Crime and Corruption Commission
QUEENSLAND

Operation Impala

An examination of corruption and corruption risks in relation to the improper access to and disclosure of confidential information in the public sector.

Call for public submissions

20 September 2019

Contents

Overview of Operation Impala

The Queensland public sector is entrusted with a range of confidential information of varying degrees of sensitivity and value. Members of the public rightly have an expectation of privacy in the handling of this information. This is reflected in various legislative controls, obligations on employees, codes of conduct, and policies and procedures.

Any misuse of information entrusted to public sector agencies involves serious breaches of an individual's privacy and may, in some cases, create a serious risk to their or others' safety.

Unfortunately, the misuse of information – either through unauthorised access or unlawful disclosure — has been a longstanding issue within the Queensland public sector. For that reason, improper access to and disclosure of confidential information, and the associated corruption risks, has been an area of focus for the Crime and Corruption Commission (CCC) since 2016.

As part of its function to reduce the incidence of corruption in the public sector, the CCC is now undertaking a public examination, to be known as Operation Impala, of this area of significant corruption risk. Operation Impala will involve public hearings and a final report to be tabled in Parliament.

This paper sets out the detailed background to Operation Impala and invites public submissions on a range of questions.

Why is the CCC examining this area?

Each year the CCC examines high risk areas of concern in relation to corrupt conduct in the public sector. In 2016, one of the CCC's areas of focus was the improper release of information by police. The following year the CCC expanded this to include the misuse of confidential information across the entire public sector. Misuse of confidential information within the public sector continues to be an area of focus for the CCC throughout 2019 and 2020.

Different agencies across the Queensland public sector have information of different detail and sensitivity. QPS and the Department of Health (DoH) have arguably the most sensitive information holdings about individuals. The Queensland public sector has access to a range of confidential information of varying degrees of sensitivity and value. Members of the public rightly have an expectation of privacy, which is reflected in various legislative controls, obligations on employees, codes of conduct, and policies and procedures.

Aggregated corruption complaints data suggests that complaints in relation to misuse of confidential information have generally declined in recent years. A closer analysis identifies that although complaints regarding QPS have declined since 2015, there has been an increase in complaints in relation to other agencies (and most notably, within the DoH). It may be no coincidence that an organisational focus in recent times by the QPS on the misuse of information has contributed to a reduction in complaints. This highlights the value of a concerted focus on this area.

The focus of Operation Impala is to look at risks when employees improperly access or disclose confidential information in the public sector through a close study of the nominated agencies with carriage of the most sensitive personal information, namely the QPS, the Department of Education (DoE), Queensland Corrective Services (QCS), the DoH, and the Department of Transport and Main Roads (DTMR).

Operation Impala will explore the different risks in the various agencies, what systems and processes are employed to mitigate those risks, and what lessons the public sector as a whole can take from the various

successes and areas for improvement.

Definition of "confidential information"

For the purposes of Operation Impala, the CCC will focus on confidential information held by agencies which is of a personal nature held by these agencies about members of the public. It is not intended that this examination will look at commercially sensitive information such as contracts or tender documents. While this type of confidential information can also be a target for corrupt actors (employees) within agencies, it is not the focus of Operation Impala.

Agencies to be examined

Queensland Police Service

The QPS performs a variety of diverse functions which are outlined in section 2.3 of the *Police Service Administration Act 1990* (PSA). Some of those functions include:

- The preservation of peace and good order in the community;
- The prevention of crime;
- The detection of offenders and bringing of offenders to justice and
- The upholding of the law generally.

Essential to the performance of the QPS's functions is the collection and examination of a wide variety of information from various sources. A valuable source of information for the QPS is the public. It is essential that the public have confidence that the officers to whom this information is entrusted will keep and use it for appropriate purposes. This has been acknowledged and acted upon by the then Police Commissioner, Ian Stewart, who issued directions to all staff in March 2016 and December 2018 on unlawful and inappropriate access to QPS information systems. The Commissioner warned staff that if information is accessed that is not connected to a purpose of one's duty, the conduct will be considered misconduct. Also, legislation provides that QPS officers and staff members are prohibited from disclosing information if that information has been obtained as a result of their employment with the QPS[1].

The total number of full-time equivalent staff in the QPS was 15,163.04 as at 30 June 2018 spread across five establishments.[2]

The QPS undertakes a range of activities designed to promote ethical behaviour, discipline and professional practice to ensure members of the public have confidence in, and respect for, the police[3]. The QPS Management Support Manual (MSM) is an illustration of one such measure. The MSM provides guidance and instruction in management support aspects of policing[4]. Chapter 5 provides guidelines relating to Information Management and Privacy, which includes the application of Information Privacy Principles contained in Schedule 3 of the *Information Privacy Act 2009* (IPA). The guidelines address general safeguards to be observed when dealing with personal information and circumstances where disclosure of personal information is authorised.

---

[1] PSA, s. 10.1.

