CRIME AND CORRUPTION COMMISSION

TRANSCRIPT OF INVESTIGATIVE HEARING

CONDUCTED AT LEVEL 2, NORTH TOWER, 515 ST PAULS TERRACE, FORTITUDE VALLEY WITH RESPECT TO

File No: CO-19-1209

OPERATION IMPALA
HEARING NO: 19/0006

DAY 8 - WEDNESDAY 20 NOVEMBER 2019
(DURATION: 34MINS)

LEGEND

PO Presiding Officer – ALAN MACSPORRAN QC
CA Counsel Assisting – JULIE FOTHERINGHAM
HRO Hearing Room Orderly – KIMBERLEY SAUNDERS
W Witness – ANDREW MILLS
LR Legal Representative –

HRO All stand. This hearing is resumed.

PO Good afternoon.

CA Good afternoon, Chair. I call Mr Andrew MILLS.

PO Mr MILLS. Would you prefer an oath or an affirmation?

W Affirmation, thank you.

PO Affirmation. Yes, thank you.

HRO I solemnly affirm and declare.

W I solemnly affirm and declare.

HRO That the evidence given by me.

W That the evidence given by me.

HRO In these proceedings.

W In these proceedings.

HRO Shall be the truth.

W Shall be the truth.

HRO The whole truth.

W The whole truth.

HRO And nothing but the truth.

W And nothing but the truth.

PO Have a seat, thanks.

W Thank you.

CA Good afternoon, Mr MILLS.

W Good afternoon.

CA You were provided with an attendance notice for today?

W Yes, I was.

CA Yes. May Mr MILLS be shown a copy of the notice?

W Yes.

CA Thank you. I tender that document.

PO Exhibit 143.

ADMITTED AND MARKED EXHIBIT 143

CA Mr MILLS you are the Chief Information Officer at the Queensland Government Chief Information Office.

W Yes, I am.

CA And you have held other positions, mainly in the area of information communication and technology in the public sector?

W Yes, I have.

CA Yes. Prior to your current appointment in 2015 you were employed as the South Australian Government Chief Information Officer which you held for six years.

W Yes, 2014 I was appointed.

CA And, prior to that, other, as I said, other information technology roles, and you also served in the Australian Army as an officer for 22 years?

W Yes, I did.

CA Thank you for that. Now, I believe you have some opening remarks you would like to-

W Yes, I would like make an opening statement.

CA -make an opening statement. Yes.

W Now more than ever information is key enabler of our lives. There is a critical need for government to utilise accurate and timely information to make better decisions. Government agencies hold a range of information, sometimes sensitive, to enable the services it must deliver. Meeting the expectations of Queenslanders on how we manage this information is crucial to maintain the trust and confidence of all stakeholders. When sensitive information is acquired or released to the wrong people the consequences can be catastrophic. The key challenge for government is striking an appropriate balance between ensuring

authorised and appropriate access to sensitive information and encouraging sharing of information for the delivery of vital services.

There have been cases over many years where not sharing data contributed to the outcomes as identified by, for example, the Royal Commission into Institutional Responses to Child Sexual Abuse; the South Australian Nyland Royal Commission into Child Protection Systems; When a Child is Missing: Remembering Tiahleigh - a report into Queensland children missing from out of home care; the Carmody Child Protection Commission of Inquiry; the Keelty Review of Police and Community Safety; and the Queensland Floods Commission of Inquiry. The Queensland Government Digital Strategy has principles including making services secure by design recognising that government and customers play a key role in keeping their data secure.

There is also a strong suite of policy supporting agency in meeting these needs. IS 33, Information Access and Use Policy; IS 38, Use of ICT Services, Facilities and Devices Policy, which encompasses monitoring of authorised and unauthorised use. If monitoring is to occur, employees must be aware of the conditions under which it happens. And IS 18; Information Security Policy.

Responsibility for implementing this policy lies with each agency accountable officer who sets the risk tolerance of the organisation. Successful implementation requires capable risk management at all levels within government agencies. It also requires a holistic protective security policy approach bringing together governance, information, physical and personal security disciplines to secure the organisations. People process and technology must all work together to manage the risk to information we hold.

The cyber security mantra of protect, detect and respond has driven implementation and policies and processes to address information security and authorised use of technology and information. We strive to protect what we can, detect when we fail and respond as effectively and efficiently when required. However the issue we're considering today is an information management issue much rather than a cyber security issue.

