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 1 - MONDAY 11 NOVEMBER 2019
(DURATION: 27MINS)

Copies of this transcript must not be made or distributed except in accordance with any order made by the presiding officer concerning publication of these proceedings.

LEGEND

PO	**Presiding Officer – ALAN MACSPORRAN QC**
CA	**Counsel Assisting – JULIE FOTHERINGHAM**
HRO	**Hearing Room Orderly – KELLY ANDERSON**
W	**Witness – SANDRA SLATER**
LR	**Legal Representative – Mr G J HUMBLE, McCullough Robertson**

CA I call Sandra SLATER.

PO Do you prefer an oath or an affirmation?

W Sorry?

PO Oath or affirmation?

W An affirmation.

PO Thank you. .

HRO Repeat after me. 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.

HRO Thank you. Take a seat.

PO Thanks, Mr Humble. I note you're appearing for this witness as well.

LR And I understand I may have to seek leave to do so, Commissioner, on the basis that I've previously represented Mr SCALES.

PO Yes. I imagine that you've turned your mind on your instructions-

LR I have.

PO -to any conflict, and there is none?

LR No.

PO Thank you. You have leave.

LR May it please, Commissioner.

PO Ms FOTHERINGHAM.

CA Yes. Good afternoon, Ms SLATER.

W Good afternoon.

CA Are you the Chief Information Officer for the Department Of Transport And Main Roads?

W Yes, I am.

CA And your areas of expertise are information and communication technology?

W That's right.

CA And you run a leader team of more than 400 staff and contractors with an annual budget of $100 million?

W Yes, that's approximately.

CA And how long have you been with the agency?

W I've actually been with the agency – I started in 1990. I've been in CIO role since August 2017.

CA And over the course of that 25-plus year career, have you been within information technology roles?

W So predominantly in IT roles. My exposure with the TRAILS and the TICA solution since 2011.

CA And you have a Bachelor of Electronics Engineering and a Bachelor Of Applied Science and Computing from the -- degrees from the Queensland University of Technology.

W Yes, that's right.

CA And you mentor and provide, create opportunities for women working in the workplace?

W Yes.

CA And you established the first women's lean-in circle within your information technology branch?

W That's right.

CA So we're just talking about your information technological systems. And the databases that we're concerned with, for the purpose of this hearing, are the ones that hold the most amounts of confidential information of the public, so we're talking about TRAILS and TICA.

W Yes.

CA So in relation to those databases, are they password restricted?

W Yes, they are.

CA And who, if any, person monitors staff to ensure that there is not any password sharing?

W So I think in terms of password sharing, we certainly have a policy under our use of devices facilities and services for ICT in the department that certainly points people to not sharing passwords.

We do have a complex password structure required. And there's two levels for our internal staff via a network password that gives them access to TMR's computer environment holistically, and then there's also separate login passwords required into the TRAILS and TICA solutions.

CA Thank you. I did forget to ask you if you were given an attendance notice for today?

W I was, yes.

CA May Ms SLATER be shown the attendance notice.

W Thank you.

CA I would like to tender that document.

PO Exhibit 23, thank you.

ADMITTED AND MARKED EXHIBIT 23

CA For both of those databases, TRAILS and TICA, are there audit logs?

W Yes, we audit every change to the system. Every look up to the system is audited with the user ID. And all of those audit logs are held in a machine readable format, which means they can't be edited even by the IT staff.

CA And then what happens with those audit logs?

W Those audit logs are able to be reviewed and audited. There are a number of analytics and scripting that actually occurs nightly which actually checks for unusual access. I think you touched on that a little bit earlier with the Director-General asking about things like after-hours access, or the number of times certain things were accessed. There's a whole suite of things that are looked for there. So we have -- the Director-General touched on, we have a compliance area in our Customer Services and Safety Regulation division, which actually is, sort of, in a separate function to the customer services area. So there are a number of different compliance activities that run through the system overnight checking for unusual access.

CA And if there is unusual access, who's that reported to and what happens with that report?

