

From: Robert h [REDACTED]
Sent: Wednesday, 12 February 2020 11:00 AM
To: Parliamentary Crime and Corruption Committee <pccc@parliament.qld.gov.au>
Subject: Inquiry into the Crime and Corruption Commission's performance of its functions to assess and report on complaints about corrupt conduct

To the Parliamentary Crime and Corruption Committee,

I would appreciate the consideration of this late submission.

There is currently no mechanism to inform persons whose privacy has been illegally breached without proper authorization and therefore all redress for such violations of human rights is prohibited by law. Either as a result of operations investigated or in the course of the conduct of the operation of the CCC. Once dissemination controls have been violated the information must be considered public domain as there is little hope of fully tracing all avenues of dissemination and bringing that information back under control. As such information that is believed to be private must be considered to now have been released to the public domain. If Queensland is a state of law then persons violated in such a manner must be given access to redress and this is only possible through notification being issued to such persons. Recently Operation Impala highlighted the widespread misuse of information and poor dissemination controls. Without the threat of serious financial penalties imposed in the form of fines and/or compensation by a court of law, the state has no incentive to take adequate precautions to ensure privacy.

If a person's personal private information is disclosed without authority to release or a credible serious threat to public safety then this has the potential to seriously injure that person, something which the state must keep itself open to accountability before the courts.

I recommend the implementation of NIST standards as soon as possible across all controlled information systems. These require, for example, the owner of the credentials (passwords, keys) used to access such systems is held accountable. It is beyond belief that so many illegal disclosures are handled in a reactive manner by monitoring systems and that access has been obtained without authorization. It is completely unacceptable that no inspectors or commissioners have been fired for the actions of officers under their command. Executives must take responsibility for the actions of those under their command. For example, the officer who left their police computer unsecured that allowed another officer to access information without authorization was not similarly punished. Persons with authorization to access information have a responsibility to secure those systems. The repeated statement, "I was doing my job," by officers accused of inappropriately accessing information implies that they were acting under orders and this must be fully investigated.

Robert Heron
[REDACTED]
[REDACTED]
[REDACTED]