CCC EXHIBIT

Submission to the Crime and Corruption Commission's Operation Impala

Contents

Acronyms

BORIS – Biometric Offender Reporting Information System

BWC – Body Worn Camera

CCC – Crime and Corruption Commission

COEP – Custodial Officer Entry Program

CSIU – Corrective Services Investigation Unit

DJAG – Department of Justice and Attorney General

DPSOA – *Dangerous Prisoners (Sexual Offenders) Act 2003*

EM - Electronic Monitoring

ETCR – Electronic Transfer of Court Results

GPS – Global Positioning System

HPP – Hardship Partner Portal

ICT – Information and Communication Technology

IOMS – Integrated Offender Management System

IPA – *Information Privacy Act 2009*

ISC – Information Steering Committee

ISMS – Information Security Management System

ISWG – Information Security working Group

JOIDA – *Justice and Other Information Disclosure Act 2008*

MOU – Memorandum of Understanding

PDP – Practitioner Development Program

PSBA – Public Safety Business Agency

PSGC – Professional Standards and Governance Command

QCS – Queensland Corrective Services

QCSIG – QCS Intelligence Group

QGCIO – Queensland Government Chief Information Office

QPS – Queensland Police Service

QPSR – Queensland Parole System Review

QWIC – Queensland Wide Interlinked Courts

RTI – *Right to Information Act 2009*

SCRAM – Suitability Checking, Recording and Monitoring

SPER – State Penalties and Enforcement Registry

TIMS – Total Intelligence Management System

WDO – Work Development Order

Introduction

This paper is Queensland Corrective Services' (QCS) submission to the Queensland Crime and Corruption Commission's (CCC) Operation Impala, an examination of corruption and corruption risks in relation to the improper access to, and disclosure of, confidential information in the Queensland public sector. It contains data and analysis completed and compiled by QCS. This paper does not represent Government policy.

QCS expects the highest integrity from every officer across the agency. Similarly, QCS recognises the Queensland community rightfully expects every public servant to discharge their duties ethically and professionally. The correctional environment comes with its own unique challenges and demands. Similarly the rigorous approach to professional standards of the QCS workforce must be just as demanding.

Commissioner Peter Martin APM and the QCS leadership team are steadfastly committed to ethical conduct and are dedicated to building a mature, corruption resistant, top-tier, public safety agency.

In the wake of Taskforce Flaxton, the Queensland Government has supported QCS to undertake a broad range of reforms to support a robust Organisational Capability division. An organisational restructure has established and resourced a robust Professional Standards and Governance Command (PSGC). Acknowledging some reforms and capability building activity may take months or years to develop, QCS has worked diligently and consistently to commence a range of reforms to build, drive and maintain a mature and corruption resistant culture that promotes disciplined ethical behaviour and professional practice through deterrence, education and system improvements. The PSGC is working closely with the CCC, the Queensland Police Service (QPS) and the Public Service Commission (PSC) to manage, report, investigate and proactively address a range of conduct, misconduct and corrupt or criminal conduct matters.

Operation Impala, following the extensive enquiry into corruption and corruption risks through Taskforce Flaxton, provides QCS with a timely opportunity to update the CCC on how the agency is implementing recommendations from Taskforce Flaxton that relate to the management of confidential information.

This QCS submission seeks to address the fundamental questions raised by the CCC regarding the use and access to confidential information in QCS operations. It provides detail on databases, legislation, agreements, policy and practice relevant to the management of confidential information by QCS to support Operation Impala's objective. Detail on information management systems operated by other public sector agencies that QCS officers' access in the course of their duties is provided for completeness.

QCS recognises the power of knowledge is intensified in corrective services settings by the diverse legislated authority of corrective services officers and the vulnerabilities of the prisoner and offender cohort. This is a significant feature of correctional operations that was examined by the CCC through Taskforce Flaxton. QCS notes that over the last three years to December 2018, allegations received by the CCC about the misuse of information by QCS staff increased significantly.

The Queensland Government has supported in principle the CCC recommendation that the Integrated Offender Management System (IOMS) be replaced and that in the interim, QCS implement remediation strategies to reduce the risk that prisoner information is inappropriately accessed and released (Recommendation 27). The Government also supported further recommendations to commission an independent capability review and identify strategies to address gaps, including in information and communication technology, and review training for custodial staff to address high-risk corruption areas (Recommendations 8 and 14).

In August 2019, the QCS Commissioner launched *Corrections 2030,* a strategic roadmap to provide the foundation to deliver QCS services through safety, excellence, empowerment, respect and accountability. *Corrections 2030* sets out the shared long-term vision to transform QCS into a forward-thinking, top-tier public safety agency.

Corrections 2030 responds to the recommendations of the CCC's Taskforce Flaxton by embedding structural and operational reforms to strengthen QCS' organisational structure; enhance internal and external oversight of correctional centres and build robust integrity and professional standards. This submission discusses the progress made to increase QCS' capability to deliver the oversight, corporate governance and risk management functions associated with a top-tier public safety agency.

QCS is committed to developing a strong and mature corruption-resistant culture. Significant work is already underway with further initiatives planned. This work will take time as QCS fully builds a best practice corruption prevention and detection system.

Overview

QCS employs over 5,000 staff across Queensland, including the Brisbane Headquarters, 11 high security and six low security correctional centres, 13 work camps and 36 district offices. In 2018-19, there were approximately 8,773 prisoners and 21,294 offenders being supervised by QCS on any given day. During the same period, QCS managed over 27,200 admissions and discharges from correctional centres. The volume of people QCS manages combined with the breadth and extent of operations, requires a flexible approach to the management and disclosure of confidential information. In this context, the need to restrict access to confidential information to prevent improper use and disclosure must be balanced with QCS' operational requirements.

The majority of human service and public safety agencies access particular confidential information to perform their specific functions. It would often be the case in other domains of public administration that access to a specific record about a specific individual is required. For example, the health record of an individual patient, or the individual subject of a police investigation. For QCS, a wide range of officers, in varying roles, require access to a broad range of information about prisoners, or offenders under supervision.

In the normal course of custodial operations it is necessary and proper for custodial correctional officers, offender management, psychological and rehabilitation services, intelligence and other corrective services officers, to access to an array of confidential prisoner information through the IOMS. In order to effectively and safely manage a correctional centre unit, a single custodial correctional officer may access to information on a daily basis that relates to up to 75 prisoners. However, as officers move about in various roles and posts in a correctional centre, they may have need to access information about many other prisoners in other units. Similarly, offender management, psychological services or rehabilitation officers may require access to all prisoners in the management of a particular centre in order to perform their roles. This is compounded by the fact that the majority of prisoners cycle in and out of custody in less than six months. This complexity demonstrates that many roles within a correctional centre will need to access and share information on a range of individuals in order to support the security and good order of a correctional centre.

While the need and type of information may differ, officers in community corrections, with caseloads in excess of 50 offenders, are often required to access the details of an array of offenders under supervision, or those prisoners in custody who are scheduled for release to community corrections supervision. Information sharing and access for non-governmental service providers and partner agencies is a common factor across the custodial and community corrections contexts. QCS offender management officers who undertake roles vital to determine the lawful detention of prisoners, may have need to access the records of many thousands of prisoners across the entire correctional system as they review and assure sentence calculations, parole assessments, or other documentation to support their functions. When viewed across the system, noting the complexity and breadth of operations, it is recognised that access to confidential information presents unique challenges for QCS and the administration of databases and systems, particularly as it relates to restricted access to, and disclosure of, confidential information by QCS officers.

Access to confidential information, which properly and rightly supports QCS operations, must be balanced against the circumstances where QCS officers may access information inappropriately or disclose that information in breach of operational, ethical and legal obligations. QCS recognises that the majority of incidents involving improper access of confidential information may occur through curiosity and misadventure. QCS officers, as noted above, have access to a wide range of information through IOMS, and if information is accessed inappropriately, it is typically to look into the records of high-profile offenders and/ or prisoners. This behaviour must be viewed as distinct from, yet part of, a continuum that includes in the most serious cases, criminal or serious misconduct activity resulting from the access and disclosure of confidential information. Serious matters of this nature have been, and continue to be, investigated through the PSGC, CCC and the QPS.

This conduct is not tolerated by QCS, and it is unbecoming of officers within a top-tier, forward thinking public safety organisation. QCS is actively working to address this behaviour through strategies that form part of short, medium and long term initiatives to build capability and support the development of a mature, corruption resistant culture following the government investment to support the implementation of recommendations from Taskforce Flaxton. These initiatives will be complemented by longer-term strategies to improve the security and functionality of IOMS.

In response to Taskforce Flaxton, the Queensland Government allocated $25.2 million over four years to strengthen internal oversight capability, improve information security and centralise key enabling functions. QCS has started to build a corruption-resistant culture by delivering capability-focused investment in its Organisational Capability Division. The PSGC, a key area of this division, has been established and an Assistant Commissioner appointed to develop capacity across the following distinct functions:

- Ethical Standards
- Audit and assurance
- Internal discipline
- Intelligence and anti-corruption
- Corporate governance and risk, and
- Operational inspection and major incident review.

The Commissioner has issued directives to all officers of QCS, reminding them of their obligations to support ethical conduct and decision making (including the requirement to maintain information security). QCS recognises that building a mature, corruption-resistant organisational culture will take time. Prevention measures underway include:

- Internal communications and a “consider yourSELF” awareness campaign
- Screensavers on QCS computers
- Delivering training and awareness workshops with QCS senior officers and management to build capability, and
- Development of a Managerial Discipline Model (MDM) to support the expectations in *Corrections 2030* to develop a mature, corruption resistant culture.

The MDM is a remedial/ developmental approach which recognises that employees will make honest mistakes. It provides an immediate opportunity to change behaviour, conduct and/ or performance leading to an improvement in both organisational and individual performance. This model is directly related to support for instances where, as mentioned above, officers access information improperly for reasons of curiosity or misadventure, rather than in more serious circumstances that amount to misconduct or criminal behaviour.

The PSGC is supporting capability and capacity building across the agency through a learning approach with complaints; noting the policy also commits QCS to ensuring procedures and practices assist in dealing with concerns and complaints to build the trust and confidence of the community. The PSGC notes that as awareness grows amongst QCS senior officers and managers, increased reporting of matters is expected. Similarly, this work will expand as capacity grows within the PSGC, to be complemented by increased detection and deterrent activity.

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?

QCS holds confidential information about prisoners and offenders, as well as their friends and relatives who may visit them while in prison. Some confidential information can also be "personal information". This is defined in the *Information Privacy Act 2009* (IPA) as:

> information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

As a Queensland state government agency, QCS adheres to the 11 Information Privacy Principles (IPPs) of the IPA concerning the collection, secure storage, maintenance, use and disclosure of personal information.

Section 341 of the *Corrective Services Act 2006* (the Act) defines an "informed person" as a person who is performing a function under the Act or a person who has obtained access to confidential information from a person performing a function under the Act. It is an offence for an informed person to disclose confidential information other than according to section 341(3). This section states that an informed person may disclose confidential information:

a) for the purposes of this Act, or

b) to discharge a function under another law or if it is otherwise authorised under another law, or

c) for a proceeding in a court, if the informed person is required to do so by order of the court or otherwise by law, or

d) for confidential information that consists of a person's private details—if authorised by the person to whom the information relates, or

e) if authorised by the chief executive because—

   (i) a person's life or physical safety could otherwise reasonably be expected to be endangered, or

   (ii) it is otherwise in the public interest, or

f) if the information merely informs someone—

   (i) of the corrective services facility in which a prisoner is being held in custody, or

   (ii) for an offender who is subject to a parole order or a community based order—that the offender is subject to the order.