W So it is referred to delegates within the business from the compliance area.

CA And what sort of timeframe does this process occur over, and what happens if there's a potential breach?

W So we've got examples. So with the overnight scripting, that certainly is available immediately once that's identified through the scripting. It is referred to the business overnight. And we have cases where we've seen that action taken within the one day's notice.

CA For detecting a breach?

W Yes.

CA And then what happens once one's detected?

W So then that's referred to the business delegates for taking the appropriate action.

CA And do you have access controls?

W Yes.

CA Could you explain to the Inquiry about that?

W Again, I talked about the two different login password requirements; one into the TMR desktop environment, and then into TRAILS TICA. So users are actually granted an access that needs to be approved by the appropriate business delegate. And each of those role types only permit certain functions within the system based on the role of that person in the Customer Services and the role that they have in the usage of TRAILS and TICA in their everyday business.

CA Any material that you've provided to the inquiry in response to our questions to you before now talk about Enterprise Grade Entity and Access Platforms and Granular Role-Based Control. Could you expand on that?

W So the Granular Role-Based control is really around certain functions, certain data only being accessible based on the role type. So I don't know the number offhand, but there are multiple different roles across the entire TRAILS and TICA solutions that are fit for different business purposes based on the nature of the role that that person's conducting.

I will say as well as in the business roles and people that are either in our Customer Services or maybe back end in the compliance and support functions, we also have specific IT roles. Undoubtedly, some of the IT staff need to have access to the data as well to be able to support the functioning of the system.

We do have what we call a privileged account where there are eight staff in the IT branch who actually have a privileged access around being able to process data changes if necessary. So they have a more complex – it is a different degree of password control there. And all of those accesses are reviewed very, very frequently.

CA And you employ the principle of least privilege to ensure that only those who need to access certain information can access?

W Absolutely.

CA Can you explain any more about that?

W So really, that's based on the minimum that you need to do, the role that you need to do. So, like I said, there's a lot of different access levels so that people are restricted to only the data and the functions that they need to do to conduct their work.

CA And so the access levels are individually assigned?

W Yes.

CA And updated on an annual basis, or more often than that?

W So there's reporting that is carried out within the IT team. We have quarterly reports that go to the managers for confirmation around the access. In terms of day-to-day practice, also where staff are exiting or going on leave, then that triggers the process for actually withdrawing the access.

There are also routine checks done against that in case that's been missed in that practice. So routine around those on leave. But also, the business, I believe -- I can't tell you how frequent that is, but they certainly have a process where there's reports generated on all access levels and regularly reviewed.

CA So I've got here that there's a six-monthly audit. And that the review in relation to extended leave and separation is a two-weekly review.

W Okay. Okay.

CA And the leave is if it is more than four weeks.

W Yes. So the IT team specifically have a quarterly review of the IT access of controls in the back end of the system. So I'd say those ones around the business controls.

CA Now, Mr SCALES talked quite a bit about the suppression service for two categories; the first category 1 including domestic violence victims and high-risk occupations, and the small business unit looking after those matters. Are you able to elaborate on anything in more detail to do with suppression service and the flags that are generated every time those records are accessed?

W So, again, any touch of any particular record inside TRAILS or TICA is audited. So we have logs against every access. The suppression policy, as the D-G mentioned, around levels 1 and 2, sort of, carry different restriction there. So we have an area in the business, the compliance area, who owns the suppression policy, and then in Geoff MAGOFFIN's team, in Customer Services, is a specific Identity Management Unit who administer that. So they're the ones who are able to actually go in and do the lock down. I'm not sure how many staff in that team then have access to the data. Within my IT team, it is then restricted to – two database administrators are the people allowed to access it from the IT group.

CA And in relation to proactive auditing, your agency employs extensive data analytics.

W Yes.

CA Could you explain about that?