[2] According to QPS 2017-18 Annual Report available at <https://www.police.qld.gov.au/sites/default/files/2018-12/QPS-Annual-Report-2017-18.pdf>

[3] According to QPS 2017-18 Annual Report, available at <https://www.police.qld.gov.au/queensland-police-service-corporate-documents/reports-and-publications/annual-report-2017-2018>

[4] Available from the QPS website, <https://www.police.qld.gov.au/queensland-police-service-corporate-documents/operational-policies/management-support-manual>

Queensland Corrective Services

QCS is governed by the *Corrective Services Act* 2006 (CSA), which provides that the purpose of corrective services is community safety and crime prevention through the humane containment, supervision and rehabilitation of offenders[5]. QCS consists of nearly 4,900 full time equivalent staff.[6] The QCS 2017-18 Annual Report provides that 8,800 prisoners are in custody and correctional facilities consist of 11 high security prisons, 6 low security prisons, and 13 work camps. Fourteen prisons are outlined under Schedule 1 of the *Corrective Services Regulation* 2017.

In the course of their duties, corrective services officers frequently have to deal with confidential information. At times, this will involve collaboration with other Queensland government departments. For example, corrective services officers are required to consider the individual risks and needs of prisoners and may make referrals to the DoH staff regarding welfare, rehabilitation and community reintegration needs of prisoners, including at-risk management, medical needs and family welfare arrangements[7]. This information can include details regarding prisoner criminal history, family contacts, next of kin and health records. This presents a significant corruption risk for QCS, particularly from the potential for misuse of such confidential information.

The CCC's Taskforce Flaxton highlighted that the power of knowledge is intensified in custodial settings by the diverse legislated authority that correctional staff hold and the vulnerabilities of the prisoner population[8]. In this context, the access and release of information can have severe consequences for the safety and security of prisoners as well as the overall correctional facility. For example, staff accessing and releasing information about a prisoner's offence, such as sex offences involving children, can directly affect the safety of that prisoner. Staff having access to confidential information also makes them a target for manipulation or coercion by prisoners or outside associates of prisoners. This has the potential to foster other corruption risks such as inappropriate relationships. Evidence given by Mark Halsey in the CCC's Taskforce Flaxton hearing addressed this corruption risk[9]:

> "… all forms of correctional corruption start with one inappropriate relationship or another, and that includes the misuse of information, because that officer is obviously getting it for someone for some purpose and that relationship should not exist for that purpose…"

The CSA recognises that every member of society has certain basic human entitlements, and that, for this reason, an offender's entitlements, other than those that are necessarily diminished because of imprisonment or another court sentence, should be safeguarded[10]. Numerous safeguards are provided for explicitly within legislation and through QCS custodial operations practice directives. For example, under the "Daily Operations- Case Management" Practice Directive, corrective services officers are required to promote the safety, security and good order of a corrective services facility through effective prisoner management[11].

The QCS Custodial Operations Practice Directive "Confidential Information- Disclosure of Confidential Information" provides that Inspectors and staff delegated by the Chief Executive to undertake investigations in relation to their role and functions have the power to inspect and copy any document kept at a corrective services facility that is relevant to the performance of their work[12]. Documents related to legal professional privilege are not permitted to be examined. Prohibition on disclosure of confidential information is enshrined

---

[5] CSA, s. 3(1).

[6] Available at <https://www.data.qld.gov.au/dataset/20174-18-queensland-corrective-services-annual-report>

[7] According to the Custodial Directive, Daily Operations- Case Management, available at <https://publications.qld.gov.au/dataset/qcs-procedures/resource/c39cafe1-5a7f-414d-9784-de111a668433>

[8] Details are available from the CCC website, <http://www.ccc.qld.gov.au/corruption/taskforce-flaxton>

[9] Evidence given by Professor Mark Halsey on 28 August 2018, p. 25 Details available from the CCC website, <http://www.ccc.qld.gov.au/corruption/taskforce-flaxton/transcripts/transcripts-taskforce-flaxton#day14>

[10] CSA, s. 3(2).

[11] Available at <https://publications.qld.gov.au/dataset/qcs-procedures/resource/c39cafe1-5a7f-414d-9784-de111a668433>

[12] Available at < https://publications.qld.gov.au/dataset/qcs-procedures/resource/69a90be3-d658-434c-bc46-e58c5e3553e3>

in section 341 of the CSA, which states that an "informed person" must not disclose confidential information acquired by the informed person as a result of the performance of a function under the CSA[13], without a permitted reason[14].

Department of Education

The DoE is responsible for the administration of the *Education (General Provisions) Act* 2006 (EGPA). The objects of the EGPA are outlined in section 5 of the EGPA.

The DoE consists of 72,341 staff, 57,038 of which are teachers[15]. The DoE is split into five divisions, namely, the Office of Industrial Relations, Policy, Performance and Planning, State Schools, Early Childhood and Community Engagement, and Corporate Services. The Office of Industrial Relations and the Policy branch of the DoE are not within the scope of operation Impala.

In the performance of their functions under the EGPA, DoE employees hold a special position of trust arising from the nature of their work. DoE employees exercise powers that have a significant impact on the lives of students and consequently there is a community expectation that these powers will be properly and prudently used[16]. The DoE is required to access and store a significant amount of personal information. This information can include information about both employees and students. For students, this can include, for example, health and medical conditions, report cards and disciplinary documents.

The EGPA requires that school staff members must give a written report of reasonable suspicions of suspected child abuse and neglect regardless of whether QPS are already aware of the matter[17]. All documents related to student protection concerns are to be stored in a 'secure location' or *OneSchool*, an automated system in all Queensland state schools which provides teachers, administrators and principals with secure, easy access to information about students, curriculum, assessment and progress reporting, school facilities and school finance[18] Unauthorised access to such information is a significant risk factor for both the relevant students and employees.