The Instrument of Delegation of the Chief Executive's Powers under the Act identifies those corrective services officers authorised by the Commissioner of QCS to disclose confidential information under section 341(3)(e).

Confidential information as defined by section 341 of the Act includes information:

- about a person's private details (which include the person's identity, private residential address or contact details), or
- that could reasonably be expected to pose a risk to the security or good order of a corrective services facility, or

- that could reasonably be expected to endanger anyone's life or health, including psychological health, or
- that could reasonably be expected to prejudice the effectiveness of a test or audit, or
- that could reasonably be expected to divulge the identity of an informant or a confidential source of information, or
- that could reasonably be expected to disclose an expert's advice or recommendation about an offender, or
- that could reasonably be expected to prejudice a law enforcement agency's investigation, or
- that could have a serious adverse effect on the commercial interests, or reveal commercial-in-confidence interests, of an engaged service provider.

Confidential information as defined by the Act does not include:

- information already disclosed to the general public, unless further disclosure of the information is prohibited by law, or
- statistical or other information that could not reasonably be expected to result in the identification of the person to whom the information relates.[1]

a. How may each type of confidential information by exploited by 'bad actors'?

As identified by the CCC in its call for submissions, confidential information held by QCS could be exploited by bad actors to promote inappropriate associations (including with media organisations), frustrate the purpose of the Act, prejudice a law enforcement agency's investigation, or affect the outcome of a matter before the courts.

b. What are the risks in access and disclosure of each type of information?

During the Taskforce Flaxton public hearings, concerns were raised about the integrity and security of information management systems within QCS including:

- the IOMS User Agreement could be misinterpreted
- the ability of QCS Information Communication Technology (ICT) systems to restrict and control access
- a lack of communication of appropriate use of information to staff, and
- audit processes to detect inappropriate use of or access to information.

As identified by the CCC, in a custodial environment, the risks of improper access and disclosure of confidential information in relation to prisoners could have serious adverse consequences for their safety, and the safety and security of the correctional centre. Furthermore, QCS intelligence gathering methods and/ or operations could be compromised.

For offenders in the community, improper access and disclosure of information could have adverse impacts on the safety and privacy of that individual and/or their family and friends. Inappropriate relationships may be exploited by criminal elements, undermining community confidence in the criminal justice system.

[1] All references to confidential information made in this document refer to the definition in section 341 of the *Corrective Services Act 2006*.

c. What are the motivators for employees to improperly access and/or disclosure confidential information?

In QCS' experience, curiosity is often cited as a motivation for staff to improperly access information on IOMS. QCS is working to address this issue by building a strong organisational culture built on ethical and professional conduct. A key motivation for the improper access and disclosure of confidential information identified by the CCC is the promotion of inappropriate relationships which may create misplaced loyalty.

Redacted due to sensitive policy and operational safety and security considerations.

2. What impact does improper access to confidential information have on:

a. The ability for agencies to perform their functions

The disclosure of confidential information forms a significant part of corrections practice. Improper disclosure of confidential information can have serious consequences for the individual whose privacy the agency breached, the agency concerned and the employee. The misuse of confidential information has the potential to detrimentally impact all aspects of QCS' operations. It poses an unacceptable reputational risk to both QCS and the Queensland Government. The purpose of QCS is community safety and crime prevention through the humane containment, supervision and rehabilitation of offenders. Corrective services officers are trusted by the community to manage confidential information in the performance of their duties. They are rightly held to a high standard of accountability as a result. Improper access to confidential information poses a risk to QCS' ability to perform its functions by undermining community confidence in the criminal justice system.

b. People whose data is improperly accessed.

As noted by the CCC in Taskforce Flaxton, the power of knowledge is intensified in custodial settings by the diverse legislated authority of corrective services officers and the vulnerabilities of the prisoner cohort. Improper access and disclosure of confidential information can have severe consequences for the safety and security of prisoners, as well as the entire correctional centre. In the community, the improper access and disclosure of confidential information could have far-reaching consequences for offenders and/ or victims. Similarly, the improper access and disclosure of confidential information about staff and/or QCS procedures could have severe consequences for the safety of staff and others. These risks could also affect the ability for QCS to perform its functions.

Management

3. How are different types of confidential information managed by the identified agencies?

Confidential information is primarily managed by QCS through IOMS, which is used by around 80% of corrective services officers on a daily basis. QCS uses a range of other databases to manage confidential information for specific purposes. These specialist databases can only be accessed by certain officers, for certain purposes. Some corrective services officers also have access to a range of databases operated by other Queensland public sector agencies, including the Department of Justice and Attorney General (DJAG) and the QPS. QCS manages Cabinet-in-Confidence information consistent with the Queensland Government Cabinet Handbook, and has a number of confidential information sharing agreements with other government agencies. This section provides an overview of the different means for managing confidential information.

Integrated Offender Management System (IOMS)

Section 10 of the *Corrective Services Act 2006* requires the chief executive of QCS to keep a record of each prisoner's details, including permitting the collection of biometric data. Deployed in 2005, IOMS is the source of truth for offender and prisoner data and is relied on to ensure accurate movements in and out of custody, record incident and contravention action and monitor compliance including appropriate supervision, substance testing, curfew checks and attendance at interventions. IOMS is the central integration component supporting both internal initiatives and information exchange with other Queensland justice agencies.

IOMS records a large amount of confidential information about current and former offenders and prisoners, including their personal details such as their name, date and place of birth, gender, last known address, physical description, photographs, ethnicity, emergency contacts and discipline record. IOMS has the capacity to record transcripts of court proceedings, verdict and judgement records, victim information, criminal histories, sentencing remarks and officer reports. It is accessed by Queensland Health staff for the purpose of entry and storage of prisoner health information, although QCS officers do not have access to the IOMS module on which this information is held.

Each step of a prisoner or offender's correctional journey is recorded on IOMS, from admission, induction, assessment, planning, participation in training and/or programs, placements within correctional centre or community corrections offices they attend, any breach matters, review and exit. It also includes supervision order details, including any community service obligations.

Reports of particular incidents, which may include photographic evidence, are also recorded on IOMS. It also holds confidential information about visitors to correctional centres, including which correctional centre they visited, who they visited and case notes on any adverse behaviour which may warrant the suspension of visits, as well as support persons such as next of kin contacts. Corrective services officers are able to log intelligence case notes on IOMS, for review by QCS Intelligence Officers.

IOMS also holds information on community corrections caseloads, including the number and personal details of offenders currently being supervised. The Parole Board Secretariat has access to an IOMS module for the management of parole board matters, including assessments and reports completed by QCS.

Victims Register

QCS administers the Victims Register through a secure, specialist module embedded within IOMS. The Victims Register provides registered persons with information on important events in the sentences of certain prisoners. The Victims Register is established under section 320 of the *Corrective Services Act 2006* (the Act). The Act sets out the process for registering as an "eligible person". QCS collects confidential information from people who wish to apply to be registered as an eligible person, including their personal information.

Information that must be provided by the Commissioner of QCS to an eligible person is outlined in section 324A of the Act, and includes:

- the prisoner's eligibility dates for discharge or release
- the prisoner's date of discharge or release
- the fact, and date, of the death or escape of the prisoner, and
- the fact and date, of any particular circumstances relating to the prisoner that could reasonably be expected to endanger the eligible person's life or physical safety.

Information that may be provided to an eligible person, to the extent the Commissioner of QCS considers it appropriate, is outlined in section 325 of the Act, and includes:

- the prisoner's current location
- the prisoner's security classification
- the prisoner's transfer –
  - between corrective services facilities; or
  - interstate or overseas under a scheme for the transfer of persons imprisoned under a sentence
- the length of the term of imprisonment the prisoner is serving
- any further cumulative terms of imprisonment imposed on the prisoner while in custody for the offence
- the results of the prisoner's applications for parole orders, or
- other exceptional events relating to the prisoner.

Case Management System (CMS)

All personal information provided as part of the application process under the *Right to Information Act 2009* (RTI Act) and the *Information Privacy Act 2009* (IPA) for access to documents held by QCS is recorded and stored on CMS. Applicants include offenders, lawyers, QCS employees and members of the community. CMS holds a large amount of personal information including names, residential addresses, telephone and email contact details, dates of birth and personal ID such as driver licenses. The subject of the requests will usually include personal information of either the applicant or another person.

All privacy complaints and privacy breaches investigated under the IPA are recorded on CMS. Personal information received by QCS regarding privacy complaints will include similar details to applications. Privacy breaches include the release of personal information to unintended recipients and unauthorized access to personal information.

CMS is a password protected data system with access restricted only to officers in QCS's Right to Information and Privacy Group. Each application for documents and each privacy matter is given a unique identifier and access to individual matters can be further restricted. QCS Legal Strategy and Services Group also uses CMS to store confidential legal advice and correspondence. Access to this area of CMS is restricted to the Legal Strategy and Services

Group. CMS is capable of producing reports on the information within it. There is no interaction between CMS and other information management systems administered by QCS.

Reporting services

Microsoft Reporting Services is a reporting tool used by QCS to retrieve, view and export information recorded in IOMS. Reporting Services can generate detailed reports on individual prisoners/ offenders, including personal details and photographs. Reporting Services:

- Replaces manual spreadsheets
- Provides quick access to data held in IOMS, and
- Provides a range of information, from agency-wide to the level of individual offenders/ prisoners (where required).

Cabinet

The Cabinet, Legislation and Liaison Office within Organisational Capability Division is responsible for the management and security of Cabinet information. Cabinet-in-Confidence documents are held and managed in accordance with the Queensland Government Cabinet Handbook. Circulation of Cabinet documents within the department is restricted to relevant officers only. Some documentation is retained by QCS and stored in a secure area while unwanted documents are securely returned to the Cabinet Secretariat in the Department of the Premier and Cabinet.

Ministerial Correspondence (MINCOR)

MINCOR is an electronic document workflow system used to manage ministerial and executive correspondence and other documents. It is a web-based application provided by an external vendor under contract for the provision of licensed software, software support and managed services, including hosting by the Queensland Government's ICT provider, CITEC.

MINCOR incorporates into one application all steps required for processing these documents from receipt and registration, draft, review, approvals and finalisation. It is not a records management system and is not integrated with any other system within QCS.

Information that can be maintained in MINCOR includes, but is not limited to:

- ministerial and executive correspondence received from members of the public, offenders and prisoners, government and non-government organisations, other Ministers and executive offices, service providers and other stakeholders
- executive and Minister briefs
- names and contact details of persons the subject of correspondence, which may include full name, address, telephone number, email address (as provided by the person), and unique IOMS number of current or previous offenders and prisoners who may be the subject of the correspondence, and
- other information relevant to the correspondence, such as emails or notes from conversations with other areas of QCS or other relevant stakeholders as may be required to assist with the process or outcome for the item.

Documents containing 'Protected' intelligence and Cabinet information are currently not placed on MINCOR. MINCOR has functionality to register and track correspondence workflows, monitor progress of actions, search actions and decisions, and report performance for senior management.

