CRIME AND CORRUPTION COMMISSION

TRANSCRIPT OF INVESTIGATIVE HEARING

10 **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 5 - FRIDAY 15 NOVEMBER 2019
20 **(DURATION: 45 MINS)**

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

30 **PO   Presiding Officer – ALAN MACSPORRAN QC**
CA   Counsel Assisting – JULIE FOTHERINGHAM
HRO   Hearing Room Orderly – KELLY ANDERSON
W   Witness – JAMES KOULOURIS
LR   Legal Representative – MUNASINGHE, S for Queensland Corrective Services

HRO   All rise. This hearing has resumed.

PO   Thank you.

CA   I call James KOULOURIS.

PO   Good afternoon. Do you prefer to take an oath or affirmation?

10 W   An oath, thank you.

HRO   If you put the Bible in your right hand and repeat after me. The evidence which
        I shall give.

W   The evidence which I shall give.

HRO   In these proceedings.

W   In these proceedings.

20

HRO   Shall be the truth.

W   Shall be the truth.

HRO   The whole truth.

W   The whole truth.

HRO   And nothing but the truth.

30

W   And nothing but the truth.

HRO   So help me God.

W   So help me God.

HRO   Take a seat. Thank you.

W   Thank you.

40

CA   Good afternoon, Deputy Commissioner.

W   Good afternoon.

CA   You are the Deputy Commissioner of the Organisational Capability for
        Queensland Corrective Services?

W   Yes.

CA   Been in that position since July last year?

W   Yes.

CA   And prior to that you were working in the New South Wales Department of Justice Corrective Services where you were the Assistant Commissioner for Governance and Continuous Improvement?

10   W   Yes.

CA   Your roles within the current position, your responsibilities are for workforce strategy, are people matter strategy?

W   Yes.

CA   Honours and awards, professional development, talent identification, succession planning and review, recruiting process review, human resource implementation?

20

W   Yes.

CA   And discipline review?

W   Yes, that's one part of my portfolio relating to our People Capability Command.

CA   And then you are also responsibility for strategy and governance-

W   Correct.

30

CA   -including organisational structural review, roles and responsibilities, governance structures, enterprise establishment, Corrective Services Act review and review of delegation?

W   Correct.

CA   You have a Master of Public Administration from the University of Sydney?

W   Yes.

40

CA   A Bachelor of Laws with honours from Macquarie University?

W   Yes.

CA   And a Bachelor of Economics Social Science?

W   Yes.

CA   In January this year, you became a member of the South Australian Government Better Prisons Advisory Board?

W   That's correct.

CA   And January 2016, until July last year, you were the board member for the Department of Justice of New South Wales Commission and Contestability Advisory Board?

10   W   Yes, that's right.

CA   Thank you for that.

       You were provided with an attendance notice for today?

W   I was. Thank you.

CA   Is that the notice?

20   W   That is.

CA   I tender that document.

PO   Exhibit 77.

ADMITTED AND MARKED EXHIBIT 77

CA   And I believe there is a more detailed – pertinent to your particular role within your agency organisational chart that you provided-

30

W   There is, yes.

CA   -that you provided us?

W   Yes.

CA   Yes. And I'll just show you a copy of that.

W   Thank you.

40

CA   I tender that document.

PO   Exhibit 78.

ADMITTED AND MARKED EXHIBIT 78

CA   I believe you have an opening statement. If you could provide that to us and also then fill us in on anything else that you haven't covered in that opening statement with respect to the organisational chart.

W   I would be happy to do that. Thank you.

CA   Thank you, Deputy Commissioner.

W   Good afternoon. I'd like to thank the Queensland Crime and Corruption Commission, the CCC, for inviting Queensland Corrective Services, QCS, to participate in Operation Impala. This provides an opportunity to review current QCS systems and processes and identifies strategies that can implement to promote a corruption resistant culture.

I'm appearing before the CCC as the Acting Commissioner. My substantive role is Deputy Commissioner QCS. I would like to personally acknowledge our dedicated and hard-working officers, many of whom are watching these proceedings, whether they work in our Community Corrections and Specialist Area, Organisational Capability, or Custodial Corrections. They all do a vital job in keeping Queenslanders safe each and every day. They often do this work in challenging, difficult and dangerous circumstances.