The DoE provides various controls over its data, such as the Information *Standards and Guidelines,* February 2016 Standard of Practice[19]. Also, the EGPA requires that any person that has been a public service employee in the department, who in their capacity has gained or has access to personal information about a State school student, must not make a record of the information, use the information or disclose the information to anyone else, other than for a reason set out in subsection 4[20]. This provision is supported by the DoE's "Appropriate and ethical use of public resources" policy[21], which ensures "that all officers are accountable for the departmental resources that they use, and that resource use is publicly defensible and clearly provides improved outcomes for the department's customers of the State as a whole". Additionally, the DoE has implemented an "Information Security Policy" on 20 November 2018 which aims to protect information against unauthorised disclosure, access or use, loss or compromise, or a breach of privacy[22].

---

[13] CSA 2006 s 341(2)

[14] CSA 2006 s 341(3)

[15] According to the DoE 2017-18 Annual Report, ,available at <https://qed.qld.gov.au/det-publications/reports/Documents/annual-report/17-18/annual-report-2017-2018.pdf>

[16] According to the DoE Standard of Practice, February 2016, available at <https://qed.qldgov.au/workfordet/induction/det/inductionprogramsandresources/Documents/code-of-conduct-standard-of-practice.pdf>

[17] According to the DoE Procedure- Student Protection available at <http://ppr.det.qld.gov.au/education/community/Procedure%20Attachments/Student%20Protection/student-protection.pdf>

[18] According to the DoE Annual Report 2017-18, available at <https://qed.qld.gov.au/det-publications/reports/Documents/annual-report/17-18/annual-report-2017-2018.pdf>

[19] Available at <https://qed.qld.gov.au/workfordet/induction/det/inductionprogramsandresources/Documents/code-of-conduct-standard-of-practice.pdf>

[20] EGPA 2006 s 426

[21] Available at <http://ppr.det.qld.gov.au/pif/policies/Documents/appropriate-and-ethical-use-of-public-resources.pdf>

[22] Available at <http://ppr.det.qld.gov.au/pif/policies/Documents/Information%20Security%20Policy.pdf>

Department of Health

The DoH, under the *Hospital and Health Boards Act 2011* (HHBA) is responsible for the overall management of the Queensland public health system[23]. This responsibility is carried out by the DoH, in conjunction with 16 Hospital and Health Services (HHSs). The object of the HHBA is to establish a public sector health system that delivers high quality hospital and other health services in Queensland having regard to the principles and objectives of the national health system[24]. Among other reasons, the object is achieved by strengthening local decision-making and accountability[25], and providing for State-wide health system management including health system planning, coordination and standard setting[26].

Part 7 of the HHBA stipulates specific confidentiality requirements for "designated persons" and "prescribed health practitioners"[27]. That Part also sets out the duty of confidentiality and exceptions that permit the disclosure of confidential information by these persons.

DoH employed 87,819 full-time equivalent (FTE) staff at the end of 2017-18[28]; 11,892 FTE staff were employed by and worked in the Department, including 4527 FTE staff in the Queensland Ambulance Service, 4,240 FTE staff in Health Support Queensland, and 1,324 FTE staff in eHealth Queensland[29].

HHSs are statutory bodies and are the principal providers of public sector health services[30]. The public sector health system is comprised of the HHSs and the department[31]. The overall management of the public sector health system is the responsibility of the department, through the chief executive (the system manager role)[32]. Among others, the chief executive is responsible for monitoring HHSs performance and issuing binding health service directives to HHSs[33]. Safeguards are provided to protect the confidentiality of information that identifies persons who have received public sector health services[34]. When performing a function or exercising a power under the Act, the best interests of users of public sector health services should be the main consideration in all decisions and actions[35].

When members of the public attend a health facility, a record is made that contains the person's name, address and contact details, nature of the problem, family history, diagnosis and treatment, test results, and Medicare and other Commonwealth benefit card details[36]. Updated information is added to each person's record upon attendance. Failure to properly safeguard this information poses a risk to both the safety and privacy of the person.

Confidentiality requirements are further supported by the DoH Use of Information and Communications Technology (ICT) Services, Standard QH-IMP-032:2016 (the Standard) Clause 3.2.4 places an obligation on "all authorised users" to ensure they only access information that is reasonably required for and consistent with

[23] According to the DoH 2017-18 Annual Report, available at <https://www.health.qld.gov.au/__data/assets/pdf_file/0031/728374/doh-annual-report-2017-2018.pdf>,
[24] HHBA, s. 5(1).
[25] HHBA, s. 5(2)(a).
[26] HHBA, s. 5 (2)(b).
[27] HHBA, ss. 142 & 142A.
[28] Department of Health 2017-18 annual report, <https://www.health.qld.gov.au/__data/assets/pdf_file/0031/728374/doh-annual-report-2017-2018.pdf>
[29] According to the DoH 2017-18 Annual Report
[30] HHBA, s.7(1).
[31] HHBA s.8(1).
[32] HHBA s.8(2).
[33] HHBA s.8(3).
[34] HHBA s.12.
[35] HHBA s.13.(1)(a).
[36] Details are available from the Queensland Health website, <https://www.health.qld.gov.au/system-governance/records-privacy/health-personal>

the performance of their role and as approved by their line manager or supervisor[37]. The Standard outlines situations which would constitute unauthorised use, such as accessing information not directly related to an authorised user's duties, and searching health information on behalf of an acquaintance or merely out of curiosity.