As an example, to address one of the risks the Australian government provides guidance on – sorry the Queensland Government provides Guidance on Personal Use of ICT resources. Misuse should result in disciplinary procedures in line with industrial and procedural fairness. However any disciplinary action must not inhibit public servants from doing their job. Tougher sanctions inhibiting the official sharing of information will increase the risk aversion of officers. This may negatively impact scenarios where information sharing is authorised but not done to avoid risk. QGCIO has developed an Information Sharing Authorising Framework to address the broad information sharing needs while protecting confidentiality and privacy rights of citizens.

The framework leverages the work delivered in the Child Safety Department to provide general guidance. It consists of four phases: define the value and

understanding the constraints; agree on obligations and methods; design build and test architecture; then use it. And with attention to what we can leverage and assure. Information management is not a single approach but many approaches at multiple levels; business, information, application and technology.

Over and over again we've found that misuse of information not primarily a technical issue. It is a capability people process and behaviour issue. One where the Code of Conduct along with education and awareness are paramount. The QGCIO works with agencies to help to lift their capability and share learnings. The Office of the Information Commissioner's Information Management Maturity Survey, recent survey, shows there's still much work to be done to lift the capability of information management across the sector. Ultimately the Government must demonstrate it is a trusted custodian of information. The public must trust public servants in handling of their information and trust that public servants have the information they need to deliver vital services to Queensland.

CA Thank you. Could you please provide an overview of the functions that QGCIO performs with respect to public sector agencies?

W So we are set up to provide advice to Government agencies and Executive Government on issues such as setting ICT strategy policies and standards; adopting better practice for ICT investment management; identifying and managing risks including the over-horizon risks; developing a proposal for major whole of government investments and agency investments; improving contract outcomes; and facilitating strategic relationships with industry partners.

CA And you mentioned – before we go into some of the details that you touched on with IS 33 and the like, you mention in your opening statement that whilst Queensland is mature in its information security policy there is not the equivalent of the Commonwealth's overarching protective security policy framework. Could you just explain what the Commonwealth one is?

W So the Commonwealth actually have an overarching framework that deals with personnel, protective or physical and information security. At this stage they are dealt with separately in the Queensland Government.

CA Now, if we could just turn to IS 18. Could you explain the basics of that and go into a bit of detail about the three policies?

W So we've had an information security policy for over a decade. Recently have been through a full upgrade and we now have what's called IS 18 2018 as the new version. We have moved from what was previously a compliance based approach which talked about technical compliance with certain things you had to do with the systems to a risk-based approach based on the business risk to the agency. As mentioned already in evidence, each agency is now required to

develop what they call an Information System Management System, Information Security Management System, for all their systems which outlines how they're going to protect each system. So it's based on system usage not not a blanket approach to different risks. So a website will have a very, very different approach to QPRIME as you've talked about today.

Basically the policy has three requirements; that they must implement ISMS based on the international standard 27001. So we have gone to an international standard approach. Must apply systemic and repeatable approach to risk management and they must meet minimum security requirements. The Department accountable officer must obtain security assurance for their systems and accountable officers must attest the appropriateness of departmental information security. So that's the basis of the policy.

CA So every agency must prove that they've reached the standard IS 18 2018. They must have – well the due date was 30th October of this year; is that correct?

W The first report for IS 18 2018, yes, was this year, October. We currently have but two of those reports and every-

CA And which agencies haven't provided you with their reports?

W At this stage we have provided – extensions have been granted to Queensland Health and Queensland Corrective Services.

CA And you mentioned that each agency has different risk levels. Out of the seven subject agencies; Health, Police, Education, the two Hospital and Health Services, Transport and Main Roads – do you see any of them as particularly more risks involved than others?

W Well they all have unique risks so I think it's – and then they have different risks.

CA Yes.

W And so it depends – and that's why we've gone to very much a focus on the business structure of each agency and for them to assess the risk they have got. An example I'll use is Transport have much more risks in areas of what we will call IOT or technical systems versus police which is much more an information risk.

CA And is it QGCIO where they can go to obtain some advice and assistance guidance?

W Yes, we have a small team that provides support to agencies and overarching. There are also a series of cross-government services which have been funded centrally to support agencies in protecting their systems.

CA And could you explain a little about policy two? So policy one relates to the due date of 30th October where two of them have extensions at the moment that they must have signed off and provided attestation. Is that right, that they're compliant?

W Yes. No, they – in a sense I'd like to say not – we aren't measuring compliance. We're measuring that they have an ISMS in place and that their accountable officer is comfortable that meets their business need.