From 2009 to 2018, the Public Safety Business Agency (PSBA) hosted and managed the MINCOR correspondence tracking system on behalf of QCS. In March 2018, QCS migrated all

QCS related data (correspondence items) from the PSBA MINCOR system in to a standalone QCS MINCOR system.

QCS MINCOR delivers a tailored and streamlined correspondence tracking system, designed specifically for QCS business processes. The new system has greater security with the ability to set and control access for MINCOR users and MINCOR items, ability to record unique identifying numbers from the QCS Resolve Complaint Management System and the department's records management system (RECFIND) for cross-referencing, reporting functionality, and QCS-tailored user support tools and training.

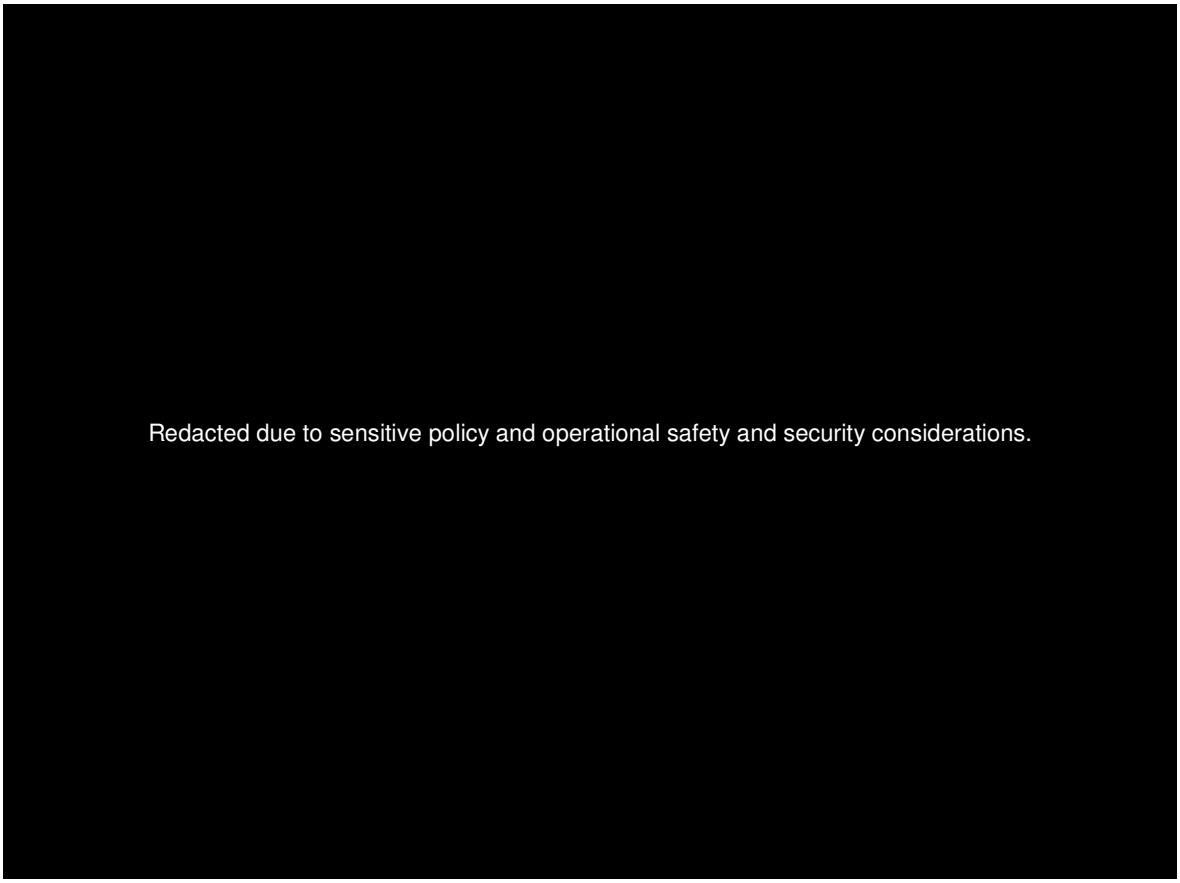
Confidential Information sharing agreements

QCS has a number of Memoranda of Understanding (MOUs) with other public sector agencies which govern the sharing of confidential information by QCS, consistent with section 341 of the *Corrective Services Act 2006*.

In Queensland, prisoner health services in correctional centres operated by QCS are provided by Queensland Health, through the Hospital and Health Services, including health, mental health and dental services. To facilitate the delivery of health services to prisoners, QCS has an MOU with Queensland Health and separate MOUs with eight Hospital and Health Services to facilitate the sharing of confidential information. QCS and Queensland Health are currently negotiating a state-wide MOU to replace the existing information sharing arrangements.

QCS also has a formal agreement for the sharing of confidential information with the following public sector agencies:

- Queensland Office of the Director of Public Prosecutions
- DJAG, the QPS, the Department of Communities, Child Safety and Disability Services (now the Department of Communities, Disability Services and Seniors), the Department of Community Safety (since dissolved, relevant constituent elements now QCS and Youth Justice) to improve collaboration between the criminal justice agencies and child protection agencies
- Queensland Court Services (DJAG) to facilitate access to the Queensland Wide Inter-linked Courts (QWIC) application
- Queensland Registry of Births, Deaths and Marriages for the exchange information to support prisoner access to identification documentation
- New Zealand Department of Corrections in relation to trans-Tasman deportations
- Australian Electoral Commission in relation to prisoners eligible to vote
- Australian Border Force in relation to immigration
- Commonwealth Department of Human Services to facilitate the provision of services (including Centrelink payments) to prisoners and offenders, and
- Australian Crime Commission for the purpose of sharing intelligence.



Resolve Complaints Management System

Each correctional centre, community corrections location and central office business unit uses the Resolve Complaints Management System to identify, record and assess customer complaints.

Under section 219(a) of the *Public Service Act 2008* a customer complaint:

- means a complaint about the service or action of a department, or its staff, by a person who is apparently directly affected by the service or action, and
- includes, for example, a complaint about any of the following:
  - a decision made, or a failure to make a decision, by a public service employee of the department
  - an act, or failure to act, of the department
  - the formulation of a proposal or intention by the department
  - a recommendation made by the department, and
  - the customer service provided by a public service employee of the department.

Complaints not recorded on Resolve include:

- allegations of fraud, corruption or official misconduct referred to the Professional Standards and Governance Command
- complaints which are considered to be employee grievances are referred to people Capability Command
- complaints received and progressed through Official Visitors (part of the Office of the Chief Inspector), and
- Matters which are subject to statutory rights of review.

Anyone can make a complaint, including prisoners and offenders under the supervision of QCS, visitors and family of prisoners and offenders, victims of offences committed by persons under the supervision of QCS, service providers, and anyone else who may be affected by the agency's actions.

Personal information recorded on Resolve includes complainant names, contact details (address, email address and/or telephone number), relevant IOMS number of a prisoner and/ or offender if applicable, name of a relevant staff member involved (if applicable), and the contents of the complaint which may include further personal information, including self-disclosed medical information. The agency's response to the complaint is also recorded. Resolve enables a unique identifier to be established for every complaint, facilitates the attachment of all documents related to the complaint and is capable of producing timely reports.

Biometrics Access Control

Section 162 of the Act permits the chief executive to store the biometric data of visitors to corrective services facilities as proof of the visitor's identity, provided the data is destroyed when no longer required. Section 137 of the Act requires a person to provide their identifying particulars (i.e. name and address) to a corrective services officer in circumstances where that person has committed or is reasonably suspected of committing an offence.

QCS uses Biometric Access Control for entry by all persons over the age of 18 (staff and visitors) to secure correctional centres. The biometric system records each visitor's fingerprint but a fingerprint image cannot be recreated from the biometric system. All persons entering a secure correctional centre are registered on the system. At each visit they are required to present their fingerprint to gain access and egress from the centre via a biometric pod. The system records all entries and exits from centres electronically.

The biometrics system is also used for the management of key security within correctional centres. Keys are assigned to users (staff) via the key safe software. All keys are then issued through the biometrics electronic key safe once the user's identification has been confirmed by way of a fingerprint. The system records all key movements electronically.

The Biometric Access Control system records the following personal information for each visitor in a secure database:

- A mathematical template that represents the relationship between key points in each visitor's index finger prints
- A photograph (optional)
- Name and date of birth
- Address and contact number
- Other identification verification details such as a drivers licence number
- Category of visitor (staff, contractor, legal visitor, personal visitor to prisoner)

- Any restricted items approved for the individual to bring into the centre (USB, laptop)
- Information regarding a visitor's medical condition which may require bypassing of some security functionality (e.g. prosthetic limb), and
- Keys assigned to users.

Biometric Offender Reporting Information System (BORIS)

In July 2014, QCS implemented biometric reporting as part of a low risk offender's reporting regime. BORIS provides a flexible reporting alternative for community corrections, providing a further tool to complement the face to face supervision of offenders in the community.

BORIS, the system which operates the kiosks and manages information, uses finger print scan technology to identify the offender and provides a short list of questions to assist the management of the offender's supervision. Using existing SMS arrangements, BORIS sends reminder messages for appointments to participating low risk offenders.

Through integrated programming, the offender's report is automatically recorded by the system in IOMS. BORIS also generates reports which are emailed to relevant staff, comprehensively detailing the day's reporting activities, to keep track of reporting compliance.

An offender's IOMS ID is used to pre-populate personal details into BORIS. This includes full name, date of birth and mobile phone number. Additional information related to the offender's supervision is also populated including their allocated officer and reporting location. Where appropriate, officers are also able to manually add or remove an offender's aliases. Biometric data and a photo of the offender are also recorded on BORIS for identification verification purposes. A biometric reader scans the offender's finger to create a mathematical template or map.

QCS ensures the offender's consent is obtained before they are enrolled into biometric reporting. Offenders are advised that participation in biometric reporting requires collection of biometric information under section 263 of the *Corrective Services Act 2006* and how the template or map is created and stored.

While BORIS maintains records of biometric data as a means for an offender to appropriately identify themselves during their supervision, biometric data is not accessible to QCS officers. The fingerprint template is not a fingerprint image and cannot be matched against actual fingerprint records held by law enforcement agencies. The system cannot convert the template back into a fingerprint image.

Furthermore, upon an offender's un-enrolment from BORIS, all biometric and personal data is removed from the system. Should the offender be subject to further periods of biometric reporting, enrolment and recapturing of biometric data must be completed again.