The DoH's privacy plan sets out details of the types of personal information held, and how the information is dealt with in accordance with both the IPA and the HHBA[38]. This plan refers to the DoH and the HHS's collectively as "Queensland Health". The plan defines personal information as any information or opinion about an identifiable living individual.

Gold Coast Hospital and Health Service

Gold Coast Hospital and Health Service (GC HHS) was established under the HHBA on 1 July 2012[39]. GC HHS's main function is to deliver the hospital services, teaching, research and other services stated in the service agreement for the Service[40]. GC HHS's workforce consists of 9,522 staff, 7,899 of which are FTE[41]. GC HHS delivers a broad range of secondary and tertiary health services from three hospitals, 13 community located facilities, plus two major Allied Health Precincts at Southport and Robina[42].

As with the DoH, the GC HHS is bound by Part 7 of the HHBA. This is stipulated in the GC HHS Privacy Plan, which states that "Gold Coast Health takes the necessary steps to protect personal information against loss, unauthorised access, use, modification or disclosure, and against other misuse"[43]. These necessary steps include password protection for accessing the GC HHS electronic systems.

Mackay Hospital and Health Service

Mackay Hospital and Health Service (Mackay HHS) was established on 1 July 2012, and its responsibilities are set out in the HHBA[44]. Mackay HHS operates according to the service agreement with the DoH, which outlines the services to be provided, funding arrangements, and performance indicators and targets. Mackay HHS is responsible for the delivery of public hospital and health services to an estimated resident population of 182,000. As at 30 June 2018, Mackay HHS had the full-time equivalent of 1,680.29 permanent staff, 535.37 temporary staff and 68.60 casual staff[45].

As with the DoH and the GC HHS, Mackay HHS is bound by Part 7 of the HHBA.

Department of Transport and Main Roads

DTMR discharges its statutory obligations under 23 Acts[46], including the *Transport Infrastructure Act* 1994 and the *Transport Planning and Coordination Act* 1994. The overall object of both of these Acts is to provide a regime that allows for and encourages effective integrated planning and efficient management of a system of transport infrastructure[47]. Both Acts contain provisions regarding confidentiality. The *Transport*

---

[37] Available at <https://www.health.qld.gov.au/__data/assets/pdf_file/0030/397308/qh-imp-032-1.pdf>
[38] Available at <https://www.health.qld.gov.au/global/privacy>
[39] According to GC HHS 2017-18 Annual Report, available at <https://www.publications.qld.gov.au/dataset/4b0d2fc9-81a7-4ced-8025-dc83da1391aa/resource/c576ed8c-3782-4ee8-a17c-2994762e3310/download/gch146annualreport17-18ls-v19-web-00.pdf>
[40] HHBA Act s. 19(1)
[41] According to the GC HHS 2017-18 Annual Report
[42] According to the GC HHS 2017-18 Annual Report
[43] Available at, <https://www.publications.qld.gov.au/dataset/gold-coast-hospital-and-health-service-plans/resource/3fb7332e-edc2-47bc-affa-0a9503286c1f>
[44] According to the Mackay HHS 2017-18 Annual Report, available at <http://www.mackay.health.qld.gov.au/about-us/publications/>
[45] According to the Mackay HHS 2017-18 Annual Report.
[46] According to the DTMR 2017-18 Annual Report 2017-18.
[47] *Transport Infrastructure Act 1994* s. 2(1)

Infrastructure Act 1994 provides a person must not, intentionally or recklessly, disclose, allow access to, record or use personal information[48]. The *Transport Planning and Coordination Act* 1994 provides that a person must not disclose, record or use information gained through involvement in the administration of the Act, unless authorised under the Act[49].

The DTMR is comprised of 7,180 full-time equivalent employees as of 30 June 2018 and 79 occupational groups spread across trade, professional, technical and administrative disciplines throughout Queensland[50]. DTMR plan, manage and deliver Queensland's integrated transport environment to achieve sustainable transport solutions for road, rail, air and sea.

DTMR's legislative obligations are reflected in DTMR's Information Privacy Plan, as displayed on DTMR's website[51]. The plan provides a guideline for employees and contractors of the department who deal with personal information in relation to the functions and activities of the department. All employees, contractors and consultants within the department have responsibilities to ensure that the personal information they handle in their everyday duties is managed in accordance with the IPA.

According to DTMR's Information Privacy Plan, DTMR is the largest holder of personal information in the Queensland public sector. The collection of personal information is a central part of many of DTMR's business activities. The personal information can include customer name, address, marital status, licence status and driving and fare evasion offence information. All datasets that hold personal information are audited from time to time by the Right to Information (RTI), Privacy and Complaints Management Team. The objective of these audits is to ascertain across the department whether records of personal information are being collected, stored, used and disclosed in accordance with the Information Privacy Principles (IPP), and to assist in identifying measures that may be taken to reduce the risk brought about by non-compliance with the IPPs.

Protections against improper access or disclosure of confidential information

Legislation that prohibits improper access or disclosure of confidential information

There are a variety of legislative protections designed to ensure confidential and personal information is only used for permitted purposes. Generally legislation that creates a Queensland agency to perform a particular function regulates how that information can be used and disclosed. Some examples of this have been discussed above.