Our officers have the ability to make a real difference in the lives of others and to be a positive force in changing the behaviours and attitudes of prisoners and offenders. QCS expects the highest integrity from every one of our officers and recognises that Queenslanders rightfully expect that they discharge their duties ethically and professionally. In rare instances where one of our officers fails to do the right thing, or acts in an inappropriate or unlawful way, they violate QCS' ethical standards, erode the public's trust in their justice system and degrade our ability to achieve our core mission, which is keeping the community safe.

I wish to clarify one matter that was discussed during Commissioner MARTIN's evidence on Monday in relation to the improper access to and disclosure of confidential personal information. QCS takes all instances of improper access to and disclosure of confidential information very seriously as the Commissioner outlined. All such incidents are referred to the QCS Professional Standards and Governance Command, PSG, for the assessment. The PSG then refers all such matters to the CCC, or to the Queensland Police Service in the first instance. Should the CCC and the Queensland Police Service determine to refer a matter back to QCS to undertake an administrative investigation, then a QCS internal investigation and disciplinary process is commenced.

The Minister for Police and Minister for Corrections, Mark RYAN, and the Queensland Government have supported QCS to undertake a broad range of reforms to implement the recommendations made by the CCC in Taskforce Flaxton and to enhance community safety for all Queenslanders.

In July 2019, the Queensland Government allocated $25.2 million, over four years, to strengthen internal oversight capability, improve information security, and centralise key enabling functions within QCS. QCS has restructured its Organisational Capability division to address capability gaps across key enabling functions and to centralise their management. Six recommendations from Taskforce Flaxton will be addressed by the restructure and a further 13 enabled as a result of its implementation.

10 QCS has also established the Human Rights Implementation Group. This group is reviewing QCS policies and practices to ensure we comply with the Human Rights Act 2019. A training program is being implemented to complement this review and to promote awareness and understanding of human rights across QCS.

QCS does note that over the last three years allegations by the CCC about the misuse of information by our officers has increased. And we have commenced a range of reforms to build, drive and maintain a corruption-resistant culture, one that promotes disciplined, ethical behaviour, professional practice, particularly through early intervention, deterrence, education and systems 20 improvements.

The management of confidential information and information systems is an integral part of our operations. Threats to the confidentiality, the integrity and the availability of information held by QCS must be managed appropriately according to risk.

Following its establishment as a stand-alone department in December 2017, and in response to the recommendation of Taskforce Flaxton, QCS has developed a new approach to information management. We are implementing an 30 Information Security Management System consistent with the Queensland Government Information Security Policy to manage our information and cyber security risks. This ISMS is a key part of our governance framework and we're looking to identify and mitigate risks arising from information and IT systems loss, misuse, theft or failure.

We're also improving our cyber security defences including implementing the Australian Signals Directorate Essential 8, designed to remediate the eight highest risks to information security. And we have developed a suite of information security policies supported by new Information Security 40 Governance Framework.

Part of the first phase of this work is the implementation of a range of enhancements to the QCS Integrated Offender Management System, IOMS, to strengthen information security in accordance with the recommendation made by the CCC in Taskforce Flaxton, recommendation 27.

I now wish to address earlier evidence before Operation Impala in relation to warning flags placed on IOMS files that trigger a security warning to executive

management where a QCS officer accesses that file. I can inform the CCC that the raising of IOMS restricted access warning flags is governed by the criteria for warning flags indicated as procedure and that is attached as an appendix to our Correctional or Custodial Operations Practice Directives Sentence Management Admission and Induction. Currently the Assistant Commissioners for Custodial Operations, Community Corrections and Specialist Operations are authorised in the use of the restricted access warning flag.

10   We are committed as an organisation to developing our staff to promote a culture of leadership excellence across the organisation. As discussed in our public submission, training is provided to all our custodial officer recruits and Community Corrections officer trainees on the following topics, amongst others. Ethical conduct, privacy, the right to information obligations, the Code of Conduct for Queensland Public Servants, conflicts of interest, obligations related to the disclosure of information under section 341 of the Corrective Services Act, how to best use our IOMS system, and in our continuing development programs offered through our QCS Academy we include a specific three to four hour session on ethical decision making.

20   The QCS Academy is also embarking on developing a learning management system to provide a greater opportunity for QCS to deliver training to managers and supervisors, given our dispersed geographic dispersal across the State of Queensland. The people capability command is also overseeing the review of mandatory refresher training, including training that responds to the needs of the prisoner cohort and that targets high risk corruption areas. This work will be considered in line with a comprehensive review of human resource policy and practice that we have now started implementing in accordance with recommendations 13 and 14 of Taskforce Flaxton.

