Submission by the

Office of the Information Commissioner

CRIME AND CORRUPTION COMMISSION

TASKFORCE FLAXTON – AN EXAMINATION OF CORRUPTION AND CORRUPTION RISKS IN QUEENSLAND CORRECTIVE SERVICES FACILITIES

April 2018

The Office of the Information Commissioner (OIC) is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government. The Crime and Corruption Commission (CCC) is welcome to treat this as a public submission.

The statutory functions of the OIC under the *Right to Information Act 2009* (Qld) (RTI Act) and the *Information Privacy Act 2009* (Qld) (IP Act) include commenting on issues relating to the administration of right to information and privacy in the Queensland public sector environment. The OIC forms part of the integrity and accountability framework in Queensland, working alongside the Integrity Commissioner, Auditor-General, the Ombudsman, and the CCC to maintain public confidence in Queensland's government institutions.

The OIC welcomes the opportunity to contribute to Taskforce Flaxton's examination of corruption and corruption risks in Queensland corrective services facilities. The OIC's submission will cover –

i. a contextual overview of the nature of OIC's work related to corrective services, and
ii. responses addressing specific questions posed in the Issues paper.

i. The nature of the OIC's work related to corrective services

OIC's statutory functions under the RTI and IP Act include:

- external review of decisions of agencies and Ministers on applications for access to, and amendment of, personal information under the IP Act
- external review of agencies and Ministers' decisions on access to information under the RTI Act
- handling complaints about an agency's breach of privacy principles relating to an individual's personal information under the IP Act
- assisting agencies to achieve compliance with privacy principles[1]
- providing information and assistance to the community and agencies through authoritative online resources and the Enquiries Service
- delivering broad and targeted training and awareness raising activities, and
- auditing and reporting on agencies' RTI and IP performance and practices.

If an applicant is not satisfied with the decision made by the agency, either on the original RTI or IP application or at internal review, or the agency did not make a decision within the required timeframe, an applicant can apply to have the decision externally reviewed by OIC.

[1] This is a joint responsibility with the Queensland Government Chief Information Officer and covers agencies' steps to reasonably secure data, which is a key risk. Agencies have a responsibility to keep data secure under Information Privacy Principle 4 and National Privacy Principle 4 in the IP Act, and Queensland Government Departments are obliged under the *Financial Accountability Act 2009* to comply with Information Standard 18.

The number of external reviews equates to around 3-4% of all access and amendment applications made to agencies under the RTI and IP Acts across the state[2].

With respect to interactions with prisoners, since the RTI and IP Acts came into force in mid-2009, OIC has received approximately –

- 110 applications from prisoners for external review of a decision regarding an application to access or amend personal information under the IP Act
- 10 applications from prisoners for external review of a decision regarding an application to access information under the RTI Act
- three privacy complaints from prisoners under the IP Act, and
- 60 written enquiries from prisoners that were dealt with by the Enquiries Service.

It is worth noting that these figures relate only to applications and complaints made by a prisoner about Queensland Corrective Services, the Department of Justice and Attorney-General and the Department of Community Safety (the three agencies that have been responsible for corrective services since mid-2009). These account for around 3% of external review applications made to the OIC, and less than 1% of privacy complaints made to the OIC. Around 100 further applications or contacts were made by prisoners regarding other government agencies, local councils, hospital and health services and universities.

Generally, prisoners apply for the external review of decisions under the IP Act when they are seeking information about themselves. For example –

- telephone call recordings
- case notes, body-worn camera footage and CCTV
- intelligence information such as parole and probation accommodation risk assessments, home assessments, privileges, and intra- or inter-facility moves
- medical treatment and drug and alcohol testing information, and
- sentencing comments, criminal history and breach history.

Less frequently, external review applications and privacy complaints relating to corrective services are made by facility employees (usually relating to grievance or disciplinary issues) and the media (usually relating to particular incidents, policies or procedures). On a recent occasion, an application was made by a victim of crime seeking information about a prisoner.

[2] This does not include privacy complaints, data for which is reported differently. The Report on the Review of the Right to Information Act 2009 and Information Privacy Act 2009 recommends changes to privacy complaint reporting to address this.

ii. Responses to the Taskforce's key questions

1. *In relation to complaints made to the CCC, what may account for the increase in the number of corrupt conduct allegations received, over the last three years, about:*
    a. *assaults/excessive use of force, and b. the misuse of information?*

In terms of the OIC's insights into corruption allegations, it is important to note the difference between an allegation of corrupt misuse of information made to the CCC, and a privacy complaint made to the OIC. The process triggered by an allegation of corruption focuses on the perpetrator's conduct with potential for criminal or disciplinary action. A privacy complaint to the OIC relates to an agency's breach of the privacy principles in the IP Act, and the process seeks to remedy the harm suffered by a victim of a privacy breach. While the same set of facts could lead to both a corruption allegation and a privacy complaint, the relevant processes and outcomes focus on different elements.

Undoubtedly a range of factors may account for the increase seen by the CCC, such as increased media attention, increasing public awareness of data and cyber risks, and avenues for complaint. Other commentators will be better placed to make observations about likely factors of influence. **The OIC's concern in this regard is that the number of complaints may be the tip of the proverbial iceberg.**

For a privacy complaint to be made, the victim of an alleged breach needs to –

- know the information exists in the first place
- be aware that a breach has occurred
- understand their options for addressing it, and
- have the capacity and resources to avail themselves of these options.

Often however, a victim of an alleged privacy breach may –

- be unaware that the information exists
- be unaware that a breach has occurred (this does not mean there is no harm from a breach)[3]
- be unaware of options for responding to a breach
- lack the capacity or resources to respond to a breach, or
- not be empowered to address a breach due to how that information is being used, e.g. threats, blackmail.

