Office of the Information Commissioner
Queensland

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

9 October 2019

Operation Impala
Crime and Corruption Commission
GPO Box 3123
BRISBANE QLD 4001

By email: operationimpala@ccc.qld.gov.au

Dear Sir/Madam

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

The Office of the Information Commissioner (**OIC**) welcomes the opportunity to make a submission in response to the questions raised in the Crime and Corruption Commission's issues paper *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* (**issues paper**).

About the OIC

The OIC is an independent statutory body that reports to the Queensland Parliament. We have a statutory role under the *Right to Information Act 2009* (**RTI Act**) and the *Information Privacy Act 2009* (**IP Act**) to facilitate greater and easier access to information held by government agencies. We also assist agencies to understand their obligations under the IP Act to safeguard personal information that they hold.

OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance and compliance with, the RTI Act and the IP Act. Our office reviews agency decisions about access to information, mediates privacy complaints and monitors and reports on agency compliance to Parliament.

Queensland's *Information Privacy Act 2009*

Queensland's IP Act recognises the importance of protecting the personal information of individuals. It creates a right for individuals to access and amend their own personal information and provides rules or 'privacy principles' that govern how Queensland government agencies collect, store, use and disclose personal information. OIC has regulatory oversight of Queensland Government agencies' compliance with requirements under the IP Act.

OIC's submission

OIC's responses to specific questions contained in the issues paper is based on OIC's experiences and the performance of our statutory functions under the RTI Act and IP Act. OIC only receives a small number of privacy complaints each year. For example, in 2018-19 OIC received 98 privacy complaints. Six of these complaints related to unauthorised access (IPP 4 – Storage and security of personal information and NPP 4 – Data security) and OIC accepted three of the six complaints.

The Office of the Information Commissioner is an independent statutory authority.

The statutory functions of the OIC under the *Right to Information Act 2009* (Qld) and *Information Privacy Act 2009* (Qld) include commenting on the administration of right to information and privacy in the Queensland public sector environment.

This submission does not represent the views or opinions of the Queensland Government.

All of the identified agencies completed *10 years on: Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)*.[1]

OIC remains available to assist the CCC with their examination of this issue. OIC's submission is **attached.**

Yours sincerely

Philip Green
Privacy Commissioner

Rachael Rangihaeata
Information Commissioner

[1] Office of the Information Commissioner - Report No. 5 of 2018—19 tabled in Parliament on 13 June 2019.

Risk and Impact

Questions 1, 1(b) and 1(c)

1. The identified agencies hold a broad range of confidential information including personal, financial and commercial information. Data may also be collected that could track individuals' movements and daily activities, such as public transport usage. Types of confidential personal information include:
    - Health and education information
    - Details about contact with the criminal justice system
    - Addresses, dates of birth and phone numbers
    - Driver licence information; and
    - Biometric information.

2. Insights from the Notifiable Data Breach (**NDB**) scheme in the private sector and Commonwealth agencies, legislated in the *Privacy Act 1988* (Cth), shows that, in the reporting period of 1 April 2018 to 31 March 2019, health service providers and finance were the sectors that made the highest number of data breach notifications under the NDB scheme.[1] The Office of the Australian Information Commissioner (**OAIC**) noted that this 'likely reflects the scale of data holdings, volume of processing activities and/or sensitivity of the personal information held by those sectors, as well as those sectors' higher preparedness to report data breaches'.[2]

3. The confidential information of high profile individuals may also be at greater risk of having their personal information accessed unlawfully. For example, it was reported that more than a dozen unauthorised medical staff were caught accessing the confidential records of Cy Walsh after he was arrested over the murder of his father, former Adelaide Crows coach Phil Walsh[3] and a former Queensland Police Sergeant was fined $4000 (with no conviction) after pleading guilty to computer hacking. It was reported that he accessed the QPRIME system on 80 occasions between April and August last year and searched the personal information of a wide range of people, including a high profile sportsperson.[4]

4. The *2017-18 Cyber Security Survey*, conducted by BDO Australia and AusCERT, identified that insider threat actors typically steal their organisations' information for 'personal, financial or ideological reasons'.[5] Insights from the OAIC NDB in the first 12 months showed that 32 percent of all data breaches were the result of theft of paperwork or data storage device, social engineering or impersonation, or an act of a rogue employee or insider threat.[6]