Misuse of information can result in far-reaching consequences for the agencies and employees entrusted to store and protect the data and the members of the public who entrust these entities to deal with their personal information according to the law.

Criminal offences

Improper access or disclosure of confidential information when stored on a 'restricted computer' may render the person liable to a criminal offence under the *Criminal Code* known as computer hacking and misuse.

Section 408E of the *Criminal Code* creates a simple offence for anyone who uses a restricted computer without the consent of the computer's controller. There are also a number of more serious offences where

[48] *Transport Infrastructure Act* 1994 s. 105ZN

[49] *Transport Planning and Coordination Act* 1994 s. 36GA

[50] According to the DTMR 2017-18 Annual Report, available at <https://publications.qld.gov.au/dataset/annual-report-2017-2018-transport-and-main-roads/resource/ac54488a-4807-4cf7-8289-40119e92190e>

[51] Available at <https://www.tmr.qld.gov.au/Help/Privacy>

the person who uses the restricted computer has a particular intention, including the intention to obtain a benefit, when they access the computer.

Use, of a restricted computer, includes accessing or altering any information stored in, or communicating information directly or indirectly to or from, the restricted computer, or causing a virus to become installed on or to otherwise affect the computer.

A **restricted computer** means a computer which requires a particular sequence of electronic impulses to gain access, and for which the controller takes steps to withhold access to the device, or takes steps to restrict access to the device to a person or a class of person authorised by the controller.

Benefit is defined to include a benefit obtained by or delivered to any person. Benefit is defined widely in the *Criminal Code*. Benefit includes anything of benefit to a person whether or not it has any inherent or tangible value, purpose or attribute.

Western Australia has a similar offence established under the *Criminal Code Act Compilation Act 1913*. Section 440A, titled Unlawful use of computer, makes it an offence for a person unlawfully to use a 'restricted-access computer system'[52].

Western Australian courts have considered numerous cases involving computer misuse. This includes the case of *Inglis v Pinch*[53]. The case involved a police constable who unlawfully used the Incident Management System (IMS), a restricted-access computer contrary to section 440A. The information obtained was relevant only to Inglis' own affairs. The information sought by Inglis was information regarding an assault of which he was the victim. Additionally, Inglis accessed information regarding the vehicle registration of his own car. Finally, Inglis accessed information regarding an incident involving trespass and damage which took place at his home. It was not disputed that, on each occasion, Inglis could have obtained the same information through lawful means. Inglis was fined $8,000 for the offences.

There are also a number of other *Criminal Code* offences which apply to public sector employees including abuse of office, and misconduct in relation to public office. Operation Impala will consider these and other legislative provisions and whether they sufficiently protect the public against the misuse of confidential information.

Privacy

Public sector agencies are required to take all reasonable steps to protect and prevent unauthorised access or disclosure of personal information. Without proper safeguards in place, personal information is vulnerable to unauthorised access and disclosure. It also places public sector agencies in jeopardy of breaching the IPA *or Privacy Act 1988 (Cth)* (PA). The IPA requires public sector agencies to take reasonable steps prevent and protect personal information from misuse, loss and unauthorised access through the IPPs. Similarly, the PA requires a number of entities, including health service providers, to take reasonable steps to prevent and protect personal information from misuse, loss and unauthorised access through the National Privacy Principles (NPPs). Failing to comply with the IPPs and NPPs may result in breaches of privacy. This has the potential to erode public confidence and cause reputational damage to the Queensland public sector.

The persistence of misuse of confidential information

In Queensland, the Criminal Justice Commission released a public report in November 2000 in relation to the improper access to and release of confidential information from police computer systems by members of the

[52] *Criminal Code Act Compilation Act* 1913 s. 440A(3)
[53] [2016] WASC 30

QPS. The investigation commenced following the investigation of a number of serious and systemic breaches of confidential information at one police station. However the investigation quickly found a number of similar issues at other police stations across Queensland.

More recently there have been a number of reviews and reports of a variety of types of misuse of information across Australia, including:

VICTORIA: Unauthorised and inappropriate access to and release of information was identified as a corruption risk in the prison setting. Corrections Victoria have increased the auditing of its databases to discourage inappropriate access and to identify security breaches. Prevention strategies include improving staff understanding of integrity risks and improving organisational culture.[54]

WESTERN AUSTRALIA: Technical vulnerabilities in database security have been identified as a corruption risk within a correctional environment. For example, database passwords not set to expire creates a risk that people who are no longer authorised to access systems could still do so. A case study identified that a highly privileged database administrator account was shared by 15 different people including 12 contractors, highlighting the importance of regular password changes. It was also identified that a process of logging and auditing of databases had not been established, meaning that changes could not be traced back to an individual.[55]

Misuse of information in policing

TASMANIA: Report into an investigation by the Integrity Commission relating to unauthorised access of information by Tasmanian police officers in response to information that significant advances in technology have increased the risk of information abuse within the public sector.[56] The investigation involved analysing complaints data and a survey conducted of a sample of current serving police officers. The investigation identified that Tasmania Police procedures were adequate and appropriate although recommendations were made that the organisation should be more prepared to enforce its policies and procedures when investigating misuse of information. The Integrity Commission commended Tasmania Police on the use of ongoing audits of access to information.