30   QCS has a zero tolerance of inappropriate access to or disclosure of confidential personal information it holds. The public rightfully has to expect the highest standards of integrity from all QCS officers as custodians of that information. The inappropriate access to or disclosure of confidential personal information is unbecoming of officers within a top tier forward thinking public safety agency. QCS is actively working to address inappropriate and unlawful behaviour through very short, medium and long-term initiatives, to build capability and to support the development of a mature corruption resistant culture.

40   These initiatives will be complemented by the implementation of significant improvements to the security and functionality of IOMS that we have commenced. QCS and myself personally are steadfastly committed to doing all that is reasonably possible to ensure the highest standards of ethics and professional conduct on the part of our officers when they exercise their official duties.

I would like to again thank the CCC for the opportunity for QCS to engage in the public hearing process and I welcome the opportunity to assist the Commission in this important work.

CA Thank you. Would you like to add anything more in relation to the organisational chart?

W Thank you for the opportunity. We've developed a fairly comprehensive organisational chart following a review with the assistance of an independent consulting firm to try and address the recommendations in Taskforce Flaxton around the centralisation of key functions. The Taskforce Flaxton report identified concerns around the consistency and quality of those services in a desperate model and the heightened corruption risk that is associated with the that.

So in the review of the organisational capability division, a number of new commands were created. So we've got a People Capability Command that essentially manages all the human resources and training requirements of the organisation, including the Corrective Services Academy, Culture Safety and Employee Wellbeing groups, among others. We have an Infrastructure Technology and Asset Services Command that centralises and delivers our digital services, our infrastructure, we have a billion dollars of infrastructure work underway over the medium term and $2.5 billion assets. Our Facilities and Assets Group, our Electronic Security Communications Unit, among others. We have a Financial Services and Strategic Sourcing Command which manages Finance, Procurement and Contract Management for a billion dollar organisation. A Professional Standards and Governance Command. That includes our professional standards capability, our investigative capability, staff intelligence function, corporate governance and risk management audit and assurance, among other functions. A Policy and Legal Command which includes a legal strategy and services group, our general counsel, right to information and privacy group, and an Operational Policy and Practice Development Group which was an another recommendation of Flaxton that we developed an internal inspectorate-like function.

We've got a Ministerial and Executive Services Command which combines our legislation group, our media and communications group and executive services. And the last command within this division is the QCS Strategic Futures Command. That has a Research and Evaluation Group, an Operational Performance Data Analytics Group to allow us to gain insights in performance and continuous improvements initiatives. An Innovation and Integration Group. A section called Partnerships and Strategic Engagement, looking at the way we engage with a variety of external stakeholders, including NGOs who help us deliver services. An Enterprise Strategy and a Human Rights Implementation Group. So that's the broad structure of the division I command.

CA Thank you. I just wanted to start off with talking about some database functions.

W   Right. Thank you.

CA   So we're interested, for the purpose of the hearings, in the databases, the main database for confidential information to be held in. So that's the Integrated Offender Management System IOMS.

W   Correct.

CA   And also the we're interested in the Suitability Checking, Recording and Monitoring, otherwise known as SCRAM system.

W   Yes.

CA   So SCRAM provides access to criminal histories and police briefs for prisoners?

W   That's correct.

CA   And it is owned by the Queensland Police Service?

W   That's correct.

CA   And IOMS, one of the types of information it stores is the health information of prisoners?

W   I don't believe it stores the health information of prisoners, is my understanding.

CA   What does it store?

W   IOMS is basically our system to manage our management of prisoners and offenders, whether they're in custody or serving orders and under supervision in the community. So it's basically our key operating system that allows us to conduct our operational activities.

CA   And there's password access in relation to both?

W   Yes, that's correct.

CA   And are there warnings at logon? Is there a warning prior to logon for both of them?

W   I'm not aware if there's a logon warning in SCRAM. I believe there is. There certainly is with IOMS, I can confirm that.

CA   And I might just go to that logon. I think you've provided us with a copy of it.

W   Thank you.

CA   That's the logon?

W That's the current logon.

CA That's the current one. I tender that document.

PO Exhibit 79.

ADMITTED AND MARKED EXHIBIT 79.