W I was touching on that before around the data analytics that we run nightly. So, yes, we – there's probably multiple things there, looking for unusual use, but also around the integrity of the system, so, you know, during the day, for instance, one example would be when we take the biometrics for someone to have a new licence and they go through the proof of their customer details to have that licence issued. You know, we're able to scan the system overnight in case anything may have gone wrong, or potentially two images have ended up against the same record, for instance. So we have had one example where that had happened and was found immediately overnight in the scripts.

CA And do you have a specific data analyst unit?

W Again, that's in the business team. So in the compliance area.

CA And you provided in your responses to our questions preceding the hearings two examples of proactive auditing. Are you familiar with those?

W Yes.

CA So one of them was – they're both to access TRAILS and TICA. The first one was access – was on 29 June 2018. Are you familiar with that?

W Was that the one with the – I've got the two case, the email or?

CA The son.

W Yes.

CA And the proactive audit and monitoring outbound emails.

W Yes.

CA Because you haven't mentioned that you monitor out-bound emails.

W Yes. So on the secured network and I'm not sure if I mentioned before about we have, sort of, two levels of fire walls across the network for accessing in. So I think you referred to earlier citizens going via online services would come in via a fire wall at the Queensland Government network, and then they also come in via another fire wall into the TMR secure network, which is where we have the TRAILS solution sitting.

From an email perspective, we have multiple tools that we deploy around monitoring ingoing and outgoing that are able to detect things like if they're phishing emails or looking for language, or, in this case, we've got one of the tools there that can actually look at images and look for unusual strings of numbers, or things related to customer details. There was one example where we have had an outgoing email, that was an image picture taken or a ticket history, and—

CA Of the employee's son?

W Yes. And the – I don't know the particulars of it. And I will say from a segregation of duties, the D-G mentioned around the Ethical Standards Unit reports directly to him.

CA Yes, we can ask more—

W And I have an Information Security Unit who can work directly into Ethical Standards without my knowledge there. So, yes, my understanding of this one is that our email tools have been able to detect that it was suspicious. So it flavours as suspicious, and then got forwarded to the appropriate area in the business.

CA And the access was on 29 June, and the detection through that proactive auditing of the emails was on 2nd July.

W Yes.

CA The next one there was access on 18th December 2018 in relation to falsifying an 18 Plus card for the employee's partner.

W Yes.

CA And that was identified the next day by proactive audit of 19 December 2018 by the identity management unit in relation to identifying a photograph mismatch.

W Yes.

CA Can you plain more about that?

W That was the one I mentioned before that was found in the overnight check. Usually there's a lot of system controls when the information goes in there, if it goes through the standard process, but as you suggested in this case, we had an image that managed to get itself put against a different customer's records. And that was found in the scripting that was run overnight.

CA And Mr SCALES mentioned this earlier, but staff were informed about this database function for monitoring the functions?

W Yes.

CA All of the functions?

W Yes. So on both the TRAILS and the TICA login screens, there are clauses there that this is private and confidential information in these systems. And I will say also, even just with our standard departmental logins into our computers in TMR, there's an acceptance screen that staff have to accept around the terms and conditions of utilising TMR ICT facilities.

CA Do those warnings include the range of consequences that misuse of the information held on the system can be disciplinary and criminal?

W No, not on that front screen. I've just had a look at them. It says “Private and confidential". So there's a flag there, but it's only a one sentence.

CA Also your recording of the information is centralised in risk ware application. Can you explain about that?

W The risk ware application is our risk management solution in the department. So all the way through from our enterprise risk registers that the D-G was talking about earlier, through to unit-based registers, we utilise that as our system to support that.

CA And I think you mentioned earlier that with the auditing, the access users that aren't needed any more, they're removed from the system?

W Yes. So routine checks there around ensuring that we haven't missed anyone who has exited or is on leave. But also for all current access types, my understanding in the business is it is not just about checking that those people still have access to TRAILS and TICA, but it also reviews the access and the role by which they have access.

CA And the internal audit for access control was reviewed in April 2019.

W Yes.

CA To check the control ranges were appropriate. And then there's an external provider that has been engaged, and I think Mr SCALES talked about that, touched on that, and that's for an audit program in the 2019-2020 year?