Organised crime cultivation of public sector employees

VICTORIA: Organised crime groups are likely to target public sector agencies with access to law enforcement information or large volumes of identity and credit card information. This information can assist organised crime groups to identify opportunities and can facilitate their criminal activity. Public sector agencies involved in the construction, planning and development, prostitution and liquor industries may also face increased risks of targeting by organised crime groups.[57]

Unauthorised access to staff information

WESTERN AUSTRALIA: A case study relating to an employee of the Public Transport Authority (PTA) who accessed confidential staff information, including leave balances, from the computer of another employee who failed to log-out of the staff personnel system after leaving his desk for a period of time. The employee used a USB to download staff information and provided it to a union organiser from the Australian Rail Tram and Bus Authority who used the information during negotiations between the PTA and the union.[58]

---

[54] Independent Broad-Based Anti-Corruption Commission 2017, *Corruption risks associated with the corrections sector*, Victoria
[55] Corruption and Crime Commission 2018, *Report into misconduct risks in WA prisons*, Western Australia
[56] Integrity Commission 2018, *Report of an own-motion investigation into the management of police information in Tasmania Police*, Tasmania
[57] Independent Broad-Based Anti-Corruption Commission 2015, *Organised crime group cultivation of public sector employees*, Victoria
[58] Corruption and Crime Commission 2018, *Report into unauthorised release of confidential information of the Public Transport Authority*, Western Australia

General information regarding misuse of information

NATIONAL: Paper examining the nature and extent of misuse of information and communication technology data in public sector agencies, including through the inappropriate access of information and misuse of email.[59] The paper identifies general trends including the finding that incidents involving the misuse of information were allegedly committed by employees who had been with a public sector agency for four years or more and, in some instances, the employees had evaded detection for a long period of time. It was also identified that those involved in the frauds mostly occupied middle management or advanced level roles and that misuse of information often lead to other types of corrupt activity, including procurement fraud. The research identified that internal oversight was useful in detecting misuse when compared with other methods.

Information management and monitoring

There are a number of agencies in Queensland which regulate or impose obligations on agencies to protect confidential and personal information. These agencies include the:

- Office of the Information Commission Queensland (OIC); and
- Queensland Government Chief Information Officer (QGCIO).

Office of the Information Commissioner Queensland

OIC has responsibility for investigating and reviewing decisions of agencies and Ministers on access to and amendment of information under the *Right to Information Act 2009* (RTI Act) and the IPA. This role includes identifying whether agencies and Ministers have taken all reasonable steps to locate relevant documents, as well as deciding applications for extensions of time to process access applications and applications from non-profit organisations for financial hardship status. It also involves determining whether particular entities are covered by the legislation.

As reflected on the OIC website, the OIC has the responsibility for[60]:

- the management and mediation of privacy complaints against Queensland government agencies;
- responsibility for the accuracy of privacy audits;
- education and training on privacy compliance;
- submissions to enquiries and reviews on privacy-related matters;
- presentations to government and the community and
- functions under the IP Act related to compliance notices, waivers and modifications of privacy principles in the public interest.

Queensland Government Chief Information Officer

QGCIO is part of the Department of Housing and Public Works. QGCIO is responsible for ensuring the government's ICT investments support policy outcomes, are focussed on service delivery to the community, represent good value for money and are reliable[61]. QGCIO provides advice to Queensland Government agencies and executive government on issues such as:

- setting ICT strategy, policies and standards;

[59] Australian Institute of Criminology 2015, Trends and issues in crime and criminal justice No. 470: *Misuse of information and communications technology within the public sector*, Canberra

[60] Available at <https://www.oic.qld.gov.au/about/our-organisation/key-functions>

[61] Details are available from the QGCIO website, accessed 11 September 2019- <https://www.qgcio.qld.gov.au/about-us>

- adopting better practice for ICT investment management;
- identifying and managing risks, including 'over the horizon' risks;
- developing proposals for major whole-of-government investments;
- identifying and managing strategic workforce capability issues;
- improving contract outcomes and
- facilitating strategic relationships with industry partners.

As such, the QGCIO is in position to provide guidance in relation to best practice for systems and standards to protect confidential information from improper use. An example of this is IS18: Information Security Policy which requires Queensland Government departments to implement minimum standards of security to protect data.

The continuum of offending

A number of factors appear to influence police and public sector employees' decisions to improperly access confidential information. However, based on an analysis of data held by the CCC, a large percentage stem from personal interest and are typically for the benefit of themselves or close family and friends. An examination of some recent investigations into corrupt conduction allegations involving misuse of information have identified the following features:

- Inappropriate associations feature prominently in investigations into the unauthorised access and release of information.
- The failure of internal controls to detect and prevent unauthorised accesses coupled with inadequate supervision frequently allows this behaviour to go undetected.
- Misuse of confidential information is an ongoing challenge cross Australian jurisdictions, illustrated by a low rate of criminal prosecutions against police or public sector employees. This may be either due to a lack of knowledge regarding the ability to charge criminally or due to cultural attitudes about the seriousness of such conduct.

Areas of concern

Corruption and corruption risks

Identified agencies (QPS, DoH, QCS, DoH, GC HHS, Mackay HHS, and DTMR) are required to collect, store and use private information to discharge their functions. Employees of the identified agencies are in a significant position of trust on behalf of the Queensland public to access and use this information only in the performance of their agencies' functions. Improperly accessing confidential information represents a breach of that trust, which creates a significant corruption risk for the identified agencies. The consequences of misuse of the information is amplified in circumstances where the employee improperly disseminates that information to a third party. Once information is released from an agency without proper authority, there is no control over it or how far that dissemination will run. Improperly accessing and disclosing such information can damage an individual and organisation's reputation, provide unfair advantages to recipients of the information and can increase the likelihood of other corruption risks. Even if the original release was not intended to cause harm, the agency or employee cannot know who may come to possess it or how they might use it.

