COMMUNITIES, DISABILITY SERVICES AND DOMESTIC AND FAMILY VIOLENCE PREVENTION COMMITTEE

Members present:

Ms LE Donaldson MP (Chair)
Miss N Boyd MP
Ms AM Leahy MP
Mr MF McArdle MP
Mr MJ McEachan MP
Mr RJ Pyne MP

Staff present:

Mr P Rogers (Acting Research Director)
Ms L Manderson (Principal Research Officer)

PRIVATE BRIEFING—QUEENSLAND AUDIT OFFICE

TRANSCRIPT OF PROCEEDINGS

(In camera)

WEDNESDAY, 16 SEPTEMBER 2015

Brisbane

WEDNESDAY, 16 SEPTEMBER 2015

Committee met at 10.16 am

BIRD, Ms Daniele, Assistant Auditor-General, Queensland Audit Office

NATH, Ms Mayus, Director, Information Systems Risk, Queensland Audit Office

CHAIR: I welcome Ms Daniele Bird, Assistant Auditor-General, and Ms Mayus Nath, Director, Information Systems Risk at the Queensland Audit Office. I am Leanne Donaldson MP, committee chair and member for Bundaberg. With me today are: Mr Mark McArdle MP, deputy chair and member for Caloundra; Miss Nikki Boyd MP, member for Pine Rivers; Ms Ann Leahy MP, member for Warrego; Mr Matt McEachan MP, member for Redlands; and Mr Rob Pyne MP, member for Cairns.

This is a private briefing for the committee. It will be recorded by Hansard so that the committee has a record of proceedings. I need to inform you about possible publication of evidence taken in private. In accordance with schedule 3 of the standing orders, currently the committee does not intend to publish or present your evidence to the House. The committee has the power to decide to publish some or all of the evidence taken in private and the House has the power to order production and publication of evidence taken in private. If the committee decides it wants to publish all or part of your evidence, it must provide you with the opportunity to make a submission about whether the evidence should be published. I now invite you both to brief the committee.

Ms Bird: As Mayus was the director in charge of the child safety audit, we thought we would present to you the presentation that we prepared when we did our parliamentary committee briefings just after the report was tabled. Then we will open it up for questions if there is more information you would like to delve into in terms of the detail.

Ms Nath: I would like to bring to the attention of the committee that this report is about managing child safety information. It is not about managing child safety operations and it is not making any recommendations about how things operate. It is about how they manage information to achieve the outcomes that they set out to achieve for themselves. Because the department of communities provides care and coordinates a number of child safety services from both government and non-government organisations, there are many parties that collect, record and exchange personal and very sensitive information, and all of this must be kept secure and confidential. Sharing the right information with the right people at the right time is critical to the safety of children. Therefore, it is critical to their operations. This is reason we did the audit.

We focused on two key questions. The first question was: is the information available to the people who need it when they need it to make the decisions? The second question was: is the information secure? A conclusion was that the department does not have the balance right between availability of information and security of information. It is because the problem is quite complex and, as you would be aware, with the sensitivity of data, if you make it too available then people who do not have to access to it can have access to it and that can be detrimental. At the same time, if it is not available then that is also detrimental. So it is a very fine balance. It is a difficult task for the department. We found that the department could not provide sufficient assurance that that information was secure. The main reason for that was that staff take information out of the system to be able to use it, and when they do that they put it in less secure environments. That was our conclusion.

If we unpack that into availability as the first thing, the first issue that we found was that the department had not planned for information requirements of various parties within the end-to-end service chain. While they have planned for internal staff and what child safety officers in regional areas need and across the wide network internally—they have planned for that and provided systems for those—they have not looked at who else needs this information and what they can do to make sure the end-to-end safety chain is efficient rather than just their internal systems.

In 2004 the department implemented ICMS, and that was to provide statewide access to everybody. But the changes to the system really have not kept up with technology, because you have really good and new technology today that will allow for collaboration amongst the various parties. They use incremental amounts of money on ICMS to keep it updated to current versions and also

operational efficiencies internally—interfacing and all of that—but to be able to look outside to share that information they have not really put that technology in. Having spent $85 million, we believe that they can do a little bit better in this area.

