, like I said, when I was asked for a credit card, I just went through just to see why my name is being mentioned, and I just looked through – I might have looked at several credit cards just to see, whether it was actually me or someone else. Like I said, I don't know who has a credit card, but I can only assume the credit card would be the senior people in the organisation.[15]

[55] During examination, after he denied disclosing any credit card information to another person, officer one was confronted with a telephone conversation:

That one I forgot. She asked me as an auditor, the Auditor General's Office that, is it common that, heads of departments get their internet paid by the agency? And she asked me, do I recall any other agencies have internet paid? She was my client, because one of my clients … and I was trying to answer her query best as possible. And I might have looked at the AG's credit card just to explain, my intention wasn't to tell her what was the nature of the credit card purchases.[16]

[56] The conversation occurred months after officer one had resigned from OAG. His explanation makes little sense. When pressed to explain deliberately accessing the Auditor General's credit card statement, he said "Look, I might've done it, but maybe for these type of reasons, it wasn't for personal gain you know, criminal offence, you know what I mean. I mean, that's the best way I can explain".[17]

[57] Officer one accessed meeting notes between the Auditor General and heads of other agencies:

I did access, because – I guess what I wanted to do is to understand the ongoing of the organisation, part of the reasons why I did that is, previously, at a job interview in the office, I was advised that, "You're not giving any strategic planning advice or strategic actions of the organisation or input … The reason why I thought that was important for me to know is, given the fact that I was assistant director, I'm the one managing the budget.[18]

[58] Officer one never audited the Water Corporation and was asked why he accessed meeting notes between the Auditor General and the CEO of Water Corporation. He was unable to satisfactorily explain his actions. Like officer two, officer one relied on the fact that the system allowed access, to claim that this meant the material he was searching was not confidential.

[59] OAG in its response said:

Internal briefing notes (prepared pre-meeting for the [Auditor General]) are not always necessarily locked down from all staff, as they generally contain publicly or internally-known information about the entity and may also be referred to by

[15] Ibid 29.
[16] Ibid 30.
[17] Ibid 33-34.
[18] Ibid 35.

other staff and teams when preparing meetings or documents. We are not sure how this is relevant to the investigation.[19]

[60] Over a period of approximately six months, officer one routinely accessed confidential information about his superiors, people who were on an equal level and other officers within OAG. His consistent explanation was that the information was available for everyone to see and he did not think it was inappropriate at that point in time. That explanation is difficult to accept.

[61] During a forensic examination of officer one's personal computer, OAG data such as payroll and personal information was discovered. The files were neatly collated in a document folder on his personal computer.

Conclusion in relation to officer one - no opinion of serious misconduct in relation to his accesses

[62] Officer one not only extensively viewed material relating to payroll data, credit card statements and other matters, but also on at least one occasion, conveyed information to a person outside the OAG.[20] His explanations in particular for accessing credit card statements lacked plausibility.

[63] There is no evidence that officer one used the information he obtained for personal gain or to cause detriment. He explained, and the Commission accepts, during the relevant period he was under extreme stress due to issues of a personal nature.

[64] Officer one's interrogations of the systems were extensive and regular, with many downloads. While the Commission accepts that officer one did not act with a corrupt intention, it is unable to determine why he acted as he did.

[65] Officer one's actions in relation to the access of data of the OAG do not reach the threshold for an opinion of serious misconduct.

[66] Again however, officer one's actions illustrate the serious misconduct risk that exists when confidential information is stored without proper controls and restrictions on access. Mere existence of policies and procedures is not enough.

Officer two

[67] Officer two has a Bachelor Degree in Accounting and is a qualified CPA.

[19] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 6.
[20] Ibid 29-32.

[68] He commenced at OAG as a graduate and has worked permanently within OAG for some years.

[69] Over the last few years, officer two developed a perception that he has been unfairly treated, compared with his colleagues. He believes he may have been overlooked for career progression. Officer two singled out conflict with a senior manager concerning a possible position to which he aspired. Whether his perception is correct is immaterial. At some point in 2018 officer two discovered OAG's systems allowed him to access information on career progression, staff reimbursement claims and secondment information for other officers after he logged in using his password.[21]

[70] OAG's response to this paragraph is noted:

> *This information is in the record keeping system and an employee has to make a conscious decision to open the system, and then to search for information using specific terms. The wording in the draft report makes it sound like information was available without conscious effort to look for it.*[22]

[71] Officer two regularly reviewed many files for which he had no professional or other reason. These have been generically described in Chapter Two. He accessed and read the details of many OAG officers.