CA And then policy two is that – that's to do with the maturity level, so their ability to manage the risk?

W Going to a risk management basis approach requires that you actually have a good risk management approach and structure. It is a maturity level and different agencies have much different levels of maturity and risk management. We have been doing quite a lot of maturity uplift work with agencies, particularly in their IT shops from our side, but broader risk management. So core of doing cyber security is actually being able to assess risk and understand what risk means and how to mitigate risk and how to put that in business terms. So a lot of our work has been around that base of building our maturity and capability of staff within the government around risk management.

CA And policy three is about what?

W There are certain minimum requirements set. And so I'll use an example today the police talked about that they've got minimum requirements that come from the Commonwealth.

CA Yes.

W So there are certain minimum requirements required that we will set across the board just because you're working in a very risky environment, so they are set.

CA And what are they?

W Oh you're probably going into too much detail-

CA Could you provide some examples?

W Okay. So you need to – okay, and please I'm probably delving a little bit into detail that I would need to confirm, but one of those would be that access to your system must be controlled. So you must have some form of system to know who's on your system and who's operating. So a password – a log on and password are required to get into government systems.

CA Okay. And then could you explain what is in place-

W I can probably go a little bit further there. So they also have to implement the information security classification framework which is part of the policy suite. So they need to be able to classify their data at its confidentiality levels.

CA Could you explain what those levels are?

W We've only just updated those. Let me just make sure I'm-

CA Are they official, sensitive and protected?

W And protected, yes.

CA Yes. So-

W So we have aligned with the Commonwealth new classification so we actually have alignment with the Commonwealth when we share information we know what levels of classification we're sharing at.

CA So official is low or negligible confidentiality impact?

W Yes. Yes.

CA Then sensitive?

W Moderate confidentially impact. And protected is highly – high confidentiality impact.

CA And with respect to the protected category, there must be controls?

W Yes. So the Australian cyber security centre provides a minimum set of controls around protected information and we've flowed those through to the Queensland Government.

CA Just turning to sharing of information between the agencies, what are the requirements with respect to that?

W So to share information, agencies must negotiate that sharing and put in place an agreement around that sharing. As I said we only provide guidance in this space. We would put a guidance in what we call the authorising framework. So that actually takes agencies through the thinking of what are the things they need to agree. And you saw an MOU this morning between Transport and Police. So how do they meet their requirements for the information that they are sharing with the other organisations to ensure that they are meeting their requirements under things such as the Privacy Act and those sorts of situations.

CA And must the data be encrypted?

W We have a data encryption. That's again a risk management decision. But, interestingly, even though that may protect it when it's not being used it can't be encrypted when it is being used because people need to be able to see what data is there. So in some senses while that will protect it from unauthorised access, it's not going to protect it during an authorised access situation.

CA And then are there any requirements for when the information is in transit and at rest?

W That depends on the classification. So again you need to classify your data until you then make decisions on what is required in those situations. I'm now starting to delve what I believe protected – I would believe protected you would need to encrypt in transit.

CA And are there any requirements for the sending – the owner of the information, the controller, to audit the receiving agency to check that the information is being protected to the degree that it is the UI-

W That would depend on the agreement in the MOU of what's been agreed. I would recommend that as good practice that you should actually have some at least confirmation back. If you're not handing over and passing that requirement legally to the other side then you would need to audit their requirements. It is depending on the MOU though would depend on the level of audit required.

CA And are there any business impact assessments that are undertaken?

W Yes. So to achieve – so as part of classifying their information, there is we actually provide what we call a business impact assessment and an example of how to do that. So we provide tools for people to actually – so for classifying data you need to understand the impact on the business, it is not an esoteric technical issue. It's actually about a business issue. So we provide the levels and work their way through it so people have got a tool to work their way through. So we get consistent implementation of those levels.

CA With respect to breaches, both unintentional and intentional, is there a requirement to notify QGCIO on behalf of the agency?

W The breach notification is actually under the Office of Information Commissioner. So it is their requirement. If it is a cyber security incident it's a requirement to notify QGCIO but the breach notification is under the OIC requirements.

CA You receive breach notifications?

W If they're cyber security related, yes. Not necessarily otherwise.

CA Some of them don't relate to misuse of information?

W So there is no requirement to report instances to QGCIO for misuse of information, no.

CA But do you get reports?

W Yes, I get reports but not necessarily all of them.

CA Right, okay. So it's a voluntary process for the agencies to report breaches with respect to misuse of information UI-

W It is usually they request assistance. So the reason we get reports is they come to us for assistance in resolving the issues.