When it comes to sharing, they share information through emails. Then the service providers take that information and they put it in their own IT environments. They could put it in SharePoint. SharePoint could be in a cloud environment. They could also be putting it in an IT vendor space where then they are dependent on the security that the vendor applies to that information. There is also duplication and out-of-date information. We found that there were about 1,009 school-aged children at the time of the audit where their school details in the department's system were different from that in the system for the education department. So there are two very well-developed new systems—Education has one and Child Safety has one—and we are not really making them talk to make sure that they interface and that there is data integrity between the two systems.

We also found that the department is not able to monitor overall trends of their child safety operations, if you like. They have individual cases for individuals. If you wanted to get down to the data for each child to see whether that child is going to school, you can find that. But if you wanted to aggregate it all for the director-general to know as a whole in a strategic way how many children are not going to school for example, that kind of information is not able to be produced—not easily anyway. It would take a lot of effort if one wanted to do it. We found that only 30 per cent of the school-aged children's information was up to date in ICMS.

We also looked at transition planning and we wanted to know at an aggregate level how well we are doing transition plans for children who have turned 15 and in the transition stage. We found that there were 1,130. Fifty-nine per cent of those were recorded as either enrolled in school or had completed school. The other 41 per cent did not have a record of enrolment in a TAFE college or anything of that sort. We thought that was an important aspect in the transition stage in making sure that the child is having some sort of education at that point in time to transition into adulthood.

The next part was around information security. If we cast our thinking back to 2009 when we did a full-blown security audit at the department, at that time we also published a report and we found that there were many opportunities for improvement in the security of their IT environment. When we looked at it this time, we looked at their five key systems and we found that they had done quite a lot of work. There was a lot of improvement in the security of those systems. So they had secured the system to recommendations of the vendors. They had secured the system to standards, although you cannot have the systems completely secure but they had put security in. The only thing is that, because the system does not provide the functionality that the staff need, they have to take the information out of the system and put it in a network drive which then gives access to other people who should not have access to that system.

Mr McARDLE: Even hacking as well.

Ms Nath: We did not hack.

Mr McARDLE: No. You did not hack but does it ease the hacking process?

Ms Bird: Or just ease the accessibility once you take it out of the secure system. We tested the systems. The systems can have all the security in the world but as soon as you take it out and use it in a spreadsheet or use it in something else and leave it somewhere insecure, unfortunately others can access it.

Ms Nath: So the risk of hacking is there, yes, when the information gets taken out. Also, when people left the department they did not reliably remove access which we think is something quite important. People's access should be removed when they are no longer with the department.

We also looked at non-government organisations. We looked at three of them. We found that that they were operating within the intent of the service level agreements which said that you should comply with the privacy legislation. So they had put processes in place to make sure that they complied with privacy legislation. However, the department did not set any standards for IT security. So they had then decided by themselves what kind of security they should put in. It was dependent on their own risk assessment. It was also dependent on their knowledge of IT. So when we did the audit they really welcomed our audit. They took all of our recommendations on board and they said, 'Come again,' because we actually helped them secure their systems.

Mr McARDLE: That is good.

Ms Nath: We have made a recommendation to the department that they should make those kinds of guidelines and standards available to the NGOs, because they want to do it.

Overall, the department has accepted our recommendations. We have a very good relationship with the department. We have worked together to come up with those recommendations. After the audit we have also had a meeting with the department.

Ms Bird: Yes. They are very keen to be proactive in terms of at regular intervals—'regular' being six months—coming back and having a discussion with our office in terms of informing us what they are doing around our recommendations. It is obviously not a requirement, but it is certainly something that they are proactively looking to do to make sure that they are meeting the recommendations of the audit.

Ms LEAHY: Obviously there are other organisations in government that probably would have dealt with similar things that you have made recommendations about. Rather than the department reinventing the wheel, has there been anything that the Audit Office can point to to say, 'There are a bunch of policies here,' or 'Here is how somebody else has actually done this,' so that it keeps that process moving through and the department may even improve some of that? Is that anything that has been considered?

Ms Nath: One that comes to mind straightaway that we though was really useful is the security standards. It has been done by one of the federal departments. I think it might have been the federal Department of Human Services. They have developed one for their NGOs and other parties that are using that information. We have provided that to the department and said, 'Here is something that is useful that you can use.'