A number of factors influence a public sector employee's decision to access confidential information. However, the majority stem from personal interest and are typically for the benefit of themselves or their associates. The failure of internal controls to detect and prevent unauthorised access coupled with inadequate supervision frequently allows this behaviour to go undetected. This can lead to systemic,

repeated efforts to improperly access personal information, which significantly increases the risk of corruption. Additionally, the observations from the CCC's own investigations are that computer misuse is rarely a stand-alone issue and is often linked to other, more serious corrupt conduct.

This risk is not limited to the identified agencies, or the Queensland public sector. It is applicable to all government agencies, both nationally and internationally. The risk is also not a new one. As early as 1997, numerous police services were identifying problems relating to improper and unlawful use of the system "RACS", and these formed a common theme amongst Royal Commissions in Australia.

Some of the corruption risks which have been identified by the CCC which are linked to inappropriate access to and release of information include the following areas.

Inappropriate associations

Inappropriate associations are a prevalent theme among matters of this type under investigation. Investigations into unauthorised access and/or the release of information almost invariably involve an inappropriate association. Inappropriate associations provide motivation and/or present opportunities for various types of corruption. Not only can police or public servants take advantage of such associations, criminals may also seek to 'cultivate' these employees for their own benefit. Once the relationship is established, the 'slippery slope' progression from low-level favours and release of information to actively concealing and engaging in higher order criminality is difficult to stop.

Inappropriate associations – especially when they are long-established – are often characterised by trust and loyalty. They can include former school groups, participation in similar lifestyles or activities (including body-building or gym cultures), secondary employment, or communities based on shared ethnicity or identity. The trust that flows from these associations, however, can be manipulated to create misplaced loyalty, whereby an officer may abrogate his or her professional and public interest responsibilities in favour of honouring perceived obligations to individuals or groups (a conflict of obligation) which can often extend to those involved in organised crime.

Organisational culture

Research conducted by the CCC indicates that the positive effects of police ethical training erode after recruits are exposed to the operational policing environment. Survey results show the transition from the academy environment to the operational policing environment can have a negative effect on police values, knowledge, perceptions, and intention to report corruption. That is, the positive effects of training appear to 'wear off' once officers are sworn-in and commence operational duties (CCC 2013).

The common perception that personally motivated checks are a 'normal' practice and that 'everybody does it' can create a culture of tolerance and acceptance towards personally motivated checks. This can lead to confusion about what is and is not an improper use and release of confidential information.

Low risk and difficulty of detection

In its simplest terms the general public expect confidential information which is lawfully obtained by any government department to be secured correctly and only accessed in appropriate circumstances[62]. The WA

[62] 2016 IPAA WA Public Sector Research Day- Showcasing public sector related research in Western Australia- WA Police Professional Standards Portfolio- Information Integrity Pathway/Roadmap for Reform- 1st September 2016

Police Professional Standards Portfolio provided a paper which explored problems relating to improper use of personal information in 2016[63]. Appropriate circumstances should equate to access for a purpose which directly relates to one's work area or function. What actually constitutes a direct relationship to a member's work area or function can be difficult to define and therefore can make auditing a challenging task.

Employees regularly access, use and share confidential and sensitive information in the performance of their duties. This information is needed to facilitate a variety of decisions both with the employee's own agency and functions performed by other agencies. Ensuring employees who need access to information to perform their duties, but restricting access to those who have no legitimate need to access the information, can be a difficult balance and impose significant requirements on an agency's system to ensure operational and service demands are balanced against the need to maintain confidence.

Investigations conducted by the CCC have previously identified that a number of Queensland government departments do not have computer systems that are auditable. Inquiries during CCC investigations have also identified that few agencies undertake proactive steps, such as audits, to identify inappropriate access to confidential information.

The sharing of passwords between employees has also been highlighted as an area of concern across several jurisdictions. Both Independent Commission Against Corruption and the Victoria Police Service have identified instances involving employees sharing passwords to save time logging into systems. CCC investigations have also identified a trend of police and public sector employees arranging for colleagues to conduct checks on their behalf. This hinders the ability to track the access to and release of information.

Call for public submissions

To support its examination of the issue, the CCC is calling for public submissions. The CCC invites your views by way of written feedback in response to this issues paper. You are welcome to provide comments on any or all of the key questions identified in the paper, and any other areas that you think are relevant to the aims of the inquiry.

Submissions are due by COB **9 October 2019**.

Please refer to the Appendix for more information on how to make a submission and how the CCC will handle the submissions it receives.

[63] Available at <http://www.wa.ipaa.org.au/content/docs/2016/Research-Day/Papers/S3.1_Do_government_organisations.pdf>

Key questions for stakeholders and community members

The CCC is interested in hearing from a range of people who have had involvement with the identified agencies in relation to the management of confidential information or improper access to or disclosure of confidential information. These include current and former employees, and representatives of government and non-government agencies with an interest in maintaining privacy of confidential information and dealing with breaches of privacy. The CCC considers it important to hear views from a diverse range of groups to inform the public hearing.