[72] In an interview with an OAG manager in February 2019 and subsequently in examination before the Commission in July 2019, officer two tried to justify and minimise his actions, which he ascribed to curiosity, frustration and stress. He was also evasive:

> *Would TRIM keep records as to who would access documents?---I don't know that. Before – I always come back to the investigation. I didn't know that.*
>
> *You didn't know they did? So what's the investigation you're discussing, you said your office is conducting an investigation?---That I had accessed multiple documents, that the office has conduct an investigation saying that there are certain files contain people's personal informations, like name, date of birth, tax file number, superannuation. Because there's been an email sent to the whole office, and then – tax file numbers, home address, date of birth, that kind of personal information that has been accessed. And then why first we say the email was quite surprised who would do that, and then I find out that actually they investigated me in regarding to the matter.*
>
> *…*
>
> *I didn't know at the time that I'm the person that did that. I didn't know I am the person that did that, for sure.*

[21] Officer two transcript, private examination, 24 July 2019, pp 55, 58-59.
[22] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 5.

I can't remember, but I don't deny the fact that if the log system is showing that, then I must have, according to the records. But for my personal memory, I deny the fact that I've seen those tax file numbers, date of births or superannuation.[23]

[73] Officer two later specifically recalled accessing graduate evaluation surveys, staff claims and secondment information. This evidence suggests that officer two's recall was more extensive than he was prepared to admit.

[74] He explained his curiosity and frustration in this way:

… it's a series of things that cumulates to a certain point that I just can't hold any more, and I - distress – I was suffering from anxiety, I couldn't get sleep, I can't concentrate on my work. I would say today. I was just asking myself, if I work hard on my job, what do I get? What's the purpose I want to achieve? I'm hopeless. I go through the proper channel, go to HR, go to the senior director, trying to find out what happened. No one tells me … So I went to the HR report, purposely searching for the answer, the reason how – if I can't find the reason to my own question, I search my own information first. I can't find it. I want to see how other people getting treated.[24]

[75] When challenged as to why he opened payroll verification reports three times:

Maybe I was just curious that they could be opened. I'm curious that these kind of documents are actually there, can be opened and can be viewed publically. I didn't hack into the system, I was just curious that it's there, that you can actually open it.[25]

[76] After initially denying that he knew what 'EMG' stood for, officer two conceded he opened the EMG meeting papers file "Either for curiosity or for the purpose of finding my answers".[26]

Conclusion in relation to officer two - no opinion of serious misconduct in relation to his accesses

[77] There is no evidence officer two passed on any information he viewed.

[78] After a comprehensive private examination, the Commission concluded that officer two did not access the information for a corrupt purpose, such as personal gain, but through curiosity. The curiosity was bred from his anxiety, stress and frustration out of his perception, whether accurate or not, that he was being treated unfairly.

[23] Officer two transcript, private examination, 24 July 2019, pp 35-36.
[24] Ibid 38.
[25] Ibid 39.
[26] Ibid 43.

[79] OAG's response:

> *Some (but certainly not all) sensitive/confidential files in TRIM had lost their tight security when new versions were created and inheritance of controls did not occur. The timing for this appears to have coincided with implementation of a new payroll system. It is now rectified with ongoing monitoring controls in place.*
>
> *In addition, other systems (the payroll system itself and the finance system) have access controls that limit access. These are not open to all staff.*
>
> *Moreover, audit files are only accessible by audit staff within the relevant division, with sensitive audit files having restrictive access to only the relevant audit team.*[27]

[80] This explanation does not detract from the fact that at the time of multiple accesses, there were no restrictions in place for accessing documents of a financial and human resources nature other than by entering a password to log on to a computer.

[81] In the Commission's opinion, officer two's actions were naïve and silly in the extreme, but do not meet the threshold necessary for an opinion of serious misconduct.

[82] Officer two's frequent and unconstrained access however exposes a serious misconduct risk.

[27] Clarifications enclosed in letter from the Auditor General to Commission, 8 April 2020, p 5.

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

CHAPTER FOUR

Misconduct risk in audits of public authorities

[83] OAG allocates teams to public authorities to conduct audits. Generally, auditors will go to the authority concerned to work, but may work anywhere, including in the OAG office. Auditors are provided with a laptop computer and an IronKey.[28]

[84] When an audit commences, an auditor will create an audit pack. Auditors work in teams and information will be shared among them. The information uploaded to an audit pack remains within the secure audit workpaper system, IPSAM. Auditors may download an audit pack onto a laptop from a prior year's audit to understand what should be contained within the audit pack. By the nature of the work, auditors are exposed to a great deal of confidential information which should and must be kept secure.

[85] There appears to be a gap in OAG policies regarding what is to be done with information received by an auditor at the conclusion of an audit. The information is held in the IPSAM system which is stored on OAG's servers, but it may also be temporarily held on an IronKey. Auditors should delete the information from an IronKey once an audit is complete and should take care not to store a copy of the information on their work laptops. However, as the Commission's investigation identified, this does occur, on occasion.