Ms LEAHY: Otherwise, it might take them a while because they are obviously focused on other things. We do not need to reinvent the wheel.

Ms Bird: It is the accessibility side that is the biggest challenge in implementation from this audit. The security side is certainly tried and tested, and there is a lot of guidance and information for them to leverage on that side. It is the accessibility side of it with the number of parties involved across the service chain that I think is going to be the challenging area for them to look at. It is certainly not a quick fix when you are talking about the types of systems and functionality that they need to enable that collaboration.

CHAIR: For me, having been a user of the system—I was in the department around the time of the implementation of ICMS and understand some of the limitations, frustrations and challenges with it—even within the system there is sensitivity where some staff can access information and other staff cannot. I suppose there are different hierarchies of access.

Ms Bird: For different levels of staff.

CHAIR: Did you look at that access? Were there any issues in that area?

Ms Nath: No. That was well controlled.

Mr PYNE: I was interested when you talked about some of that more strategic information such as school attendance. You said everyone should want that. I think it would be such an important requirement and basic in addressing policy and looking at issues that that information is available at a higher level.

Ms Nath: We thought the same. I think it is really around the way ICMS was first designed. It was designed per child. It was designed for the person. It is a very individual way in which information is organised in the system. Then what we do need over the top of that is a layer that extracts that information and provides overall strategic views. Even for data-cleansing purposes, for example, some of the address details are not correct in the department system. You are not able to know that until you run those kinds of reports. That is not available in the system. You are right: if they want to draw reports, even for reporting for the Commonwealth government, it takes them about three months or so. By the time they publish it, the information is three months old.

Mr McEACHAN: Expanding on that analysis, has consideration been given to looking at what kinds of trends and analysis are to be considered, I guess, putting the horse before the cart and going, `Okay, what is it that we actually want to get out of the starter before we build a system that enables us to analyse the data? What is it that we are looking for that helps drive the right kind of policies, that helps solve problems as they come up?' Has there been consideration for that? Is that something that you look at?

Ms Nath: The first issue that we raised was around information planning. We were looking for information to see whether we have an understanding of what are the various information needs of people. Then you can collect those types of information, process them and then you can report them. We also noticed that the Carmody report had a fair few outcomes based reporting for the department.

We did not quite delve into that area, because that piece of work was already done. What we thought was also important to be done in tandem with the Carmody implementation was this information management piece. We only did this aspect of the work, but I think they already have that kind of information. As they are implementing our recommendations, they are actually implementing it with the Carmody project that they have underway.

CHAIR: The department has quite a large component of field staff who take information physically out of the office. Is there a policy or something in place on how they manage that outside the office? I do not know whether they still take paper—they print things and take it out. How do they ensure that information is secure once it is out?

Ms Nath: It is also based on staff's knowledge of the policies. That process is very manual and they rely a lot on manual records and physical files. When we did our audit we did not find any incidents of files lying around or people not taking care of the sensitive information. It felt like people were really wanting to keep everything secure and confidential, so much so that they did not really make it available when it was needed.

CHAIR: You can go too far one way.

Ms Nath: With the confidential side of it, everybody is very cognisant of that. Even the NGOs would say, 'That is privacy legislation, you cannot see this.'

Mr PYNE: I have to say that I have found privacy legislation to be an impediment to helping people on numerous occasions. Would it not be more concerning if someone like Act for Kids could not access information; do you know what I mean?

Ms Nath: Yes.

Mr PYNE: I understand the need for privacy and keeping information secure, but I see sometimes it is kept too secure so that the people who need to know do not know.

Ms Nath: That is right. That is what we are saying: there needs to be an awareness program around privacy legislation itself, as to what it says and whether it really stops you from sharing that information. When we went to the residential care facilities, none of the children in those facilities had healthcare plans, had education plans. It was just not available to people providing those services.

CHAIR: And they are all covered by confidentiality as well, so it is not a risk to the department that that information is going to be—

Ms Bird: No. And those are examples of information that exist that would have been helpful to share. It can go both ways.

Mr PYNE: Increasingly, more and more service provision is done by NGOs and not-for-profits and they are people who genuinely are in that space because they do want to help. They need the tools to help people.