CA And what type-

W But there is no requirement to report breaches to me, no.

CA And what type of detail do they give you in request of the breaches?

W That varies depending on the situation.

CA And what assistance do you provide them with rectifying or UI-

W It varies, we provide a support to agency. So we may go and do an investigation, a part investigation for them or support them in investigating the outcomes. Or look at how they could avoid it in the future. We're more future-looking than we are past. So a lot of it is – an accountable officer will come to us and ask us to look at the situation and provide advice and provide advice into it, so in some senses that first look at what's going on.

CA Do you consider that there are currently sufficient regulatory regimes in place in Queensland?

W In response to what?

CA For information security?

W I believe so. I think we are – we are maturing and we're getting better at it and it requires a lot of work. But I believe the requirements are there, yes.

CA And you mentioned IS 38. Could you just expand on that a little?

W So basically the –it sets the official use of official usage. That includes both equipment data and work through and it looks at issues around usage. The policies are that departments must implement policies addressing employee use and monitoring and then their monitoring of those services. So the agencies have to set their own policies. There is no central policy on that. And but must ensure employees are aware of, understand and acknowledge their

responsibilities and policy obligations when using services facilities and devices. So it is about setting expectations on agencies to let their staff know what they're allowed and not allowed to do with ICT facilities.

CA And, just lastly, could you explain what Tell Us Once is?

W Tell Us Once is a current project that's looking at how we better share digital identity and attribute information between agencies, and also support our citizens as customers of the government in managing how we use their information. So it is around implementing some control. So an example will be if we have their address that they have provided to one agency, we'll ask for their consent to share that with other agencies, or not, and which agencies they wish to share it with. So instead of them having to fill out forms each time they go onto a website that that information would write it automatically.

So it is about sharing of identity credentials which there will be several. But it's also about how we share their attributes and share their personal information amongst different agencies so we can meet that balance between – one of the biggest complaints we get is I have to keep giving agencies the same information again and again and again. How can we make that better? So that work is – that project is underway at the moment and it is going through.

CA Just a little bit more on the effects on agencies of sharing information and the need for there to be a balance. Could you explain about One Child and Digitalised Licence.

W Okay two – it's Our Child. So after the Royal Commission into the death of Tiahleigh, one of the key issues was that the information wasn't shared from Child Safety to police in a good time. And it was a long period between her going missing and they realising that she was actually in care. So out of that was the development of a platform and a system that has enabled the sharing of initially both education and Child Safety information on all children in care in Queensland. What it has done though is actually not released that information. It has put it in a situation that as a policeman, if there's a report of a missing child, that policeman can go and look at those two sets of information on their QLite or on their QPRIME capability. But the information is not released. It's fully audited and they actually have to justify why they're going into that system. So that system logs all access, which one's been looked at, why they've been looked at and it's been quite successful in providing a really good way of sharing information without impacting on the ability for people.

Yes, it can't stop a photo of the screen etcetera but it does control – put quite a lot of controls in place around what is really highly sensitive information. What it has done is also provided the raw information not aggregated. So which can provide intelligence to a police officer. There's a different address on education there is in the Child Safety data; that might provide some intelligence to them. That system has now been broadened and expanded that out to several other agencies including people like the guardian. So bringing that information

together. So it is available during a high-stress situation. The challenge is usually if you don't do it automatically it will take too long to get that information out.

And at the moment we're working – Transport are looking at digitising the drivers licence which will have two advantages, one we'll be able to authenticate citizens through that as part of the digital ID through Tell Us Once. But also it should – because the ability to control – currently when you give over your physical licence all the data is available to anybody that sees that because it's got your address, it's got your birth date on it and it's got your name and your photo. The ability to authenticate, yes, you're over 18 without handing that information over will come with that capability.

CA Is there a second initiative with respect to digitised licenses?

W Second initiative? Well Tell us Once and digital licenses are the two aligned projects, so.

CA So is there any assistance provided to agencies and advice with respect to not collecting and storing superfluous information that isn't necessary to perform their function?

W One of the principles we're bringing into information is minimum viable information; do not collect any more than you actually need to to do your job. But also working with a lot of agencies around – in the past when we were in an analogue world they used to collect data to do things whereas it may be held by another agency. So a lot of the work we're doing with agencies as they're starting to go to a digital form of those, they may actually just be able to another agency to confirm. So one area is concessions, a lot of the time you need to collect data that a person is labelled – that has a disability is allowed to have concessions. Instead of collecting that data why don't you go – once we start aligning the digital ID we should be able to go to the agency that has the list of people with disability to get confirmed that they are, they have the disability sufficient to get that concession.