[86] The misconduct risk is illustrated by reference to the WA Police Force.

[87] In the course of its forensic examination on the OAG laptop issued to officer one, a number of audit files were found.

[88] Among other documents, the Commission discovered a spreadsheet containing names, addresses and other personal details of 8,800 police officers and police department employees and contractors.

[89] Officer one expressed surprise at this material, which dated back to 2015, the last time he conducted an audit of the WA Police Force. He was unaware the spreadsheet was on the computer.

[90] Officer one denied giving information from that spreadsheet to any other person. There is no current evidence that he shared any of the information. However, the WA Police Force has been made aware of the list and given a copy of the computer image to further examine.

[28] For a description of an IronKey, please see paragraph [115, 119].

[91] If the Commission did not alert the WA Police Force to the information being retained outside of the purpose for which it was given, namely an OAG audit, it would be unaware the information was potentially compromised.

[92] Public authorities, when providing sensitive information to a third party, should consider that party's policies in respect of what they will do with the information given after it is no longer needed. Public authorities ought to also consider whether such policies are followed.

CHAPTER FIVE

Serious misconduct risks

Access to confidential personal information

[93] Operation Phoenix uncovered serious misconduct risks surrounding the acquisition and storage of information and the access to information held by public authorities.

[94] Although OAG was the centre of this investigation, all authorities should urgently check their systems and settings to ensure confidential information is secure and available only to those who have a legitimate need for it.

[95] For example, while payroll and human resource officers will need access to confidential information about their officers, it is far less clear whether anyone else in an organisation would need unrestricted access to that same information.

Use of personal IT equipment

[96] Officer one gave evidence that he could, and did, download information from an audit pack onto his personal computer: "I might have my second laptop, typing away, while looking at the evidence. It's just easier doing that rather than flick through a screen, it's more efficient and that's what I find".[29]

[97] He said he worked on his personal computer because it was much faster than his work laptop, which was made slow by underlying software.

[98] There is little point in securing sensitive data with encryption codes if it can be transferred so easily.

[99] Forensic examination of officer one's personal computer revealed numerous files containing letters to other authorities, response letters to OAG outlining the implementation of audit recommendations, and at least one letter with an attachment entitled 'commercial in confidence'.

[100] The OAG information located on officer one's computer confirms his evidence about the use of his personal computer to assist with his auditing duties.

[101] Officer one's use of his own computer was irregular but without malicious intent. It was in breach of OAG policy. He appears to have done so to be

[29] Officer one transcript, private examination, 7 February 2020, p 82.

more efficient. However, the ready transfer of confidential information to personal IT equipment, is a misconduct risk.

Specific misconduct risks

Transfer of data

[102] Although information might be securely stored on an IronKey USB, it can be easily disseminated.

[103] When the IronKey is plugged into an officer's laptop, information can be taken from it and transferred to the hard drive, where it can be downloaded by USB or other device, copied and shared.

[104] Security is highly important because of the potential misuse of information. No restrictions were in place preventing data exfiltration directly from an OAG computer, either by IronKey or non-IronKey USB device. An IronKey will operate with a non-OAG computer, once authorised by password.

Identity theft

[105] Identity theft occurs when personal information is used to steal money or gain benefits in a false name such as a passport, phone account or driver's licence.

[106] The apparent ease with which both officers were able to regularly interrogate the payroll systems of the OAG is a significant misconduct risk to the identity of all officers of that organisation.

[107] Information of a personal nature, such as name, address, date of birth and bank details, is valuable to criminals seeking to impersonate another person or create a ghost account. It may also assist for direct access into a bank account by a hacker.

Access to home addresses

[108] The misconduct risk is obvious.

[109] If criminals gain access to addresses of serving police officers that information can be used for intimidation or other serious criminal offences against individual officers. Officers working in covert and other high-risk operations might well be exposed.

Blackmail

[110] Even if information is not shared, there is a serious misconduct risk in having access to confidential information.

[111] Officer one accessed the business credit card statements of the Auditor General. As he conceded, and the Commission confirmed, there was no questionable credit card use by the Auditor General.

[112] However, the potential to blackmail a superior officer if there was a questionable transaction is obvious.

Manipulation for personal gain

[113] If access is gained to confidential information, information might be altered or manipulated for personal gain.

Organised crime targeting public authority officers for information

[114] The sensitive nature of the information held by some public authorities is demonstrated by the WA Police Force spreadsheet. Authorities audited by OAG include oversight agencies such as the Ombudsman, Public Sector Commission and Corruption and Crime Commission. There is a risk of organised crime targeting officers to obtain sensitive information for nefarious purposes.