10 CA I see here there's the strong focus of what we've heard expert evidence about from Professor SMITH, to ensure that the range of possible sanctions is spelt out. So you've got the Corrective Services Act and also the Criminal Code there. And you also talk about the Civil Information Privacy Act?

W That's right.

CA So that's a good example of a warning for other agencies?

20 W We think it's very important to spell out to our staff, not only trying to enforce positive culture, but also, too, to identify for staff the ramifications of breaching personal information security and so they understand the full range of sanctions that would likely be applied in such a scenario.

CA Now, you mentioned the recommendation 27 from the Taskforce Flaxton report. Have you got that there?

W I don't, no.

CA I'll just show you a copy of Exhibit 5.

30

W Thank you.

CA So that recommendation, to replace the IOMS with a system that recognise information management security standards, and in the interim with priority, implement remediation strategies to reduce risk and identify information management as a strategic risk. So what remediation has occurred?

W The Government, as part of the State Budget released in July 2019, has allocated $2.5 million to Corrections to undertake that immediate remediation work. So 40 our approach has been twofold. The first part is to enhance the capability of ICT and ICT services within QCS. And so what we did there is have a comprehensive review undertaken of the structure. And that review has been finalised, and we're now actively recruiting to positions within ICT.

  The second element of the remediation work has been the engagement of a project manager, business analysts and programmers to start the detailed scoping, planning and then ultimate execution of remediation of the IOMS system to enhance information security. The key focus of that work initially

will be on a more proactive stance in being able to identify the inappropriate use of the IOMS system from both an auditing and a deterrence and a prevention aspect. So there's a number of elements to that that we're actively looking at. One is to enhance the ability to undertake proactive audits of usage of IOMS.

CA   What proactive audits currently happen? Are they manual, or-

W   They are. So generally what happens now is that an allegation is made regarding the inappropriate use of the IOMS system. We have an audit capability. So we can interrogate a user's access within IOMS, but that's a more reactive approach in that an allegation is made or a complaint is raised, and then the system is interrogated. And then the process I described in my opening statement of that complaint or allegation being forwarded to our Professional Standards Group who assesses it and then on to the CCC and others.

CA   Yes.

W   What we would like to do in the system is to have a more proactive approach and enhance our ability to prevent, detect and deter people from the inappropriate use of information. That $2.5 million will be very useful in providing us with the resources to undertake that work. And so what we're going to look to do is a whole range of things that we're exploring. One is to be able to identify unusual activity within IOMS; for example, where a record is accessed by multiple people at multiple locations concurrently.

Another element would be to develop personas for our staff. So we understand what our staff do, obviously, but in terms of a systems approach to have the IOMS system linked in with our establishment data and our understanding of what officers would require depending on their role and function and location by way of access. So at the moment the IOMS data sets or access to IOMS is not – sort of, the word I'm looking for is we don't compartmentalise, sorry, the information with IOMS. So once an officer has access to IOMS they essentially have access to the whole system, bar a few specific modules. So we would like to have the system designed so that we can limit access based on the principle of right, you know, the need to know. And so that officer's, depending on their role and function, will have access to the specific parts of IOMS not the system as a whole.

CA   And that's the, sort of, way forward now you have the resources?

W   That's correct. That's what we're doing now. So we've engaged a project team, the business analysts within ICT and they're now actively scoping and will deliver that program of works in the short to medium term. As a result of Flaxton, sorry, the recommendation.

CA   So there will be regular audits going forward?

W   There are audits now.

CA   What are the audits now?

W   The audits now are twofold. So there are particular modules. So the victims' rights module, the victims register rather, sorry, module. Audits are conducted on a weekly basis in terms of who has access to that system. That part, that module is locked down. Only those in the victims' rights register and some specific senior management have access to that part of IOMS and there's reports weekly.

10

In terms of IOMS access, it is twofold. There's the yearly audits of who actually has access to the IOMS system. But, secondly, there's an onus on our management to report changes in staffing, staff movements, resignations etc so that access can be terminated. But we'd like to move to a system that it's dynamic where that happens automatically.

CA   And for SCRAM you audit that every six months?

W   For SCRAM, that's managed by the QPS.

20

CA   Yes.

W   What we do is a relevant operational manager needs to make a decision based on the role and function of the officer as to whether access is required. We then provide that information to the QPS. They provide that user with an individual login and password. Each interaction, we understand that an officer has in SCRAM or each record is logged, and then it is our obligation, QCS, to notify police when the officer leaves that particular role and no longer requires the access and/or leaves the organisation and we notify police of that. Our regional or relevant managers undertake a six monthly audit of access to the SCRAM portal.