Body Worn Cameras

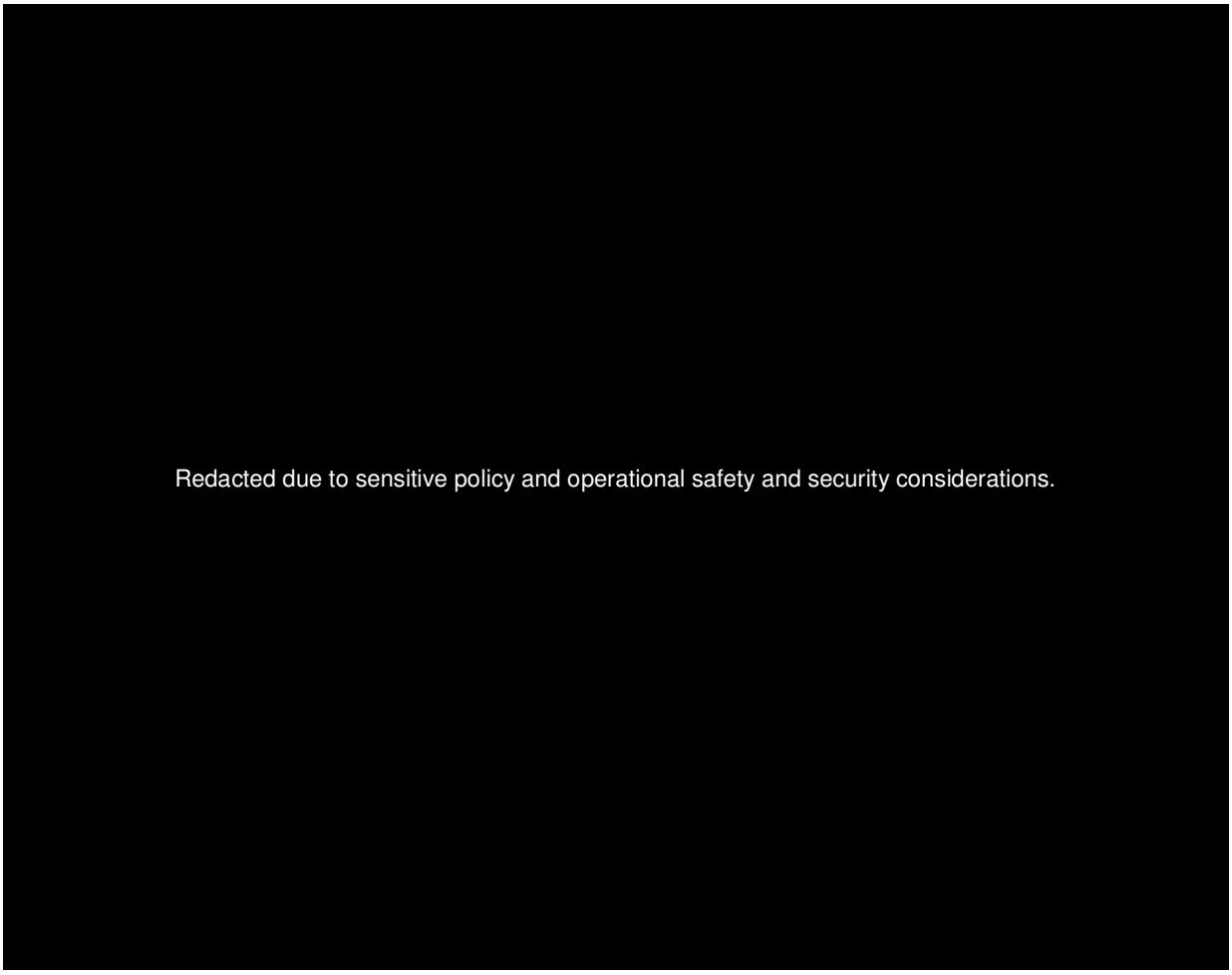
QCS has rolled out Body Worn Cameras (BWCs) to all correctional centres in Queensland, including the privately operated centres. Each BWC is used by multiple staff, and is deployed according to the needs of each correctional centre including to prisoner visits, detention and safety units, maximum security, and other areas as operationally appropriate.

BWCs have the ability to record video in variable light situations and have enhanced audio features. The batteries have the capacity to record for more than 12 hours, allowing staff to use these devices during their entire shift, if required. Recordings are managed in the same manner as QPS, supported by a digital evidence management system which allows recordings to be stored in a highly controlled environment with data encryption and restricted access. Footage is securely stored in the Evidence.com database.

BWC footage that may be stored on the Evidence.com database may include:

- footage of a variety of incidents which may include assaults and indecent behaviour
- Corrective services officer responses to incidents, and
- footage of medication rounds, and incidents where a medical response was required.

Footage may be retrieved and stored as evidence for intelligence reports. It may also be used to review incidents for internal training purposes. BWCs are allocated to correctional officer posts within correctional centres. Officers are required to collect the BWC at the commencement of their shift and return it to the appropriate docking station after use at the end of their shift. Any recordings are automatically uploaded to the evidence management system, and once downloaded, the recordings are automatically deleted from the BWC. There is no ability for footage to be deleted directly from the BWC.



Databases administered by other agencies

There are a number of other databases not administered by QCS that corrective services officers access to perform their functions. These databases allow the transfer and recording of information required to manage offenders in the community and prisoners in custody. Systems and databases include:

- Suitability Checking, Recording and Monitoring (SCRAM) Portal (administered by QPS)
- Queensland Wide Interlinked Courts (QWIC) and Electronic Transfer of Court Results (ETCR) (administered by DJAG), and
- State Penalties and Enforcement Registry (SPER) (administered by Queensland Treasury).

Suitability Checking, Recording and Monitoring (SCRAM) Portal

The SCRAM portal provides an automated solution for the receipt of QPS authorised documents including a person's Criminal History, Queensland Court Outcomes, Queensland Person History and QP9s (police facts). Documents can be accessed via a search tool requiring an offender's full name and date of birth. Officers can also search for police facts for specific offences using a Bench Charge Sheet number if known.

The SCRAM portal allows 'controlled read only' access to the QPS ICT system "QPRIME" for external Government stakeholders. The QPS Police Information Centre provides QCS with access to the SCRAM portal to acquire Queensland police documents in accordance with the *Justice and Other Information Disclosure Act 2008.*

SCRAM access has not been rolled out to officers within the custodial environment. As at 27 September 2019, QCS had 778 individual SCRAM users across community corrections (705) and Sentence Management Services (73).

Access to SCRAM allows QCS to retrieve police documents in real time via an individual log in. Access improves the timeliness of access to documents crucial to the management of both prisoners and offenders and promotes informed decision making by QCS.

Queensland Wide Inter-linked Courts (QWIC) (DJAG)

The Queensland Wide Inter-linked Court (QWIC) system is a large and complex system containing individuals' court dates, court orders and outcomes, traffic history, domestic and family violence orders, and the name, date of birth, address and contact details of individual defendants and applicants. QWIC is accessed by various court staff, Coroners staff, other departmental staff and where necessary and personnel from other agencies, including QCS.

QCS requires access to QWIC to assist in the efficient management and lawful detention of prisoners who have been sentenced to imprisonment by the courts and/or offenders requiring QCS supervision in the community. QCS staff access QWIC to confirm lawful detention and release, details of court appearances and outcomes, custodial requirements for remand and sentenced prisoners including prisoners given immediate court-ordered parole, confirm details of and appropriately manage community-based orders supervised by QCS, obtain information concerns domestic violence orders involving prisoners and/ or offenders listed as either the named Aggrieved or Perpetrator in a previous or current Domestic Violence Order. Where relevant, details will also be obtained where a named person is listed as a child, relative and/ or associate of the aggrieved.

The Electronic Transfer of Court Results (ETCR) project was intended to provide QCS with greater efficiency in the handling of court data by automating the capture of court results into IOMS, reducing manual effort and errors. Information in ETCR messages comes from QWIC through the Integrated Criminal Justice Hub processing and routing system. However, some

data in QWIC is not included in ETCR messages. The project was implemented across two IOMS releases in 2018, with the first completed in May and the second in December 2018.

Release 1 delivered:

- new ability for automatic notification of court results in IOMS and via emails as soon as court results are received
- updating Court Results in IOMS when a court result message is accepted
- improving the accuracy of matching court results to offenders, and
- converting offence codes to match codes used by the courts.

Release 2 delivered:

- updating the Offender Diary in IOMS from court results, and
- automatic creation of movements in/receptions, reducing manual data entry for staff.

The following benefits will be realised when QCS is making full use of ETCR messages by further automating updates to information in IOMS:

- reduced time taken to manually key data such as court events, court results
- reduced time taken to search for or confirm court results, as notifications will be provided automatically, and
- reduced data errors that can arise by manually typing court results into IOMS.

State Penalties and Enforcement Registry (SPER)

QCS partners with many not-for-profit organisations and local councils to supervise SPER customers performing unpaid community work as part of a court order or as part of unpaid debt registered with SPER through the Work Development Order (WDO) program.

In order to manage WDOs, QCS staff use the SPER Hardship Partner Portal (HPP). The HPP is a web based data portal used by approved QCS staff to undertake a suitability assessment with the SPER customer. The information entered into the system by a QCS officer includes a customer's IOMS number (where relevant); their SPER party ID, full name; office allocation; date lodged; and total amount for individual WDO (the maximum is 198 hours so QCS would not see the total debt the person had if it was in excess of 198 hours). The information allows SPER to review and either approve or decline an application for an individual to undertake a WDO. The HPP does not provide QCS staff access to addresses or phone numbers.

Information Security Management System

For QCS to effectively and efficiently perform its functions, it often needs to disclose confidential information. This may include sharing personal prisoner, offender, and victim information QCS holds with other government departments including the Parole Board Queensland (PBQ), DJAG, QPS, the Department of Youth Justice, Queensland Health, as well as other corrections jurisdictions (for example, to facilitate prisoner transfers) and non-government organisations such as community service providers.

The management of confidential information and information systems is an integral part of QCS' operations. Threats to the confidentiality, integrity and availability of information held by QCS must be managed appropriately according to risk. Following its establishment as a standalone public sector agency in December 2017, and in response to recommendations from Taskforce Flaxton, QCS has developed a new approach to information management to increase business involvement in understanding, identifying and managing risks.

QCS will transition managing these risks in a business-centric manner through the implementation of an auditable Information Security Management System (ISMS). QCS and its employees will implement the ISMS based on the size and scale of each relevant business area, taking into account the specific information security risks of that business area. The ISMS includes a suite of agency-specific policies, supported by an internal governance structure, designed to:

- protect QCS' information and assets
- promote the appropriate use of confidential information across QCS
- identify potential issues and develop treatment strategies, and
- escalate risks to the Commissioner, as appropriate.

This approach is consistent with the *Financial and Performance Management Standard 2019*, the Queensland Government Information Security Policy (IS18:2018), and the international best practice standard ISO27001:2015 – *Information Security*.

The initial focus of the ISMS involves a series of remediation strategies, in response to recommendation 27 of Taskforce Flaxton, to improve critical ICT systems supporting processes relating to offender management. Phase 1 will focus on IOMS, with Phase 2 addressing issues related to TIMS, BWC, BORIS and the Prisoner Trust Account System. The ISMS rollout will then be expanded to include all information management systems across QCS.

Overview of ISMS policy framework

Redacted due to sensitive policy and operational safety and security considerations.

Information security

The *Information security policy* outlines the requirements for the management of information security to protect QCS information assets and ICT assets which create, process, store, view of transmit information, against unauthorised access, accidental modification, loss or release. This policy is consistent with Queensland Government Chief Information Office (QGCIO) *Information security policy* (IS18:2018) and support the whole-of government commitment to information security. The policy is based on the implementation of ISO/IEC 27001:2015.

Information security classification and handling policy and procedure

The *Information security classification and handling policy* and its supporting procedure guide the management of information security classification and handling to ensure that QCS information assets are appropriately protected.

Consistent with this policy, QCS staff must assess the risk that loss of confidentiality, integrity or availability of information might cause damage to the organisation and consider whether specific controls are warranted.

The procedure document provides direction to QCS for determining the security classification of information and applying suitable confidentiality controls and labels to documents, imagery, audio, video, media, equipment and other material within QCS so the confidentiality of information is not deliberately or unintentionally misused.