CHAIR: You mentioned in the report 'cloud computing'. Is using the cloud in information sharing being considered?

Ms Bird: Do you mean instead of via Communities?

Ms Nath: I do not think we mentioned it in this report but we currently have—

CHAIR: You mentioned there might be options when you were going through it. It was an option.

Ms Nath: It was a collaboration, a collaboration tool.

Ms Bird: A collaboration option.

CHAIR: Like SharePoint or different things.

Ms Nath: I mentioned that some people are actually putting it in the cloud—the NGOs—but whether they were aware of the level of security they needed to have if they were putting something in the cloud, that was the question for us at the time. We did not believe that they had the level of security, although they put the security in when we went in and we started talking to them and showed them all the things that they could do. But we did not audit all the NGOs; we audited only three. The option is there for people to use the cloud and other collaboration tools as well, but they all need to do it making sure that it is done securely and—

CHAIR: That is another audit.

Ms Bird: That is another audit.

Ms Nath: Currently we are doing an audit on cloud computing.

Ms LEAHY: The cloud is quite good and has its benefits. I think the problem, being a regional Queenslander, is the lack of access to the cloud. That is the issue and the data transfer rates, say, if you are an officer of the department at Thargomindah. I cannot even get on Facebook in some places. It is going to be the problem of the lack of access across regional Queensland that will cause significant issues. The cloud is good and gives you great access and it gives great control over who has access, but—

Ms Nath: That is very true. There are other risks with the cloud as well that people need to take into account.

Ms LEAHY: The question is: where is that server? Whose jurisdiction does it sit in? Is it sitting in Indonesia? Is it sitting in America?

Ms Nath: That is right, and do we want it to be there? We thought the department should set those sorts of standards for the NGOs so that we know where we should put our information.

CHAIR: Does the department do training with staff around information security regularly or do they do their own checks to ensure regularly that that information is being kept securely?

Ms Nath: They do provide the training, but what we found was that when it gets to the NGOs the training on IT security is not there. Also, if the training on security is there, people are keeping everything confidential. As far as people go, everybody is doing the right thing. Their intentions are all in a good place. But it is also about collecting information, it is about updating it on time into the system and updating all of that information to be accurate information and complete information. I do not think staff always pay attention to that, because that is an additional job for them. The main job is safety for children. They are concerned about that. Putting information in is not something that the department has provided training in, as to how important and how critical it is.

CHAIR: To keep it up to date, yes.

Mr McARDLE: I pose the question also about what to put in. It is not just how to spell it, shall we say, but what data is important. Is that equally a concern that you have?

Ms Nath: That is right.

Ms Bird: That gets back to your point as well in terms of thinking ahead about what you do need to report on, what trends you want to be able to track. Obviously that then drives at the outset what data you need to collect and put into the system.

Mr McARDLE: If that is the case, is there a risk of corruption of the end data? If you collate the data together, if those who are inputting do not know what to put in, in a very broad sense, does that raise a risk as to the outcome not being as accurate as it should be, given that children have issues around their safety? Is that a potential as well, or not?

Ms Nath: I think the department is not entirely sure about the data when it comes to aggregation. There is a lot of work that goes into data cleansing and all that when they are actually reporting to the Commonwealth for that purpose, whereas when we were looking for how many children are not enrolled in schools we have just got records of 1,300 and we can just quote numbers. But do those children actually not go to school or is it that we have not recorded it properly? We do not know. We do not know how many children do not go to school at a high level.

Mr McARDLE: That is a fairly worrying comment that you have just made because, based upon that, the government will spend money or not spend money on certain policies, certain initiatives.

Ms Bird: It is a fundamental piece of information, you would think.

Mr McARDLE: Exactly.

CHAIR: Or how many children do or do not have healthcare plans. Without going into it manually, the department could not tell with any certainty?

Ms Nath: Unless you went into each and every child's record, but when we went into each and every child's record and did a comparison between the department of education data and the department of communities data, we found disparages in those as well. Because data is correct, the data integrity issues—

CHAIR: Data integrity is a big issue.