30

CA   With respect to information sharing from a database perspective, which agencies is there a requirement to do that with?

W   We share data with a range of agencies; Queensland Health, other law enforcement agencies for various purposes, including the CCC and the courts primarily.

40   CA   And is it the owner, the sender, from your perspective who is responsible to avoid the misuse of that information and safe storage?

W   I would say that would be a joint responsibility in terms of both us as an organisation and the recipient organisation as well. I'm often governed by the existence of MOUs which spell out the requirement for both parties to keep the information secure and I would expect the community would expect nothing less.

CA   Now, we have another witness from your agency providing some more detailed evidence in relation to discipline, but if I could just take you through a couple of things and if you're not able to speak to it-

W   Sure. Thank you.

CA   -then he will be able to hopefully.

W   Thank you.

CA   So you mentioned that all misuse of information matters are sent to the – could you just explain exactly where they go?

W   Yes. So all allegations of misconduct including the inappropriate access or use of information is referred to the Professional Standards and Governance Command. And what would happen there is they would undertake an assessment of that allegation. Our hope is within 72 hours or sooner. And then where there is an allegation as to the misuse of our information systems or information that allegation is then immediately referred to both the CCC and the Queensland Police Service.

In the event that those agencies refer the matter back to QCS for an administrative investigation, then we start a process of both, one, investigating that allegation, and when the investigation is allocated, it is then assigned to a decision-maker in the organisation. The decision-maker also writes to ask the officer to show cause so we can ensure the natural justice obligations we have we meet. And then ultimately, once the investigation has concluded, if it substantiates the allegation, the decision-maker is provided with advice in relation to, and a copy obviously of all the papers, but advice on the investigation the other matters pertinent to their making a decision as to the sanction they would seek to apply. But that's in matters where the CCC or police do not look to prefer criminal charges or take that matter further-

CA   -So you're a – sorry?

W   -at that point. Yes.

CA   So your agency deals with the criminal referral first, and then waits until that has occurred and then does disciplinary action.

W   Correct. We don't want to undertake any activity that might jeopardise a criminal investigation. But we feel seriously that those issues are very serious and should be referred for consideration of criminal action first.

CA   Could you explain where in that scenario the managerial discipline model sits?

W   That hasn't been developed or promulgated yet, but that's an approach we're looking at in terms of trying to strengthen the culture of ethical behaviour

amongst QCS. And so what we're looking to do is to bring in a number of elements to help us enhance culture including looking at early intervention, prevention and deterrence and to help equip managers locally to deal with issues before they escalate to issues where an officer then crosses the line and engages in inappropriate or unlawful activity. So that's a body of work we're undertaking now.

10 We've spent significant effort in re-designing the structure for the professional standards and governance command to bring in extra capability in response to the findings and the recommendations of Taskforce Flaxton we're embarking on a fairly large recruitment exercise as we speak to develop a whole series of new functionality, a staff intelligence function, enhancing the resources available to ethical standards group, and there's a large body of work of which that's a part.

CA Thank you. And with respect to when a staff member resigns throughout the process of the investigation and any disciplinary action, is it common – is it that you always pursue post-separation declarations where possible?

20 W Yes, it is. And I would argue that is best practice. My experience in other jurisdictions in having command of similar functions with an organisation would be that pursuing post-separation discipline where possible is best practice in terms of the seriousness with which those matters should be held.

CA And in your opening statement you talked about the education, some of the educational aspects. Could you explain in a little bit of detail the training that is specific to information privacy; namely, is it mandatory, assessed, participant recorded, online or in-person, and the content, does it include the whole range of sanctions for disciplinary and criminal?

30 W Sure, I'm happy to answer that question. So we undertake fairly comprehensive training on a range of ethical standards matters and that begins when custodial corrections trainees first start with our organisation and undertake their initial pre-deployment training. That's a 10-week course. A key part of that is around ethics, including the appropriate management of personal information, particularly that recorded on IOMS.