---

[1] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/ at page 13.
[2] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/ at page 13.
[3] https://www.smh.com.au/national/health-staff-caught-spying-on-cy-walshs-medical-records-20160223-gn1shx.html.
[4] https://www.abc.net.au/news/2017-05-03/sergeant-fined-for-accessing-police-details-of-netball-star/8492910.
[5] The 2017–18 Cyber Security Survey, conducted by BDO Australia and AusCERT, cited in Queensland Audit Office Report on *Managing Cyber Security* Risks, Report 3: 2019-20 at page 5.
[6] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf at page 10.

5. While financial and commercially sensitive information (e.g. trade secrets, intellectual property etc.) may be considered the most valuable given the opportunities for financial gain, it is OIC's view that all confidential information is at risk of unlawful access and/or disclosure. For example the current residential address of a victim of domestic violence may hold significant value for an employee seeking to determine the whereabouts of his or her ex-partner.

Questions 2(a) and 2(b)

6. Governments collect and hold vast amounts of confidential information on behalf of its citizens and citizens trust that Governments will protect this information from unauthorised access, use and disclosure. Increasingly, this information is held electronically in large scale holdings, increasing the risks to the agency and the individual of improper access to and disclosure of this information.

7. With regards to personal information, the OAIC Australian Community Attitudes to Privacy Survey (**ACAPS**) found that just over half (58%) of Australians consider state and federal government departments are trustworthy custodians of their personal information[7] and one third (34%) of the community is comfortable with the government sharing their personal information with other government agencies.[8] The ACAPS survey also found that ninety-five per cent of respondents agreed that they should be told if a government agency loses their information.[9]

8. All agencies must protect individuals' personal information. Failure to do so exposes individuals to risk, erodes trust and confidence in government, jeopardises public take up of services, and damages an agency's reputation. The lessons learnt from the roll-out of My Health Record underline the importance of securing the trust and confidence of the user to the success of the scheme. In an environment of declining levels of trust in government, this becomes increasingly important.

9. Unauthorised access to or disclosure of confidential information can have serious consequences for individuals and agencies. For individuals, the potential consequences include, but are not limited to:[10]
    - Reputational damage
    - Harm to physical or mental health
    - Financial loss
    - Identity theft
    - Family violence; and
    - Physical harm or intimidation.

Enablers and Facilitators

Questions 6 and 7, 7(c) and (e)

[7] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey, 2017 at page i.
[8] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey, 2017 at page ii.
[9] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey, 2017, p16.
[10] NSW Department of Communities and Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper* at page 1.

10. Rapid advances in technology have facilitated the ability of agencies to collect large stores of confidential information. This had led to productivity gains, improved efficiencies and streamlined service delivery for many government agencies providing better outcomes for citizens, notably in the delivery of health services and law enforcement. However, this same technology also presents a range of challenges for agencies in ensuring this information is not subject to unauthorised access, use and disclosure.

11. Governments are required to strike an appropriate balance between the public interest in ensuring the effective and proper conduct of government and the protection of confidential information.

12. As noted by the Victorian IBAC, while electronic storage and exchange of information delivers productivity benefits for the work of the public sector,[11] it has also made it 'very easy to disclose information – in terms of time, quantity and sensitivity – and difficult if not impossible to retrieve it'[12]once disclosed.

13. OIC notes there is in existence general awareness training concerning responsibilities of public sector employees to comply with a range of obligations including, for example, the Code of Conduct for the Queensland public service, recording keeping obligations under the *Public Records Act 2002* and the *Public Sector Ethics Act 1994*.

14. All agencies should include training about right to information, information privacy and information security in their mandatory induction process for all employees. Training should be comprehensive, contemporary and tailored to the agency's context.[13]

15. OIC's compliance audits, reviews and surveys have found that 'leadership is critical to an effective right to information and privacy culture'.[14] Higher levels of information management maturity require active engagement across a department. Champions at a senior level must lead this change, demonstrating how the agency values, manages and shares information and data appropriately, and how respective business units contribute. Cultural change requires clear communication of objectives and benefits for stakeholders, including for key Government priorities and services.[15]

16. As such, OIC considers training, cultural change, penalties reflecting the seriousness of unlawful access and disciplinary proceedings are important components of a framework to

---

[11] IBAC Victoria, *Unauthorised access and disclosure of information held by Victoria Police, An analysis of corruption risks and prevention opportunities*, September 2019 at page 5.