Access to information

The *Access management policy* outlines the approach for managing user access to QCS ICT. It provides that access to all ICT assets must be approved under the access control terms and conditions outlined in the policy, based on the principle of 'need-to-know'. This means that only the minimum level of access to perform the task must be granted in order to carry out a task effectively. It also provides minimum requirements for obtaining access to QCS systems, including approval processes and user account and password management.

Acceptable use of ICT services, facilities and devices

The *Acceptable use of ICT services, facilities and devices (conditions) standard* prohibits the following:

- knowingly downloading, sending and/or broadcasting material from the internet or email containing viruses, spyware or any other contaminating or destructive features
- stealing ICT services, facilities, devices and information and/ or allowing unauthorised persons, external or internal to QCS, to use QCS ICT services, facilities or devices
- sharing proprietary or confidential information without authority
- failing to comply with confidentiality agreements with third parties
- failing to secure QCS ICT system and software access logins and passwords
- accessing, searching or misusing information from QCS systems without an authorised business purpose
- distributing confidential information held by QCS to external organisations or individuals for non-work purposes, and
- extracting, disclosing, modifying, adding or deleting QCS business information when not for a work-related purpose.

Disposal

The *ICT Asset management and disposal policy* provides for the appropriate disposal or transfer of ICT assets, and requires disposal of an asset to be authorised by the delegate of the Director, Offender Information Systems, and performed in a manner that ensures no QCS information is exposed.

Operational and human resource security

The *Operations security procedure* establishes protocols including, but not limited to:

- keeping portable media secure
- securing hard copy materials classified 'sensitive' and above

- destroying hard copy materials when no longer required
- securing computers, keys, and doors when workspaces are unattended
- a number of human resource security measures, including:
  - performing criminal background checks for all new employees and contractors
  - providing annual security awareness training relevant to role functions
  - signing appropriate security acknowledgements, employment contracts and undertakings
  - termination processes including revocation of access rights, and
  - providing that employees who commit a security breach are subject to a formal disciplinary process under the Code of Conduct for the Queensland public service.

The *use of private email and messaging applications standard* (**Attachment 10**) provides that:

- All QCS information must be managed according to relevant legislation and policy
- All QCS employees must ensure all government business is conducted and managed through their QCS (Queensland Government) email account or other QCS mandated system, and
- Unsolicited work emails to a private account must be transferred to the QCS network.

4. How is misuse and improper access detected by the agencies?

Reporting an information security incident

The *Information security incident and action procedure* outlines the process for reporting and correcting security incidents or security weaknesses from internal and external sources within QCS. This procedure establishes protocols for:

- identifying what constitutes an information security incident and how to report it
- conducting an incident investigation including gaining specialist advice from the QCS Ethical Standards Group or the QGCIO
- reviewing, authorising and implementing corrective action, and
- logging and reporting an incident.

Professional Standards and Governance Command

In response to recommendations 30 and 31 of Taskforce Flaxton, the PSGC has been established to build, drive and maintain a mature and corruption resistant culture that promotes disciplined ethical behaviour and professional practice through deterrence, education and system improvements. Misconduct in relation to the improper access and release of confidential information may be detected through internal PSGC investigations, prisoner and offender complaints, either to QCS or the CCC, investigations by the Corrective Services Investigation Unit (CSIU), QPS. The PSGC is involved in the development and delivery of programs and services to maintain an ethical culture and promote ethical decision making throughout QCS.

Specifically, the PSGC is responsible for matters including:

- promoting ethics awareness and ethical decision making through the provision of advice, training, workplace support strategies and policies
- assessment of conflicts of interest and other employment declarations
- referrals to external stakeholders for assessment and investigation as required, including the CCC and the QPS via the CSIU
- investigating allegations of misconduct and corrupt conduct
- completion of reports to decision makers involving misconduct matters
- development of the QCS risk management framework, including strategies to address fraud and corruption
- management of the internal audit of QCS functions
- compliance with ISMS requirements, and
- development of integrity-related intelligence capability and functions.

It is important that QCS is able to make decisions about the management of the correctional system based on robust information and analysis. This allows QCS to better understand its current position, plan for the future and ensure appropriate allocation of resources and supports. The PSGC's functions are a critical component of this process.

A number of reviews and reports have highlighted the need for QCS technology systems to better manage information, including the Queensland Parole System Review, the Queensland Audit Office's Criminal Justice System – Data reliability and integration report, KPMG's Report of ICT services across DJAG, and most recently, the CCC's Taskforce Flaxton.

With a clear remit to build, drive and maintain a mature, corruption resistant culture within the department, the PSGC has identified a number of initiatives and opportunities to enhance the capability of the organisation. These initiatives are intended to address the unique needs of QCS, while ensuring consistency with the best practice approaches identified by the CCC during Taskforce Flaxton. These include:

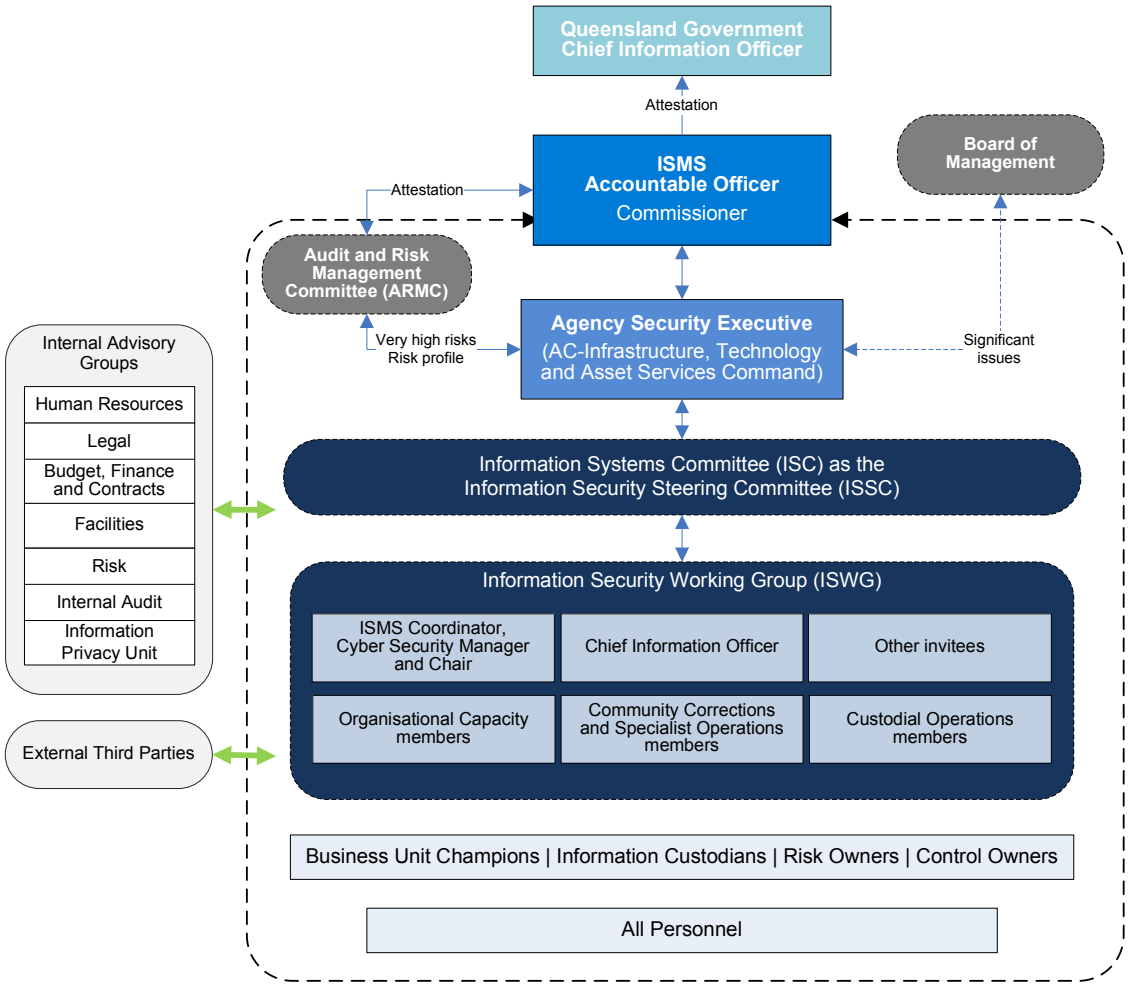
- development of corruption prevention promotional material such as posters and screen savers which will be deployed across all areas of QCS
- prisoners receiving written communication from PSGC outlining their rights and responsibilities and information on the complaints and referrals process
- staff receiving written communication from PSGC which will provide advice regarding ethical decision making, corruption prevention and support processes available
- ongoing information and awareness sessions, at each correctional centre, involving PSGC staff conducting discussion/focus groups on corruption prevention
- implementation of a formal case management/complaints management model including electronic system/database and triaging practices that allow for monitoring data issues, trends and emerging risks
- regular reporting to the QCS leadership team
- the introduction of a corruption prevention advice hotline

- facilitating professional development of senior leaders best practice approaches for corruption prevention and risk intelligence
- initiating professional development for PSGC staff in corruption prevention and risk intelligence
- proactive partnerships within operational areas of the agency
- establishment of a risk intelligence unit within PSGC focused on gathering, analysing and reporting on intelligence data and trends in relation to corruption related risks
- partnering with relevant stakeholders to undertake research to identify and embed best-practice outcomes into PSGC practice
- further investment in effective technologies and systems that assist in corruption prevention and risk monitoring
- expansion of risk intelligence functions to incorporate more sophisticated and proactive vetting and probity strategies into recruitment, selection, promotion and honours and awards functions, and
- a review of the existing support available for witnesses and disclosers to identify areas for improvement; and integrated accountability oversight services within the organisational design.

5. Does each identified agency monitor the ongoing effectiveness of the information security governance activity?

Information security governance

The Assistant Commissioner, Infrastructure, Technology and Asset Services Command has been designated the QCS Agency Security Executive, responsible for implementing the ISMS. The Agency Security Executive is responsible for chairing the QCS Information Steering Committee (ISC), which reports to the Executive Leadership Team and Board of Management. The ISC is responsible for the development of ISMS policies and frameworks, supported by advice from content experts on the Information Security Working Group (ISWG). The following diagram shows the QCS ISMS governance structure with the associated interfaces and dependencies.



The QCS Information Security Governance Framework sets out the following information security objectives:

- Provide a structured approach to information security management that is consistent throughout QCS and cognisant of the need to manage political, commercial and reputational risk
- Maintain the confidentiality, integrity and availability of information assets in compliance with policy, legal and regulatory requirements
- Implement manageable and effective information security controls to ensure appropriate protection of QCS information assets
- Establish a consistent approach to the assessment, management and treatment of information security risks
- Provide a mechanism for continual improvement of the information security practices of QCS
- Provide QCS personnel with sufficient training to ensure they have an appropriate understanding and observance of relevant security responsibilities, and provide them with confidence in the effectiveness of QCS security controls
- Provide assurance to internal and external stakeholders, and other interested parties of the security and privacy of their information entrusted to QCS, whether in storage, processing or transmission
- Obtain assurance that external third parties are appropriately managing and securely exchanging QCS information, and
- Ensure that all breaches of information security and suspected weaknesses are reported and investigated.