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

CHAPTER SIX

An opinion of serious misconduct

[115] IronKey is the name of a proprietary brand encrypted USB portable storage device. A USB flash drive is a common data storage device which includes flash memory. It is, amongst other things, used to transfer data.

[116] The OAG IronKey devices were (and still are) used as a secure transfer mechanism for auditors to receive data from a public authority subject to audit. An auditor provides the IronKey to the authority for insertion into a computer. The auditor enters the password to decrypt the IronKey to allow the data transfer.

[117] All OAG computers are installed with McAfee DLP (Data Loss Prevention) software. DLP software is designed to detect, log and alert when data is removed from a system, and if configured to do so, stop data removal.

[118] DLP software is configured to ensure compliance with business policy. This may include an overt or covert alert when a data storage device is plugged into a target computer, or cause an inability to read or copy.

[119] An IronKey USB flash drive is encrypted and password-protected. The data on the IronKey self-destructs, in that the data in the device is rendered inaccessible if the wrong password is entered 10 times. When an IronKey self-destructs, the advanced encryption standard keys are erased and the IronKey may be permanently unusable.

[120] There are warnings associated with entering incorrect passwords. Each incorrect password attempt will display a warning indicating the number of attempts remaining. After every three consecutive bad password attempts, the device must be removed and reinserted.

[121] The final password attempt displays at least two very distinct warning messages stating that self-destruction is permanent and there is no way to recover an IronKey once it has self-destructed.

[122] Mr Yusoof Ariff was an Assistant Director with OAG. He was issued with an IronKey. In early 2019, he was asked to return the IronKey issued to him.

[123] Mr Ariff was examined by the Commission about the IronKey. After some hesitation, he admitted the deliberate destruction of the IronKey by entering the wrong password 10 times. He knew that would render the IronKey unusable and its data irrecoverable.

[124] His explanation to the Commission is that he was angry at the time.

[125] There is another more sinister explanation possible. Mr Ariff destroyed the IronKey because he did not want an examination of what had been stored on it, or what had been done with data from it. In examination, Mr Ariff stated he stored everything work related on the IronKey. Destruction of the IronKey prevents the Commission from confirming precisely what was on the IronKey.

[126] The Commission is unable to determine whether the true purpose was: anger, concealment, or something else.

[127] Regardless, Mr Ariff acted to destroy the IronKey in order to cause detriment to the OAG, both by loss of the device itself (a relatively small sum) and the data it held (which is unknown and therefore immeasurable).

[128] In the circumstances, an opinion of serious misconduct is appropriate.[30]

[129] An opinion that serious misconduct has occurred is not, and is not to be taken as a finding or opinion that a particular person is guilty of or has committed a criminal offence or a disciplinary offence.[31]

[30] CCM Act s 4(a)-(c).
[31] Ibid s 217A(3).

CHAPTER SEVEN

Conclusion

[130] Public authorities store personal information about citizens. The potential for misconduct in relation to that information is one of the themes which guide the Commission in selecting which matters to investigate.

[131] The Commission was surprised at the ease of access to large datasets of personal information within the OAG.

[132] Security surrounding data imported into OAG from public authorities who are subject to audit, as illustrated by the WA Police Force spreadsheet, was insufficient.

[133] There are lessons for every public authority. This report emphasises the importance of securing private information so that it may be used for legitimate purposes and no other.

Recommendations

[134] OAG conceded that its security settings were inappropriate and has taken action to tighten access to confidential information. It is **recommended** that all public authorities take urgent action to ensure appropriate security classifications and restricted accesses are in place in respect of the various classes of information held by each authority.

[135] In a report into unauthorised release of confidential information of the Public Transport Authority (18 October 2018), the Commission recommended that authority tighten access controls over confidential information including logins. This report, less than two years later, suggests that other public authorities may need to further examine controls over access to confidential information.

[136] OAG has policies to deal with confidential information obtained during the course of an audit, but as illustrated, policies and procedures may be insufficient by themselves.

[137] Information of a highly confidential nature, such as police officers' names and addresses, should be subject to rigorous protections, both before, during and after audit.

[138] The Commission **recommends** that OAG review its procedures to ensure that following an audit, data is only retained in a secure location.

[139] The Commission **recommends** that public authorities ensure confidential material used for an audit by the OAG remains confidential at the conclusion of the audit.

[140] The Commission **recommends** public authorities consider their policies with respect to securing confidential information and ensure that regular internal checks are conducted to identify and deter unauthorised accesses and disclosures.

[141] As can be seen with the officers in this investigation, public officers may either misunderstand or be unaware of their responsibilities concerning confidential information. The Commission **recommends** public authorities consider whether there are gaps in the security of confidential information and, if so, engage in training and education initiatives to raise awareness around identification, detection, prevention and reporting information misuse.