[12] Commissioner for Law Enforcement Data and Security, Social Media and Law Enforcement, 2013 at page 44 cited in IBAC Victoria, *Unauthorised access and disclosure of information held by Victoria Police, An analysis of corruption risks and prevention opportunities*, September 2019 at page 5.

[13] Office of the Information Commissioner: Report No. 2 of 2018-19 – *Information Management: Queensland government department maturity* at page 14. OIC published its report *Awareness of privacy obligations: How three Queensland government agencies educate and train their employees about their privacy obligations* on our website. (https://www.oic.qld.gov.au/about/our-organisation/key-functions/compliance-and-audit-reports/audit-of-awareness-of-privacy-obligations)

[14] Office of the Information Commissioner: Report No. 2 of 2018-19 – *Information Management: Queensland government department maturity* at page 1.

[15]Office of the Information Commissioner: Report No. 2 of 2018-19 – *Information Management: Queensland government department maturity* at 2.

deter employees from unlawfully accessing personal information. Some of these are explored in more detail below.

Prevention and Detection

17. In addition to the strategies outlined in paragraph 16, OIC considers that agencies should:
    - limit access to personal information to those staff necessary to enable the agency to carry out its functions[16]
    - implement access security and monitoring controls to ensure personal information is only accessed by authorised persons;[17] and
    - adopt audit logs and audit trails to monitor access by individuals, including both regular users and administrators to indicate when an employee has accessed or viewed material and changed or destroyed material. 'Access monitoring software that provides real time (or close to real time) dynamic review of access activity can also be useful for detecting unauthorised access to personal information'.[18]

18. OIC notes that 'all access and use of the My Health Record system is monitored by the Australian Digital Health Agency Cyber Security Centre'.[19]

19. Project management methodologies and tools should include privacy impact assessments (**PIAs**) as key deliverables during design, development and operation of all agency functions. This is core business for any agency when it is managing personal information. A PIA identifies risk of non-compliance with obligations set out in the IP Act and controls to mitigate that risk, including risks of misuse of confidential information by Queensland public sector employees.

20. Results from OIC's *10 years on: Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)* (**10 years on**) indicate that – just over a quarter of agencies are taking a privacy-by-design approach and embedding PIAs into their project management frameworks. Government departments (around 50%) and HHSs (around 60%) have higher rates of integrating privacy-by-design approaches into their operations. However these practices should be core business for all agencies[20]and are an important component in the protection of privacy.

21. While changes in technology present challenges in ensuring confidential information is not improperly accessed or disclosed, it also offers technological solutions to address this issue. Artificial intelligence and machine learning may provide some of these solutions.

Legislative Framework and Reforms

---

[16] Office of the Australian Information Commissioner, *Guide to securing personal information*, https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/
[17] Office of the Australian Information Commissioner, *Guide to securing personal information*, https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/
[18] Office of the Australian Information Commissioner, *Guide to securing personal information* https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/
[19] https://www.myhealthrecord.gov.au/for-you-your-family/howtos/frequently-asked-questions
[20] Office of the Information Commissioner - Report No. 5 of 2018—19 – *10 years on: Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)* at page 30.

Questions 12 and 12(a)

22. There is in existence a legal and regulatory framework that governs the general disclosure and use of official information by Queensland public sector employees:
    - The *Right to Information Act 2009* and the *Information Privacy Act 2009* require government agencies to make their information available subject to limited exceptions and exemptions. Agencies must also safeguard personal information in accordance with privacy principles for collection, use, disclosure, access, storage, security and disposal of personal information
    - *Code of Conduct for the Queensland Public Service*: specifies the obligation to ensure the appropriate use and disclosure of official information, including confirming that such information cannot be used for personal benefit
    - *Criminal Code Act 1899*: provides a criminal offence for a public official to use information gained in the course of their employment to obtain a dishonest benefit or to cause detriment to another person
    - The Queensland Government Enterprise Architecture requires departments to comply with the information standards, principles and policies. It describes values, beliefs and behaviours for government's management of information; and
    - Legislation specific to the agency may set additional requirements.