So instead of collecting extra data, find out where government already holds it and start working through how you can access that and get the confirmation from that agency that they have that approval instead of just collecting the data yourself. So we do collect data all the time and we collect the same data many times because of how we do business. How do we align that up and start saying – and a lot of that will be then, once we collect it once, getting consent from the citizen for them to say how we are allowed to use that again.

So it's all about building consent into our processes and working our way through that. And that should then ease a lot of the issues around a lot of data sitting on systems that is just there because we needed that for once-off, so working with those issues. It will never get away from big databases because that's where we stand, but it should reduce the risk.

CA Thank you, Mr MILLS. I don't have any further questions.

PO Mr MILLS just a couple of quick things. The initiative involving data sharing arising out of the Tiahleigh PALMER case.

W Yes.

PO What's the mechanics of that, was there a separate database created or access to an existing database UI-

W No, it's actually – it live feeds from the actual databases on a case by case basis as a request comes in. What it's done is matched the client number in both databases so once they request, that client – and with police so those three they've matched those. So the police are let in, "I'm after this person" and then that will draw that up. It then deletes it once that one's over. So it's not held. It's accessing the back end databases where the data needs to be anyway for business. It's not making another set of that data which is actually a really good outcome.

PO And that data is held by which agency? Is it Child Safety?

W Child safety are the home of that. So they control the system; police just access.

PO Can I just ask you generally about a form of control of access or more particularly the ability to target audit certain risk areas.

W Yes.

PO Are you aware of any initiatives in the data analytics area that might assist in target auditing?

W I suppose a parallel – and look I'll go back to cyber security. Cyber security is very parallel to access. They are both big data issues. And, as you heard police, the millions of accesses. So the only way we've managed to survive in a very hostile cyber security environment is to automate a lot of the checking of what's coming in to government. Right. So we do millions and millions of malware attempts to get through our gateway. We've automated a lot of that. So there is a parallel there. It's not cheap. It's expensive at the moment but it's getting better.

So there are systems coming along that will do that. I don't think any auditing that has manual – okay, yes, you've always got to have a human at the end but anything that's not automated or has some automated intelligence or assistive intelligence involved, it's just not going to be cost effective so over time there is also some really interesting new technology coming along around the ability to compare encrypted data. So that ability to take two or three disparate databases, encrypt them into the analytic system, the analytic system then tells

you these are the 15 that match each other. Then that's all you're going to look at.

So there is some really different, again, quite front edge, it's straight out of research, but that then gets rid of the having to try and de-identify data to do analytics which is actually proving less and less effective. So there is a lot of work going on in that space. The one thing I suppose I haven't mentioned is regardless of how we go the Commonwealth are bringing in data legislation and it is going to have an impact on us because actually it will by law require us to share things like Disability, Child Safety. So there is going to be a whole heap of change over the next couple of years in how we do that so we're probably going to have to get pretty well better at what we do and how we do it.

PO Tell me, does your office engage in any data analytics projects or are you just sort of monitoring or aware of what's going on around the place?

W We in a sense we set the policy. We don't do the projects. There are a couple of data, big data groups, so the – within treasury the statisticians office does a lot of data analytics, has for years. And actually has legislation that allows it to do that side and it is supporting a lot of the place-based activities on at the moment which are data based. There is a lot of data around Logan we're doing a lot of work on matching data and working it through but in a really structured and quite secure way. But also within other parts of HPW there is data capabilities being developed and worked through. It's recognised as next generation.

To me the challenge though is analytics needs to sit near the business because it's actually answering business problems. So it's not a back office issue. Some of the data wrangling work can be done separately, but it's really got to be driven at the business lawyer. And we have probably got a skill – it's a bit like cyber security, we've got to skill the business in how to do it and how to use their data and how to do better outcomes from than actually taking it away from the business.

PO Yeah, you've got to have a purpose in mind to start the data project otherwise you're just chasing your tail.

W Yeah and historically we haven't done data projects well. I kind of would say that probably, no, I don't think I've seen a highly successful data marked project. I think we spend a lot of money and not got much value. So I think small focussed within the business is probably a better way to go.

PO Thank you. Anything arising, Ms-

CA No, thank you, Chair.

PO Thank you, Mr MILLS. Thanks for coming. Thanks for your patience and you're excused.

W Thank you.

END OF SESSION