Key ISMS milestones achieved to date include:

- Completion of the separation of QCS security systems from DJAG
- Establishment of the ISMS governance structure in February 2019
- Development and publication of 19 new ISMS polices, standards and procedures
- Integration of information security into QCS risk management policies and frameworks
- Development of an ISMS Risk register that is considered at meetings of the ISWG. A key risk identified as part of this process is the misuse of QCS sensitive or protected information resulting from unauthorised access. Appropriate risk controls have been identified, consistent with IS18:2018, and remediation strategies identified
- Establishment of the Digital Services and Information Technology team, which has driven the development of ISMS policies and provides support to the ISMS governance
- Preparation of an internal assurance process, development of the Queensland Government Chief Information Officer annual return, and Commissioner letter of attestation
- Implementation the of Windows 10 rollout to be followed by Office 365 to improve the organisation's ICT functional and security posture, and
- Implementation of the Australian Signals Directorate Essential 8 cyber resilience strategies requiring continuous ICT technical security activities to meet new threats.

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?

As identified in the Taskforce Flaxton final report, complaints received by the CCC in relation to the misuse of confidential information by QCS officers increased in the three years to December 2018. This increase may be the result of a range of factors, including:

- Improved understanding of prisoner rights
- Increased public scrutiny of QCS' operations during the CCC's Taskforce Flaxton, including the call for submissions and public hearings held during 2018.

QCS has committed to undertaking a review of prisoner complaint processes in response to Taskforce Flaxton. This review aims to improve prisoner understanding and confidence in the system, and consistency of complaint handling across correctional centres (Recommendation 29).

a. Do these factors create a corruption risk or facilitate other corruption risks?

Increased awareness of prisoner rights and public scrutiny do not create a corruption risk. Rather, they should be encouraged to help build a corruption-resistant culture at QCS. Furthermore, the commencement of the *Human Rights Act 2019* from 1 January 2020, will likely increase the number of complaints made by prisoners. However, this indicates a positive change based on the promotion of human rights.

QCS is working to address these risks by improving its ICT systems and promoting ethical behaviour to reduce the likelihood of staff improperly accessing information. Only by identifying corruption risks can QCS adequately respond and continue to build a corruption-resistant organisational culture in line with the recommendations of the CCC's Taskforce Flaxton and *Corrections 2030*.

b. Are these factors systemic or symptomatic of idiosyncrasies with the particular agency?

The *Human Rights Act 2019* applies to all public entities. The increased awareness of individual rights and additional public scrutiny as a result of the commencement of the *Human Rights Act 2019* will affect QCS due to the unique nature of corrective services, which necessarily limits personal freedoms.

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?

QCS' operational environment presents some unique challenges in relation to corruption risks relevant to the misuse of information, including:

- Failure to report corruption
- Inappropriate relationships, and
- Misuse of authority.

QCS is working to address these risks and eliminate gaps in legislation, policy and practice that may enable corrupt conduct to occur in relation to improper access and disclosure of confidential information.

The CCC's Taskforce Flaxton identified the need for QCS to establish a centralised function responsible for policy and practice management throughout the agency to promote performance standards and consistency and review Custodial Operations Practice Directives including the Directive "Confidential Information – Disclosure of Confidential Information" to improve clarity and consistency (Recommendation 9). As part of the Organisational Capability Division restructure, QCS has established the Operational Policy and Practice Development Group within the Policy and Legal Command to implement this recommendation.

a. Are there unique challenges presented in an agency in relation to the handling and storage of confidential information?

QCS manages a large volume of confidential information across a number of information systems and databases. Further, QCS staff access confidential information held by other Queensland government agencies in the course of their duties (see above response to Question 3). QCS also operates a dispersed business model, with correctional centres and community corrections offices and reporting locations across the entire state. As a result, systemic oversight and monitoring of staff activity in relation to the handling and storage of confidential information can be challenging and requires sustained and consistent attention.

b. What are the deficiencies within each agency's systems that facilitate information misuse?

Redacted due to sensitive policy and operational safety and security considerations.

QCS is committed to tightening access levels for IOMS users to prevent authorisation compliance issues and 'permission creep', where users may retain permissions for roles and locations after they have moved. QCS also reviewed the wording of the IOMS User Agreement to ensure it provides sufficient and clear direction regarding appropriate/ authorised use to QCS staff when accessing the system.

An IOMS Access Audit is completed annually to identify staff that no longer require IOMS access to perform their role. Quarterly audits are also conducted to identify those staff who have had a change in access approved.

An e-learning course has been developed to address staff obligations with regard to the IOMS User Agreement and confidential information, and is live on the QCS intranet. The self-paced course includes multimedia interactions, exercises, full audio descriptions, and will be accessible from any QCS computer. The course addresses: information privacy, authorised use/ access to information, being an 'informed person' under the *Corrective Services Act 2006*, safe information technology practices, and provides direct access to relevant policy/ procedures. The module includes a mandatory assessment with a certificate issued on successful completion. When implemented, it is anticipated the course will become a mandatory requirement for all current QCS staff and IOMS users.

c. Is there effective training to encourage ethical behaviours and awareness within agencies?

For community corrections officers, the Practitioner Development Program (PDP) includes a session facilitated by the Ethical Standards Group entitled "Ethical Standards and Professional Boundaries". This session canvasses the use of confidential information and ethical behaviour and conduct in QCS. The management of confidential information and disclosure under section 341 of the Act is discussed in other sessions of the PDP, including "Collaborative Case Management" and "Managing Offenders – Assessment".

The Custodial Officer Entry Program (COEP) is a 10 week full-time course. It is a mandatory requirement for becoming a QCS custodial officer and forms part of a Certificate III in Correctional Practice (Custodial). COEP participants must demonstrate competency in the following lessons related to ethical behaviour:

- Legislative obligations under the Act, including offence provisions
- Legislative obligations under the *Right to Information Act 2009* and *Information Privacy Act 2009*, tested by completion of written examination
- Legislative obligations under section 341 of the Act relating to the management of confidential information
- Obligations under the QCS Computer Networking Guidelines, which form part of Custodial Officers' Professional Code of Conduct. Training includes:
    - Information and network security
    - Appropriate use of computers and network access
    - Rules for network access
    - Records management
    - Email use
    - Community expectations about being trusted with sensitive information
    - Compliance with legislative requirements
    - The reputation of QCS and the Government, and

- The value of information as a commodity.

- Obligations under the Professional Code of Conduct, including practical training on ethical standards, conduct and the treatment of prisoners
- Obligations to keep and maintain logbooks and registers, including accuracy and completeness, archiving and appropriate access
- Obligations to maintain professional boundaries between officers and prisoners
- Obligations in relation to the QCS social media policy, and
- Best practice dynamic security techniques to maintain the safety and security of a correctional centre.

d. Are officers aware about what constitutes improper access to information?

Every time a user opens IOMS they must agree to the user terms of agreement which contains the following warning:

> 'IOMS usage is monitored, for management, audit and review purposes. Information gained through access to IOMS means that you are an informed person under section 341 *Corrective Services Act 2006*. Unauthorised disclosure of such information is an offence under the *Corrective Services Act 2006*.'

In addition to the training described above, all custodial officers sign an IOMS agreement during the COEP which acknowledges their status as an informed person under the Act, that it is unlawful to disclose confidential information inconsistent with the Act, and the consequences for breach of these obligations.

e. Are employees of identified agencies deterred from accessing personal information without authorisation?

The warning described above is displayed every time a user accesses IOMS. Induction training for both community corrections staff and custodial officers covers their responsibilities under section 341 of the Act, including penalties for non-compliance.

All QCS officers are required to declare potential perceived conflicts of interest and secondary employment. Risk mitigation initiatives have been implemented to prohibit the access of personal information that may compromise the integrity of QCS' operations, or create real or perceived bias or partiality. Best practice deterrence includes the prompt identification and investigation of issues as they arise, with investigators capable of gathering evidence. Swift action may be important to prevent the loss of evidence, and the clarity of recollection of the parties involved.

f. Do employees feel entitled to view all personal information given their employment within an identified agency?

IOMS access is granted for a particular purpose and restrictions are embedded in IOMS which aim to prevent staff from accessing and editing information not relevant to their role/function. IOMS records every action made by a user, including making a case note or activating a warning flag. Security controls are also included to warn staff from inappropriate access to information, such as a warning notice that accessing a particular offender file (such as notorious offenders or prisoners) will trigger an alert to the executive management.

Prevention and Detection

8. What steps can agencies take to protect themselves and discourage employees from improperly accessing information?

QCS has taken active steps to improve its organisational integrity and reduce corruption risks through its response to Taskforce Flaxton and *Corrections 2030.* However, building a corruption-resistant culture will take time. Work underway to implement relevant recommendations from Taskforce Flaxton are outlined below, which provide an overview of the steps QCS is taking protect itself and discourage employees from improperly accessing information.

Recommendation 27

That QCS:

a) replace the Integrated Offender Management System with a system that meets recognised information management and security standards

b) in the interim, and with priority, implement "remediation strategies" to reduce the risk that prisoner information can be inappropriately accessed and released

c) identify information management as a strategic risk.

Action taken to implement Recommendation 27

A project to address Taskforce Flaxton recommendation 27(b) is currently in its initiation stage. The objectives are to implement an information access model where corrective services officers will view information on a 'need to know' basis and enable proactive monitoring of use and misuse of information systems, though:

- short and medium term IOMS remediation activities including the amendment of the IOMS security access model and strengthening security control mechanisms used to view and exchange IOMS information both internally and with external parties
- developing and implementing a proactive model of monitoring usage of IOMS information and data, and
- developing relevant policy settings, appropriate governance and undertaking a significant staff education/ training effort focused on information security and user responsibilities in dealing with sensitive information and data on a 'need to know' basis.

These activities will involve a degree of technical complexity and will require carefully managed business change.

The project is currently undertaking planning, initiation, engagement and consultation. A project board will be formed to late 2019 to approve the plan and guide the project through to completion. A project manager has been appointed and the project team is being recruited. The project's first delivery stage will focus on implementing a self-service monitoring and reporting tool (to monitor access to information) as a priority. A number of preliminary activities have been completed to lay the foundations for more far-reaching IOMS information access and security reforms later in the project.

Recommendation 8

That QCS:

a) commission an independent capability review to assess the agency's capability to efficiently and effectively deliver its strategic intent

b) develop strategies to address capability gaps (particularly human resources, information and communication technology, operational performance reporting and ethical standards)

c) monitor strategy development, implementation and outcomes at the QCS Board of Management.

Action taken to implement Recommendation 8

In mid-2019 QCS commissioned an independent review to assess the agency's capability to efficiently and effectively deliver its strategic intent as outlined in *Corrections 2030*. In order to address identified capability gaps across human resources, ICT, operational performance reporting and ethical standards, QCS restructured its Organisational Capability Division. QCS is undertaking the development of its own Capability Blueprint with the assistance of the Public Service Commission in 2019. Implementation of the organisational structure and Capability Blueprint will be monitored by the QCS Board of Management. This activity will provide QCS with the resources it needs to develop a corruption resistant organisational culture and build QCS into a forward-thinking, top-tier public safety organisation.

Recommendation 14

That QCS review mandatory refresher training to include training that responds to the needs of the prisoner cohort and targets high-risk corruption areas.

Action taken to implement Recommendation 14

As part of the restructure of Organisational Capability Division, the People Capability Command has been established and an Assistant Commissioner recruited to lead it. The Assistant Commissioner, People Capability Command will be responsible for overseeing the review of mandatory refresher training to include training that responds to the needs of the prisoner cohort and targets high-risk corruption areas. This work will be considered in line with the comprehensive review of human resource policy and practice to be implemented in response to Recommendation 13.