23. To date, the extent of misuse of confidential information across public sector agencies is not known. While Queensland Government Departments are required to report information security incidents to the Queensland Government Chief Information Office (**QGCIO**), this reporting requirement only extends to a compromise of ICT systems or cyber security event. In the absence of a mechanism mandating the reporting of unauthorised access to and disclosure of confidential information it is difficult to accurately ascertain the extent of the problem.

24. OIC notes that SA Health committed to report quarterly how many staff have been disciplined for inappropriately accessing patient medical records during the previous three months. SA Health reported that From 1 June 2019 to 31 August 2019, two SA Health staff received reprimands for inappropriately accessing patient records, and two staff received warnings.[21]

25. The Commonwealth Government's NDB Scheme (introduced in February 2018) only applies to federal government agencies. As detailed previously, public expectations as reflected in the ACAPS survey undertaken by the Office of the Australian Information Commissioner, suggest the public expect to be notified that a privacy breach has occurred, particularly if they or their identity are at risk of harm. This also assists individuals affected to manage risk and take steps to mitigate any harm that may flow from the breach.

26. The IP Act does not require agencies to notify affected individuals or the Information Commissioner of a privacy breach. Public sector agencies are encouraged to voluntarily report data breaches to OIC. As noted previously, Queensland Government Departments have obligations to report information security incidents to QGCIO in meeting their security

---

21 https://www.sahealth.sa.gov.au/wps/wcm/connect/public+content/sa+health+internet/about+us/publications+and+resources/reports/privacy+breach+update

incident reporting requirements under the Information security policy (IS18:2018). In 2018-19 OIC received a total of 24 notifications of privacy breaches.[22] This reflects increased agency awareness and public expectations.

27. OIC reports annually on the number of privacy complaints received and the outcome of the information commissioner's dealing with those complaints.[23] Currently, Ministers or agencies are not required to report on the number of privacy complaints received or the outcome of those complaints.[24]

28. A privacy breach occurs when an agency fails to comply with one or more of the privacy principles set out in the IP Act. They can occur inadvertently or maliciously, from human error, a technical issue or a database being hacked. Agencies that collect, use or store personal information should have documented policies in place for managing a privacy breach. The OIC *10 years on* final self-assessment sought information from agencies about their preparation for, and response to, any privacy breach.[25] Agencies were also asked about occurrence, frequency and notification of any breaches. In response to these questions, only 55% of agencies reported having a documented process for managing privacy breaches, and 39% of agencies reported that a privacy breach had occurred. Comments from agencies indicate that awareness of privacy breach risks is increasing and prioritisation of privacy breach mitigation is underway.[26]

29. As noted by the OAIC, 'the requirement to notify individuals of eligible data breaches goes to the core of what should underpin good privacy practice for any entity—transparency and accountability. Being ready to assess and, if appropriate, notify of a data breach provides an opportunity for entities to understand where privacy risks lie within their operations, to address the human and cyber elements that contribute to data breaches and to prevent or minimise harm to individuals and the community….The requirements under the NDB scheme incentivise entities to ensure they have reasonable steps in place to secure personal information'.[27]

30. In response to the Queensland Government's statutory review of the RTI and IP Act in 2016, OIC made a number of recommendations including introduction of a mandatory data breach notification scheme in Queensland and providing the Privacy Commissioner with an 'own motion' power to investigate an act or practice whether or not a complaint has been made. This power would complement our existing audit and evaluation function which is critical to providing Parliament, agencies, the community and OIC with assurance about agencies' legislative compliance and good practice.