Mr McEACHAN: Interdepartment communication would be a massive advantage for managing the safety of the children and the development of policy. If your information about school attendance is accurate and a child is not attending a school regularly, that would indicate a need to look more

closely as there might be a problem there. Or if a child is presenting at hospital, from what you are saying, there just is not that communication?

Ms Nath: No, there is the communication. When we started the audit we saw some activities happening, trying to reconcile, but it just was not possible. They were not able to do it. It was too hard to do. Then we took the data ourselves and we started doing the reconciliation and we came up with all these exceptions. Presenting an exception to the department, then they were like, `This is only a record, but in actual fact they could be going to school.' What we are talking about in our audit is really 11,000 children who were under care at the time. Out of that, it was 1,000. If you need to go to individual ones and ring up to find out, it is a lot of work. By the time you get to it, they would have started going to school again. We were looking for outcomes like regular absenteeism or people who are regularly taken away from or suspended from school—things like that. We were not able to get to a number of those.

Mr McARDLE: With children in communities in the cape it has always been a concern to me how they record the attendance. They record in the morning but not post that as well. Is there a distinction between the data for children who attend school in the cape as opposed to those who attend in the south-east corner? Is there something there?

Ms Nath: We did not specifically look at that.

Mr McARDLE: Okay. That is fine.

Ms Nath: But you can get the information. Address details, school details are all available.

Mr McARDLE: That is okay. That is fine. Thank you.

Ms Nath: So I must say that the department staff do have the right intention. They are wanting to take care of the children. Child safety officers have a hard job, as you might know, Leanne. We are not sort of putting things out there to say, `Operationally no problems,' but they definitely need to manage their information differently. We thought with the Carmody recommendations, while they are implementing them, it is a good opportunity where they can get in and improve this procedure.

Mr PYNE: The one service provider who has contact with all children at some point is Education Queensland?

Ms Nath: That is correct.

Mr PYNE: Are you able to access information from EQ? Is that information available?

Ms Bird: We did for this to get the correlation.

Ms Nath: Yes. There is information about schools—about school attendance and also grades, NAPLAN results, if that is still around. All of those things are available at Education Queensland. The department of communities can request for and can get access. They are also trying to reconcile the data as well.

Mr PYNE: So would there be the chance that it could just sync every six months or something like that, or not really?

Ms Nath: It is a bit difficult. I think the systems a lot of departments have are a little bit clunky for that purpose. I do not think they were designed to collaborate interorganisationally; they are all for internal purposes.

CHAIR: I know when police report electronically, it is outside the ICEMS system.

Ms Bird: That is it. If you look at all the parties that need to come together from a child safety system, it is multiple departments, and that is a lot of what Carmody spoke to as well in terms of that need to work out how they can collaborate.

CHAIR: So potentially the security of all of that information outside that system is not as secure as it would be inside that system.

Ms Nath: Yes.

Mr McARDLE: With the education department earlier this year there was a glitch in regard to notifications going to the police. Did those notifications not get to Communities as well? I thought they had been put through to the department. Is there an issue about what did come through?

Ms Nath: We have not specifically done an audit in that space, but we do know that there was a computer glitch so information did not get passed after it came to Education—so wherever else it needed to go to, but it was only—

Mr McARDLE: But as a matter of tracking that, did you get a chance to track that information coming from Education to Communities?

Ms Bird: No. That happened post our audit.

Ms LEAHY: Is that something, though, that the Audit Office may look at in the future—how departments share that information? I think there was a firewall that caused some issues.

Ms Bird: On that particular one, yes.

Ms LEAHY: For instance, with the department of child safety, there is Housing, Police and Education. They all need to come together. I am just wondering if there is—

Ms Bird: On our strategic audit plan with the Carmody implementation underway at the moment, as you know, we nominate topics that we will explore as potential future audits. That is certainly on there. An aspect of that would be looking at what it recommended around that collaboration. Obviously we need to give them sufficient time to implement that. I am not suggesting that it is a next year. It is potentially the year after that it gets on.

CHAIR: Thank you both so much for coming along this morning and updating us. We really appreciate you briefing the committee.

Ms Bird: You are welcome.

Ms Nath: If you have any other questions, please feel free.

CHAIR: Yes. Thank you.

Committee adjourned at 10.49 am