Related initiatives

Public releases related to disciplinary action

QCS has improved the transparency surrounding disciplinary action. A public release is now issued whenever a QCS officer is suspended as a result of a PSGC, CCC or QPS investigation. The release includes information on the officer's location, the allegation made against them and a commitment on behalf of the organisation to professional and ethical conduct.

Consider yourSELF

The PSGC has developed the "consider yourSELF" ethical decision making framework to build, drive and maintain a mature and corruption resistant culture across QCS. The SELF test was announced by Deputy Commissioner Koulouris on 22 July 2019 and has been promoted internally through broadcast emails, screensavers and posters.

The SELF test applies to every QCS officer across the state:

Scrutiny – will my action or decision withstand public scrutiny?

Ethical – is my decision ethical? Compliance with policy, procedures, Standard of Practice, Code of Conduct

Lawful – Are my actions/ decisions lawful?

Fair – Would my decision/ action be seen as fair?

9. Are prevention measures integrated into information systems?

The following section provides an overview of the integrated access control and security measures, including training, embedded within each information system managed or accessed by QCS.

Integrated Offender Management System (IOMS)

IOMS is the key electronic information management system used by over 80% of QCS staff on a daily basis. A unique user ID and password is required for each employee to access confidential information held on IOMS. The Instrument of Delegation for Systems Access is used to restrict access to confidential information to specific business functions. Different types of confidential information have different security classifications which limit officers' access if classified below a certain level.

Corrective services officers cannot view 'protected' information including victim, intelligence, and Parole Board information. IOMS users must sign a user agreement with conditions of use and must have a QCS network account. The appropriate level of IOMS access is determined and approved by local managers, rather than by the central Digital Services and Information Technology team. QCS performs quarterly reviews to ensure individuals who have performed different roles don't retain their previous level of access.

Redacted due to sensitive policy and safety and security considerations.

Victims Register

A number of internal procedures govern the management of information on the Victims Register and are published on the QCS intranet:

- Victims Register – Placement and Removal of Applicants
- Victims Register – Release of Information
- Deputy Commissioner Instruction – Release of Information to eligible persons outside of normal business hours
- Executive Director Instruction – Domestic and Family Violence Protection Orders – Parole Process
- Victims Register – Completion of Registration Checklist, and

- Victims Register – File Audit.

The instrument of delegation of the Chief Executive's functions under the *Corrective Services Act 2006* and the *Dangerous Prisoners (Sexual Offenders) Act 2003*, and the Instrument of Delegation for IOMS Systems Access limit who can approve access to the Victims Register IOMS module, approve registrations on the QCS Victims Register and release information to persons registered on the QCS Victims Register.

Case Management System (CMS)

CMS is a password protected data system with access restricted only to officers in QCS's Right to Information and Privacy Group. Each application for documents and each privacy matter is given a unique identifier and access to individual matters can be further restricted.

Reporting Services

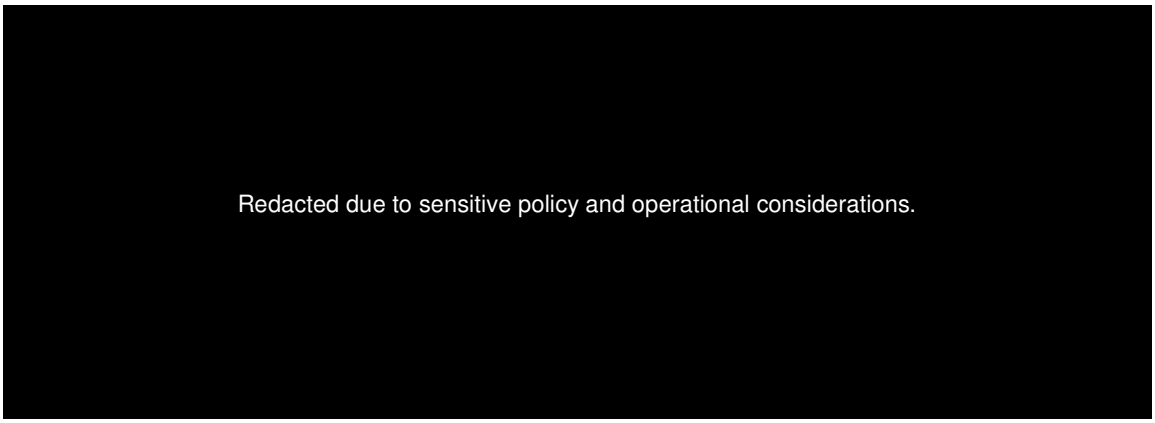
Access to Reporting Services requires a Service Now access request to be approved by the user's Manager. Access to the different reports is determined by user location and/or role. Many are available to all users with access to Reporting Services, others are restricted to specific groups. Only General Reporting Access is given automatically on approval. Reporting Services has similar access controls to IOMS. It is possible for an officer to have access to Reporting Services but have no access to IOMS. Each time a user runs a report, a record is created on an audit log. Only Reporting Services administrators are able to access the audit log to monitor a user's activity.

MINCOR

QCS MINCOR has security settings, including the ability to apply security settings to directorates, MINCOR users and MINCOR items. In September 2018, security in MINCOR was further enhanced with the 'closing' of security between directorates meaning that a user can now only access information in those directorates in which they have a MINCOR role and the required user security clearance.

MINCOR users are allocated a directorate and/or business unit, generally in accordance with their role in the organisation structure. This limits each user's ability to view or access items from outside of their directorate and/ or business area, except in circumstances where they have been delegated a role in a particular item or granted access to multiple directorates for purposes of MINCOR processing. A QCS network account and MINCOR user account are required to log on to MINCOR. The approval process for access to MINCOR is currently being amended to ensure consistency with approvals required for all security clearance levels (that is to be confirmed by Executive Services).

MINCOR users are allocated a 'security clearance' and individual MINCOR items are allocated a 'security classification'. The security matrix shows the user clearance levels that may be applied in QCS MINCOR, the various security classifications that can be applied to MINCOR items, and the items that can be accessed at each user security clearance level. The Parole Board Queensland (PBQ) uses the QCS MINCOR system but manages its MINCOR functions separate to QCS.



Resolve Complaints Management System

Access to Resolve is limited to Corrective Services Officers whose role involves recording and managing complaints on behalf of their area. It is password protected, and all actions taken in resolve are recorded with users names recorded against the action. Resolve users are able to view items they are not involved in – while this is useful in determining when a complainant has raised the same or similar complaints previously, it is a limitation of the system's security.

Biometric Offender Reporting Information System (BORIS)

Officers are automatically logged on to BORIS by using a username and password through their individual staff profile. There are three levels of access in BORIS:

System administrator (usually a community corrections District Manager) - This operator has the highest level of access and is able to use the administrator program on the server to create Allocated Officers with management access.

Allocated Officers with Management Access (usually Supervisors and Senior Case Managers) - These officers have management access enabled on their account. They have access to additional reports and the administration tab. These officers are able to create other Allocated Officers with Management Access and Allocated Officers without Management Access.

Allocated Officers without Management Access (probation services officers and case managers) - These officers cannot create access for other officers and do not have access to Management Reports or the administrator tab. They can create and modify offenders and appointment schedules and run non-management reports.

Body Worn Cameras

Access to Evidence.com is restricted and requires a unique user ID and password for each user who has access to the database. Access to the database is fully auditable. Audits are completed if improper use or access has been suspected or identified.

Access to Evidence.com is facilitated through a Service Now request (via the QCS intranet) and requires direct manager approval. Prior to access being granted, the Manager of Custodial Operations and Practice reviews the application checking the need for the access and that the manager of the applicant has approved the access request.

Access to Evidence.com is granted to managers and above, intelligence officers, violence prevention co-ordinators, Office of the Chief Inspector staff, Contract Management Unit staff, and other staff assessed as demonstrating a need to access the system. There are restricted licensing arrangements which limit the number of users who can be granted access. The BWC user is unlikely to have access to the system.

Access to and use of any information stored within the evidence management system is for authorised users only. Authorised users are assigned varying permissions to allow them to use the functionality of the evidence management system. For example, administrative access (full access) is limited to Custodial Operations head office staff only. Any unauthorised access and use is strictly prohibited, for example use of another officer's user ID and password. Footage which is identified as particularly sensitive is restricted as required through the permissions functionality.

A General Manager of a correctional centre must nominate staff to manage the BWC recordings within the evidence management system (local administrator). The evidence management system enables BWC recordings to be uploaded directly from the BWC when the device is plugged into a docking station. Staff nominated by the General Manager must review the collected BWC recordings and assign a category for classification. Classification ensures a recording is stored in the evidence management system for the legislated period of time. All BWC recordings relating to an incident must be retained. The process of classification and storage is however a manual process, and may result in some evidence not being classified and subsequently deleted from the system.

GPS monitoring

A request to access the Electronic Monitoring System is only supported where the QCS staff member requires access for the purpose of executing their duties e.g. supervising an offender/parolee subject to electronic monitoring, or monitoring room/ surveillance staff members. The Electronic Monitoring System is accessed via a web-based portal with a unique user ID and password for each user.

Restrictions are built into the system based on the level of access user accounts have. Monitoring staff have cross-system access to both parolees and offenders managed under the DPSOA and have the ability to read and write within the system. Case management staff, supervisors and administration staff have read-only access restricted to the relevant cohort i.e. community corrections staff can only view parolees, while the High Risk Offender Management Unit can only view DPSOA offenders.

Control of access is restricted based on the requirements of a staff member's role, with the request for access to be approved by their relevant District Manager. While the system does not currently have access restrictions in place for high profile offenders or district offices, the system is capable of this type of configuration if required.

Other databases not administered by QCS

Suitability Checking, Recording and Monitoring (SCRAM) Portal

User access to the SCRAM portal is granted and monitored by QPS. QCS officers are granted SCRAM portal access through the use of an external user access request form. QPS are provided with the personal details of officers and in return provide each officer with an individual log in. Once a user profile has been created an email is sent to the officer with log in details and the URL for the external website. Frontline QCS services access the SCRAM portal through the QCS network and if working remotely, through encrypted QCS laptops. QCS is unaware if the SCRAM portal can be accessed outside of a government network on a personal device. Where an officer leaves QCS either permanently or for an extended period of time, the Manager has the responsibility of notifying QPS PIC to remove the respective officer's user access to the SCRAM portal.

Queensland Wide Interlinked Courts (QWIC)

QCS has an MOU with Queensland Court Services (DJAG) for access to the QWIC application. Access to QWIC is provided to QCS in accordance with the provisions of *Justice and Other Information Disclosure Act 2008* which enables the Chief Executive of a justice agency to make arrangements with the chief executive of another agency for justice information to be made available for a justice purpose.

Only QCS users who require access to QWIC to perform their role functions are provided access. This includes users from community corrections, custodial operations, Escort and Security Branch, and Sentence Management Services. QCS users are provided 'Read-only' access and cannot make changes to any information recorded in QWIC. QCS users can search case files, persons, court schedules (with the exception of closed court participants), and file summary navigation fields including applications, location history, bail/custody, order history, charges, participants, events, and related files. QCS users cannot search applications.