---

[22] Office of the Information Commissioner Queensland, 2018-19 Annual Report at page 30.
[23] Section 193(3) *Information Privacy Act 2009*; Section 5(2) *Information Privacy Regulation 2009.*
[24] Recommendation 12 of the Report on the review of the *Right to Information Act 2009* and the *Information Privacy Act 2009* (October 2017)recommended amending the annual reporting requirements under the *Information Privacy Regulation 2009* to require reporting on the numbers of complaints made to agencies, including the outcome of these complaints.
[25] Office of the Information Commissioner - Report No. 5 of 2018—19 – *10 years on: Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)* at page 27.
[26] Office of the Information Commissioner - Report No. 5 of 2018—19 – *10 years on: Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)* at page 27.
[27] https://oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

Question 13

31. It has been the consistent finding of a number of legislative reviews that Australia's privacy regulatory framework does not provide individuals with adequate remedies for invasions of privacy.[28]

32. Recently, the ACCC recommended in its *Digital Platforms Inquiry – Final report* giving individuals a direct right to bring actions and class actions against APP entities in court to seek compensation for an interference with their privacy under the *Privacy Act 1988*.[29] The ACCC's recommendations also include introduction of a statutory tort of serious invasions of privacy (recommendation 19) and higher penalties for breach of the *Privacy Act 1988* (recommendation 16(f)).

33. The IP Act allows an individual to make a complaint about an agency's breach of the privacy principles. If an individual – who need not be a Queensland citizen - considers that a Queensland government agency has failed to comply with its obligations under the privacy principles, they are able to make a formal complaint to the agency in the first instance, and to the OIC if they are not satisfied by the agency response.

34. If an accepted complaint cannot be mediated, the complainant can ask OIC to refer the complaint to the Queensland Civil and Administrative Tribunal (**QCAT**) for its determination and orders. QCAT may make an order restraining the agency from repeating any act or practice, order the agency to carry out certain acts, award compensation to the complainant not exceeding $100,000 and/or make further orders against the agency.[30] Payment of a stated amount is to compensate the complainant for loss or damage suffered by the complainant because of the act or practice complained of, including for any injury to the complainant's feelings or humiliation suffered by the complainant.[31]

35. Since enactment of the IP Act, QCAT has made two awards of financial compensation. In both cases, QCAT made an award of $5,000.[32] OIC notes the matter of *Zil v Queensland Police Service* [2019] QCAT 79 is currently the subject of an appeal.

36. The Queensland *Human Rights Act 2019* protects 23 human rights, including the right to privacy and reputation. The Bill does not provide for a standalone cause of action allowing an aggrieved person to access remedies, including damages, for any contravention of their statutory human rights under the Bill. The Bill does, however introduce a complaints mechanism, allowing individuals to make a complaint about entities performing public sector functions that are acting in a way that is not consistent with human rights, including the right to privacy and reputation.

---

[28] In its 2008 Report, *For Your Information: Australian Privacy Law and Practice*, the ALRC recommended that federal legislation should provide for a statutory cause of action for serious invasions of privacy. The 2016 New South Wales Legislative's Council Inquiry on *Remedies for the serious invasion of privacy in New South Wales* and the Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18* (2010), Ch.7 made similar recommendations.

[29] Recommendation 16(e), Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Final Report, June 2019 at page 35.

[30] Section 178(a) of the IPA.

[31] Section 178(a)(v) of the IPA.

[32] *PB v WorkCover Pty Ltd* [2018] QCAT 138 concerned the collection and disclosure of an individual's medical records by WorkCover in relation to a worker's compensation claim. *RM v Queensland Police Service* [2017] QCAT 71 considered whether an email about the WorkCover claim of a QPS employee breached (IPP) 4,9,10 or 11.

37. OIC notes that on 26 November 2018, the Australian Parliament passed new laws to further strengthen the privacy and security protections within My Health Record, including increased penalties for misuse of information, signifying the seriousness of misuse of a person's health information and the potential for damage to an individual or healthcare provider organisation. Civil fines for inappropriate or unauthorised use will increase to a maximum of $315,000, with criminal penalties including up to 5 years' jail time.[33]

38. It is OIC's view that existing provisions in the IP Act require strengthening to provide adequate remedies for individuals who have had their privacy breached by public sector agencies. As outlined earlier, the damages flowing from unauthorised access to and disclosure of personal information can be significant. Penalty provisions in the broader legislative framework should also reflect the seriousness of unlawful access to and disclosure of personal information.

[33] https://www.myhealthrecord.gov.au/about/legislation-and-governance/penalties-for-misuse-health-information