W Yes.

CA I just want to move on to information sharing.

W Mmm-hmm.

CA Mr SCALES talked about having several different agencies where there's a need to share information, including the Queensland Police Service as an example. And your agency, it facilitates TRAILS access in three-ways; is that correct?

W Three-ways?

CA Three-way system-to-system web service.

W Yes.

CA To provide interface between TRAILS and the other agencies' information system.

W Yes. So particularly with the police, for instance, there is – there are some police branches that actually maintain and do some registration and licensing business, so they have direct access to TRAILS and TICA as an agent of TMR to do registration and licensing business. The other one via web services is an interface that's provided into the police QPrime and their field-based QLight system that can connect to TRAILS to enable them to do things like looking up of the photos while they're out on the road.

CA So there's the system web face, system-to-system web service, TICA and then SITECH Confirm.

W SITECH Confirm is an information brokerage service.

CA And all accesses are logged and auditable?

W Yes.

CA Now, for all of those information sharing arrangements that you have with the other agencies, there's either a memorandum of understanding or a service agreement with the other agency?

W My understanding is there is. I'm not across those. They are owned by the business area responsible for the data.

CA And do you know if there is auditing of the access?

W So any look up into our TRAILS database, yes. Any access to use TRAILS and TICA for the purpose of registration and licensing is the same as all our standard user controls. In the information brokerage, I can't comment. I would assume there's some type of reporting interface back to the business on all of those calls in.

CA I will just show you a memorandum of understanding with the Queensland Police Service, pages 1 and 4, but I've also got the whole document for you as well. That's from October 2014.

I tender that document.

PO Exhibit 24.

ADMITTED AND MARKED EXHIBIT 24

CA Are you familiar with that document?

W I don't know it in detail, no. I'm not a signatory or a party to the document.

CA No, but it is a specific information technology memorandum of understanding, so...

W	For the sharing of the data.

CA	Mmm.

Are you able to speak to that, or could you let us know someone else who can?

W	So in our Customer Service, Safety and Regulation branch would be the functional leader for the exchange of the information and the role that the police have with, one, being able to do the registration and licensing on our behalf, and the other also is the ability to look up the data to help them with their police business.

CA	I won't ask you in relation to that unless you know-

W	I can talk to the IT controls which is around the access controls into TICA TRAILS, as I mentioned earlier, or all the login and all the look ups.

CA	It was just in relation to – the memorandum of understanding stipulates that the security obligations, who has them for sharing the information, and says that the responsibility for ensuring appropriate use rests with the receiving agency. So the police.

W	Yes.

CA	And as your agency is owner of that information whether there's an audit of the police's security management of that information that is shared; do you know if that occurs?

W	I'm not aware. No. I can say that we have access logs against any access to the data or look ups to the data.

CA	But once that information goes to the police, then you're not aware of an audit to ensure that that information, which has been shared is securely stored?

W	No, I don't have knowledge. No.

CA	Is the data sent encrypted?

W	So I can talk to the access into the system. So it is still being accessed from within the TMR environment. So we've got it in a private, trusted network fire wall behind the TMR. And with the police, because they're also within the Queensland Government, we also co-exit within the Queensland Government network, so it is within the trusted environment there.

PO	So you’re not transmitting the—

W	We’re not transmitting it, yes. My understanding is it is looked up directly from the interface into TRAILS via the web services, yes.

CA Thank you. No further questions.

PO Thank you.

Mr HUMBLE, do you have any?

LR I've just one question: so Ms SLATER, who within the TMR department do you think is most able to comment about the – speak authoritatively about the memorandum of understanding.

W I believe that would be Andrew MAHON who is our General Manager of Land Transport Safety and Regulation.

LR Thank you. No further questions.

PO Thank you.

CA May Ms SLATER be excused?

PO Yes. Thank you, Ms SLATER, you're excused.

They're the only witnesses today?

CA Yes, they are, Chair.

PO Thank you.

So we adjourn until 10 tomorrow morning.

HRO This hearing is adjourned.