To help guide your submission, the following questions are provided. Please note your submission does not need to address every question. We encourage interested parties to provide information in response to matters raised in this issues paper as relevant to them. This may include other matters not raised in this issues paper.

Risk and Impact

1. What types of confidential information held by the identified agencies are the most valuable and/or at the highest risk of being improperly accessed by employees?
    a. How may each type of confidential information by exploited by 'bad actors'?
    b. What are the risks in access and disclosure of each type of information?
    c. What are the motivators for employees to improperly access and/or disclosure confidential information?
2. What impact does improper access to confidential information have on:
    a. The ability for agencies to perform their functions
    b. People whose data is improperly accessed.

Management

3. How are different types of confidential information managed by the identified agencies?
4. How is misuse and improper access detected by the agencies?
5. Does each identified agency monitor the ongoing effectiveness of the information security governance activity?

Enablers and Facilitators

6. In relation to complaints received by the CCC (see page 4), what factors may be contributing to the increase in corrupt conduct allegations regarding misuse of confidential information over the previous four years?
    a. Do these factors create a corruption risk or facilitate other corruption risks?
    b. Are these factors systemic or symptomatic of idiosyncrasies with the particular agency?

7. What features of the legislative, policy and operational environment within each agency may enable corrupt conduct to occur in relation to improper access and disclosure of confidential information?
    a. Are there unique challenges presented in an agency in relation to the handling and storage of confidential information?
    b. What are the deficiencies within each agency's systems that facilitate information misuse?
    c. Is there effective training to encourage ethical behaviours and awareness within agencies?
    d. Are officers aware about what constitutes improper access to information?
    e. Are employees of identified agencies deterred from accessing personal information without authorisation?
    f. Do employees feel entitled to view all personal information given their employment within an identified agency?

Prevention and Detection

8. What steps can agencies take to protect themselves and discourage employees from improperly accessing information?
9. Are prevention measures integrated into information systems?
10. Is it difficult to detect improper access to information?
11. How are changes in technology making it easier or more difficult to ensure confidential information is not improperly accessed or disclosed?

Legislative Framework and Reforms

12. What other reforms can help prevent, detect and deal with corrupt conduct relating to misuse of information within the five identified agencies, and lessons that can be extrapolated to the broader Queensland public sector
    a. What are the barriers to successfully implementing these reforms and how could these barriers be removed or mitigated?
13. Are there adequate legislative protections and remedies for people who have had their privacy breached by employees in public sector agencies?

Other Issues

14. Are there any other issues that are relevant to understanding improper access and disclosure of confidential information in the identified agencies or how to address these risks?

Appendix: Making a submission

Invitation for public submissions

We would like to hear your views and experiences. To make a submission to the CCC:

- Review the "Key questions for stakeholders and community members" (see page 16, 'Key questions for stakeholders and community members')
- Ensure that your submission clearly addresses one or more of these key questions. If it does not, the CCC may decide not to accept your submission. Your submission does not need to address every question.
- Clearly identify how you would like the CCC to treat your submission, based on the following options:
  - **Public submission** — the CCC may refer to or quote directly from the submission, and name the source of the submission, in relevant publications. Public submissions may be published on the CCC website.
  - **Anonymous submission** — the CCC may refer to or quote directly from the submission in relevant publications but will not identify its source. Anonymous submissions, with all identifying information removed, may be published on the CCC website.
  - **Confidential submission** — the CCC will not quote or refer to the submission in any report or publication. Confidential submissions will not be published on the CCC website.

If there is no clear selection of one of these options, the CCC will regard your document as a public submission. Note that the CCC will not make public any submission or, where practicable, any part of a submission that:

- contains allegations of corrupt conduct or police misconduct
- contains identifying information about a third party (the names of people, businesses or organisations), offensive material (including abusive or threatening behaviour), defamatory material, or links to other websites
- does not address issues relevant to the review
- infringes the intellectual property rights of others
- promotes commercial interests.

- Send your submission to the CCC **by COB 9 October 2019 by** one of the following methods.

Email: operationimpala@ccc.qld.gov.au

Post: Operation Impala
Crime and Corruption Commission
GPO Box 3123
Brisbane Qld 4001

Fax: 07 3360 6333

Allegations of corrupt conduct

The submission process is not the correct avenue for reporting suspected corrupt conduct to the CCC.

Should you wish to do this, please see the CCC's website for further information: www.ccc.qld.gov.au

The CCC will forward any submissions containing allegations of corrupt conduct to its complaints area for assessment.

Privacy statement

No submission marked as confidential will be published on the CCC's website. However, any submission may be subject to disclosure under the Right to Information Act 2009, and applications to access submissions will be determined in accordance with that Act.

Submissions are due by COB 9 October 2019.

The CCC may not consider late submissions

Crime and Corruption Commission
QUEENSLAND

Contact details

Crime and Corruption Commission
GPO Box 3123, Brisbane QLD 4001

Level 2, North Tower Green Square
515 St Pauls Terrace,
Fortitude Valley QLD 4006

07 3360 6060 or
Toll-free 1800 061 611
(in Queensland outside Brisbane)

07 3360 6333

More information

www.ccc.qld.gov.au

mailbox@ccc.qld.gov.au

@CCC_QLD

CrimeandCorruptionCommission

CCC email updates
www.ccc.qld.gov.au/subscribe