Once access to the network is established, QWIC can be accessed via a QWIC User ID and password. The Courts Service Centre grants this access after completion of the required and approved forms. Access to QWIC is subject to relevant information security processes and procedures of QCS, including the prohibition of searching for or accessing information that is not for work purposes, in addition to the limitations set out in the MOU.

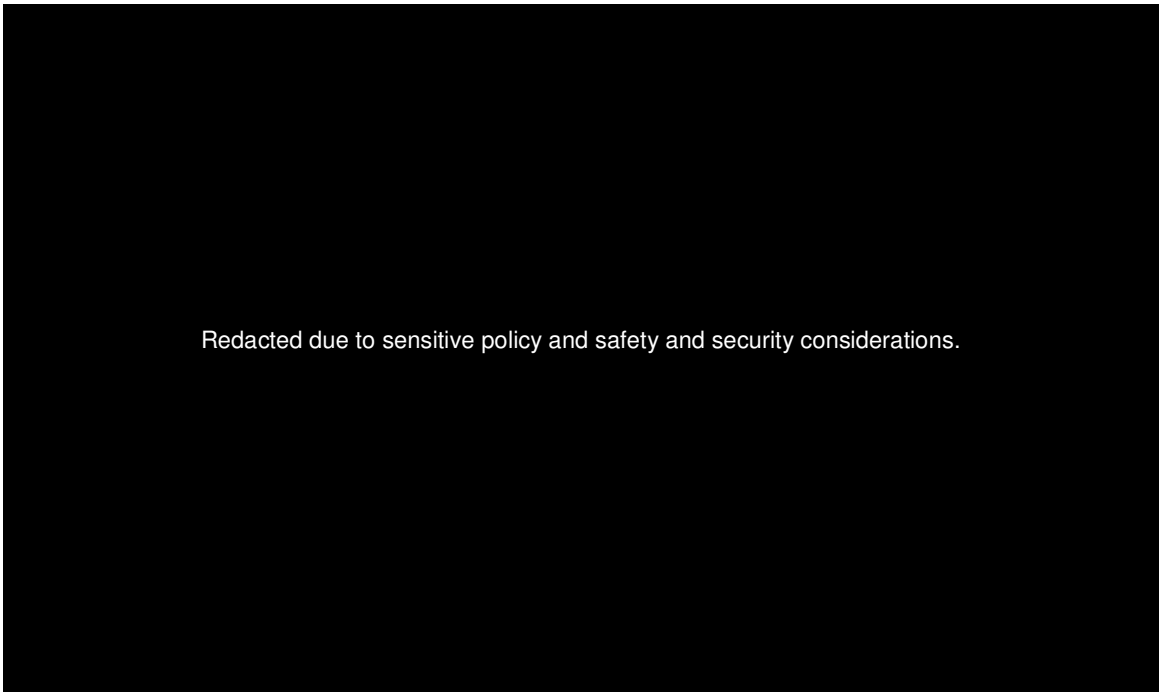
State Penalties and Enforcement Registry (SPER)

QCS staff apply to SPER for access. Each QCS user is given a unique username and password issued by SPER. QCS staff only have user access, meaning they can only access files under the region the work in. Only one QCS employee has Manager access which allows access to any WDO file across the state. Management of the HPP is undertaken by SPER.

Access requests are sent to the QCS staff member who has Manager access. The SPER form is completed by this delegate and sent to SPER to action. Checks are made by QCS to validate the QCS employees employment status (date of commencement) and the region access requested at this time. Training to support the use of the HPP has been provided by SPER in the form of training manuals. These are available on the QCS intranet.

10. Is it difficult to detect improper access to information?

As discussed above, QCS manages a large volume of confidential information across a number of information systems and databases. Further, QCS staff access confidential information held by other Queensland government agencies in the course of their duties. QCS also operates a dispersed business model, with correctional centres and community corrections offices and reporting locations across the entire state. As a result, systemic oversight and monitoring of staff activity in relation to the handling and storage of confidential information is challenging. Specific detection activity in addition to the response provided to Question 9 is provided below.



Biometric Offender Reporting Information System (BORIS)

Access audit reports are generated quarterly. If a staff member has not accessed the system recently (regardless of role) their access is removed, and they will need to reapply and establish their reasons for access renewal, if applicable. The Deputy Commissioner, Community Corrections and Specialist Operations is the custodian of the EM system, access is through the web-based interface with data being stored in the cloud based system in an on-shore data centre.

Body Worn Cameras

Staff must comply with the requirements of the Custodial Operations Practice Directive - 'Confidential Information: Disclosure of Confidential Information' prior to the release or sharing of recordings from the evidence management system.

Recordings are not to be downloaded from the evidence management system to a secondary or alternate storage system (USB, disk) unless authorised by the General Manager or nominee. In those circumstances the reason for the downloading of the recording must be noted in the evidence management system. This will generally only occur in circumstances where the recording is required for an inquiry and/or investigation or for court purposes.

While there is some ability to restrict the footage (viewing rather than sharing access) there remains a risk a staff member may make a video of the footage by recording it on a mobile telephone or similar device. This risk is very low due to the security measures that restrict the ability for mobile telephones to be brought into a correctional centre.

As Evidence.com is accessed via the internet, there is the ability for staff to be able to log in to the system when not in a secure work location, for example, at home, and facilitate the viewing of footage by the public. This risk is mitigated by the full auditability of the system. Every time footage is viewed, an electronic audit trail is maintained.

Other databases not administered by QCS

Suitability Checking, Recording and Monitoring (SCRAM) Portal

Relevant Managers are responsible for a six-monthly audit of SCRAM access in line with current IOMS audit requirements. The QPS Ethical Standards Command also conducts an audit in accordance with its own system improvements and assurances and removes access for any account that hasn't been used in more than 90 days.

QWIC

QWIC User ID's are reviewed on a monthly basis. For external agencies, the monthly Security Access Report will be emailed to the Local Area Network (LAN) Administrator by the Training and Development Unit. Any anomalies are identified by the LAN Administrators. The Courts Service Centre will be informed by the LAN Administrator of any changes required. A QWIC user's access is then updated by the Courts Service Centre and an e-mail confirming any changes made to a QWIC Users ID access is sent to the requesting LAN Administrator. The actioned QWIC Security Report is signed off by the Registrar and kept as formal verification that QWIC Access for individual locations is current. A yearly review and action of QWIC LAN Administrators is conducted at the end of each financial year.

11. How are changes in technology making it easier or more difficult to ensure confidential information is not improperly accessed or disclosed?

Taskforce Flaxton recommended QCS replace IOMS (Recommendation 27). The benefits of implementing an upgraded ICT solution include:

- A new security layer to enable configuration of granular access control which will align to QCS' staff role/function requirements for system/ data access. This will improve security management access to user's relevant role/ level within the organisation, limit security breaches, enable improved audit tracking of system/ data access to inform investigation and avoid the costs of security breach investigations
- Improving forms and case management, which will allow for better data input and validation and greater reporting and tracking of incidents
- Implementing an enterprise content management system which will provide secure storage of sensitive information, such as psychological reports, and enable restrictions on access to offender related documents through security controls and an audit trail of access
- Delivering secure content, such as briefs and legal documents, direct to prisoners from their legal representatives which will limit the need or availability of QCS staff to access this information, and
- The introduction of improved analytics capability, drawing data from across the environment to conduct predictive analysis.

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

The Queensland Government's response to the 33 Taskforce Flaxton recommendations establishes the framework for QCS' transition to a top-tier, forward thinking public safety agency by embedding a corruption-resistant organisational culture across its operations. A number of the recommendations will help QCS prevent, detect and deal with corrupt conduct relating to misuse of information. Recommendations that could be usefully extrapolated to the broader Queensland public sector in the context of Operation Impala are outlined below.

#	Recommendation
1	That QCS: (a) develop a comprehensive measurement strategy to assess the performance of its anticorruption strategy (b) incorporate anti-corruption performance reporting into appropriate governance committees to ensure appropriate oversight (c) publicly report anti-corruption performance outcomes.
3	That QCS review its risk management framework to improve the identification, management and oversight of corruption risk.
4	That QCS review its organisational structure to: (a) support the delivery of its ten year strategy (b) provide greater role and function clarity (including span of control, reporting lines, delegations and authorisations, employee performance management) (c) be sufficiently agile to accommodate future changes in the agency's strategy (d) improve standards, drive performance and deliver efficiencies (e) promote internal communication.
6	That: (a) QCS establish an organisational-wide cultural change program to assess current culture, create a shared vision of the ideal culture, develop and implement initiatives to support cultural change, and monitor and report on the implementation of initiatives and cultural change (b) the organisational-wide cultural change program be monitored by the QCS Board of Management to ensure alignment of culture, strategic intent and performance priorities, and to ensure the program is adequately resourced.
9	That QCS: (a) establish a centralised function responsible for policy and practice management throughout the agency to promote performance standards and consistency (b) review Custodial Operations Practice Directives and local instructions to improve clarity and consistency.
11	That QCS develop an agency-specific Code of Practice to complement the Code of Conduct.

14	That QCS review mandatory refresher training to include training that responds to the needs of the prisoner cohort and targets high-risk corruption areas.
17	That QCS: (a) implement an agency-wide, electronic system to record conflicts of interest and management action (b) develop and implement a declarable association policy.
19	That QCS develop an integrity testing regime to identify and strengthen deficient systems and processes, and support the investigation of people suspected of engaging in corrupt conduct.
28	That QCS: (a) establish an agency-specific Public Interest Disclosure policy and process (b) review the processes and supports available to witnesses and disclosures who are employees (c) improve complaints management processes (consistent with the recommendations made by the Queensland Ombudsman in 2016).

a. What are the barriers to successfully implementing these reforms and how could these barriers be removed or mitigated?

All of the above recommendations were supported or supported-in-principle by the Government in its response to Taskforce Flaxton, noting the benefits of implementation across the public sector. Operation Impala presents an opportunity to develop a whole of government response to corruption risks associated with the misuse of confidential information to improve trust and confidence in the public sector and embed a corruption-resistant culture across all Queensland government agencies.

13. Are there adequate legislative protections and remedies for people who have had their privacy breached by employees in public sector agencies?

There are a number of legislative provisions which facilitate and protect the consensual and non-consensual disclosure of personal information. This includes the *Corrective Services Act 2006*, IPA, RTI Act, *Dangerous Prisoners (Sexual Offenders) Act 2003* (DPSOA), and the *Justice and Other Information Disclosure Act 2008* (JOIDA).

The Senior Privacy Officer audits QCS' compliance with the requirements of the IPA and investigates information privacy complaints and breaches. They perform the following further functions:

- Delivery and development of information privacy training
- Development, analysis and provision of advice on standards, guidelines, policies, procedures, and proposals relevant to information privacy management
- Make decisions on the release and amendment of QCS documents under the RTI Act and the IPA, according to administrative release guidelines.

The community (staff, prisoners, offenders, and victims) entrusts QCS with their personal information, as defined under section 12 of the IPA. To maintain this trust, QCS needs to handle personal information appropriately, and safeguard it. This includes protecting confidential information against loss, unauthorised access and other misuse. The Act contains strong offence provisions to protect information, including section 133, which makes it an offence to interfere with records kept under the Act, with the maximum penalty of 100 penalty units and 2 years imprisonment. Further, the disclosure of confidential information outside the provisions of section 341(3) may result in prosecution with a maximum penalty of 2 years imprisonment or 100 penalty units.

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?

QCS does not have any other issues to raise.