So there's a four-hour session on ethical standards, and that covers a whole range of issues; ethics, right to information, privacy, the appropriate use of our systems. And it is very much scenario-based training so that officers can get an understanding of the challenges they'll face in the workplace and how they
40 might best equip themselves to ensure they meet all their ethical and legal obligations. There's also a specific six-hour session on the use of IOMS and the appropriate use of IOMS. But in particular 30 or 45 minutes of that session is specifically on the acceptance agreement. So the declaration that our officers sign in terms of the appropriate use of IOMS, so it is on the custodial side when they first enter the organisation.

For our Community Corrections Officer trainees who return to the academy for a two-week program there is also very detailed training on ethical standards issues including information security.

In addition, we do a number of elements to train or inform our officers on best practice and the expectations around the security of information. Everything from screen savers to articles in our corrections news, to emails that are sent out. The organisation we now publicly disclose where we suspend officers and provide some detail on the circumstances involved. We have engaged a new privacy – senior privacy officer, and that officer will be tasked with updating our procedures on privacy and training staff across the organisation. And ICT have developed a training package around information security and IOMS, which we're very close now to rolling out.

CA   Can I just show you the IOMS Training Use Agreement and Confidentiality Obligations.

W   Thank you.

CA   So I note there under Informed Person the fourth to last dot point mentions the section 408E of the Criminal Code.

W   That's correct.

CA   So that's a strong message. I tender that document.

PO   Exhibit 80.

ADMITTED AND MARKED EXHIBIT 80

CA   There are a couple of – well, there's a policy and a standard about acceptable use, they're both about acceptable use of ICT services. We'll just go to the policy first and then the standard. I'll show you both at the same time.

W   Thank you.

CA   Just while we're getting those, your agency has updated their policy as recent as August this year.

W   That's correct.

CA   Yes. And how often do you review your policies?

W   Now with our additional capability onboard we'd be looking to review that policy at least annually.

CA   Thank you.

W   Or as circumstances may emerge.

CA   Now with the policy, it is easy and simple, clear to read, Professor SMITH said is best practice. However there is a little bit missing from the unauthorised use, that's page 3, under 4.4. It doesn't mention the Criminal Code in there, so it doesn't give the range of disciplinary and criminal sanctions. So would that be something you'd be looking to update?

10

W   Absolutely. In terms of creating a culture of corruption resistance, I think it is very important that we communicate to our officers what the sanctions may be should in the rare instance an officer improperly use or access information we hold.

CA   I tender that document, the policy. And then the standard, the same applies to that one as well. So you'd be looking to-

W   Of course.

CA   -to update that one. I tender the standard.

20

PO   The policy is Exhibit 81.

ADMITTED AND MARKED EXHIBIT 81

PO   And the standard is Exhibit 82.

ADMITTED AND MARKED EXHIBIT 82

30

CA   Now with the problem, the concern, the risks of misuse of confidential information, there is the – at times the underlying – and that comes out in some of the case studies – stress, anxiety, personal issues going on. And so to try to mitigate that risk what does your agency provide by way of well-being assistance and counselling and programs and the like?

40

W   That's a key or the absolute priority for us is the safety of our officers and it is a very important responsibility for QCS. So we've got a range of initiatives in place to support our officers. We have a contract arrangement with a private provider, SMG Health for the provision of employee assistance services. And they provide counselling, post-incident critical response and management support services. And this includes ten counselling sessions per year available free to employees and their immediate families. We've got a manager hot line which provides support and advice to managers and executives again through the SMG service provision. An on-site crisis response service following a critical or traumatic event that may involve our officers in the performance of their duties. And SMG also provide and ask the expert service which gives online professional guidance on a range of topics. Our staff also may have access to the networks of peer supporters that are trained to deal with specific support situations. And we've also identified the need to enhance our effort in

that area, so under the new organisational structure we've appointed a Director for Culture Safety and Wellbeing to head up a group in our people capability command and they will soon be recruiting specialised staff, experienced in employee assistance and organisational development to provide a first-responder role. And these in-house resources along with our contracted service provider we think are an important element in providing our officers the support they need.

CA Thank you. Thank you, Deputy Commissioner. I don't have any further questions.

PO Mr MUNASINGHE, do you have anything?

LR No-

PO Mr SCHMIDT, sorry, carry on?

LR No, I don't have any.

PO Nothing for you, thank you.

LR Yeah, no further questions.

PO Thank you. Thank you, Deputy Commissioner – or Acting Commissioner, I should say, you're excused. Thanks for coming.

W Thank you.

PO 2 o'clock?

CA Yes, thank you, Chair. Thank you.

HRO This hearing is adjourned.

END OF SESSION