Further, as prisoner complaints are generally made via letter, literacy may impact an individual's ability to progress a complaint.

[3] A current private sector example is the delay in Facebook's notification to its subscribers of data breaches.

2. *What are the most significant corruption risks in Queensland correctional facilities?*
    a. *What are the consequences of this type of corruption for prisoners and how the correctional facility operates?*
    b. *What are the consequences of this type of corruption for the community?*
    c. *How does this type of corruption undermine integrity and public confidence in QCS and engaged service providers?*

Unauthorised access, and unauthorised use or disclosure of sensitive or confidential information are significant corruption risks.

While this is the case for any agency entrusted with sensitive information, the power imbalance between staff and prisoners, as well as the general diminution of privacy in prison settings per se, may exacerbate this risk.

As noted in the CCC Annual Report for 2016-17, the large amount of confidential and sensitive information that public employees use to carry out their duties 'is held in trust for both the individuals concerned and the Queensland community generally. Community members have every right to expect that such information is not being accessed or disclosed to anyone who does not have a legitimate and lawful reason to use it.'[4]

Abuse of this trust, whether wilful or accidental, can have devastating impacts for individuals and diminishes the credibility and integrity of government. Recent examples that have garnered media attention include –

- a Queensland police officer's deliberate accessing of a domestic violence victim's current address and release of this information to her former partner
- a Child Safety correspondence error that saw a mother and her children's whereabouts sent to a dangerous former partner
- a system error that resulted in a domestic violence victim's address being auto-populated into court documents and then released
- the illegal accessing of confidential information by an Australian Tax Office official and release of this information to a family member, and
- inappropriate 'snooping' by South Australian health department staff into the health records of a high profile patient.

[4] Crime and Corruption Commission, 2016-17 Annual Report, page 23

Incidents like these demonstrate that unauthorised access and privacy breaches occur across all sectors. They can lead to: reputational damage to the entities involved; a diminution of trust in government; concern in the community that can lead to reduced use of electronic services and therefore compromise effective service delivery; and potentially dangerous or embarrassing outcomes for individuals whose privacy has been breached.

3. *What factors create a corruption risk or facilitate corruption in Queensland correctional facilities?*
    a. *How do these factors create a corruption risk or facilitate corruption?*
    b. *Are these factors systemic (present across all correctional facilities) or symptomatic of local conditions (that is, factors specific to an individual prison or work camp)?*

Systemic factors creating a corruption risk include inadequate controls over access to information, inadequate security controls for systems, and inadequate record keeping.

Inadequate control, tracking and audit of access to records can increase risk of unauthorised access and use of personal information. Recent External Review applications made to the OIC indicate that there is strong community interest in transparency and accountability around government staff accessing information about individuals, for example applications from individuals for access logs relating to their QPRIME records. Although these records have on occasion been considered exempt from access for formal applications made under the RTI Act[5], they are often sought.

Inadequate record keeping is also a risk. Although the following anecdote relates to an isolated application, it may point to a gap in record keeping practices and prisoners' information rights in corrective service facilities. The application included a request for access to CCTV footage of an assault. However, the footage was apparently not retained. This is believed to have been despite the quick notification of the applicant's intention to make a claim about the assault, and was therefore potentially in contravention of document retention requirements. Although this is an isolated incident in terms of the types of applications made to the OIC, whether failures in such circumstances to retain footage occur more frequently may warrant investigation.

[5] Under schedule 3, section 10(1)(f) of the RTI Act, in some cases, disclosure of these records 'could reasonably be expected to prejudice QPS' lawful methods and procedures'. For example, Kyriakou and Queensland Police Service [2017] QICmr 29 (9 August 2017), page 2.

4. *What legislative, policy or procedural changes could be made to address corruption risks in correctional facilities?*
    a. *What are the barriers to successfully implementing these reforms and how could these barriers be removed or mitigated?*

Practical options to address corruption risks include mandatory data breach notifications, and rigorous tracking and auditing of access to information.

An example of a mandatory data breach notification arrangement is the Federal government's Notifiable Data Breaches (NDB) scheme that commenced on 22 February 2018. It requires entities that are subject to the Commonwealth *Privacy Act 1988* to notify individuals when their personal information is involved in a data breach that is likely to result in serious harm. Relevant authorities must also be notified. This NDB scheme has formalised community expectations for transparency when a data breach occurs. While long term evidence is required to confirm that the NDB scheme will improve accountability, transparency and harm minimisation following a data breach, these outcomes are expected.

The introduction of a comparable arrangement for entities that are subject to Queensland's IP Act would ensure that individuals are made aware of breaches involving their data, and could improve public confidence in the transparency and accountability of entities that hold personal information.

With respect to tracking and auditing access to personal information, rigorous access controls and auditable access logs are vital to ensuring the accountability of government staff with access to sensitive information about individuals. While many existing IT systems do not facilitate comprehensive logging and auditing of every inquiry or access transaction, this function should be considered a priority in upgrades or acquisitions of databases storing personal information. The Federal government's MyHealth Record, which can generate an audit log of who has accessed each medical file, may be an appropriate example of this function.

5. *Are there any other issues that are relevant to understanding corruption risks in Queensland correctional facilities or how to address these risks?*

Neither the number of applications made to the OIC, nor the nature of them, appear to expose a pattern of corruption. However, the absence of a pattern is not evidence of absence of risk. Unauthorised access and use of sensitive information is likely to be occurring at a higher rate than is reported. Open, accountable and transparent government that respects privacy is essential for safeguarding both individual and societal information and privacy rights.

The OIC is available to provide further information or assistance to the Taskforce as required.