LEGISLATIVE ASSEMBLY FOR THE
AUSTRALIAN CAPITAL TERRITORY

STANDING COMMITTEE ON ENVIRONMENT, PLANNING, TRANSPORT AND CITY SERVICES

(Reference: Inquiry into the procurement and delivery of MyWay+)

Members:

MS J CLAY (Chair)
MS F CARRICK (Deputy Chair)
MR P CAIN
MS C TOUGH

TRANSCRIPT OF EVIDENCE

CANBERRA

THURSDAY, 13 MARCH 2025

This evidence was originally heard by the Environment, Planning, Transport and City Services Committee during an in-camera hearing on 13 March 2025. After consultation with the witnesses who provided evidence at the hearing, the Committee resolved, on 5 June 2025, to make this transcript publicly available. For further information, please contact the Committee Secretary.

Secretary to the committee:
Mr J Bunce (Ph: 620 50199)

By authority of the Legislative Assembly for the Australian Capital Territory

Submissions, answers to questions on notice and other documents, including requests for clarification of the transcript of evidence, relevant to this inquiry that have been authorised for publication by the committee may be obtained from the Legislative Assembly website.

WITNESSES

Privilege statement

The Assembly has authorised the recording, broadcasting and re-broadcasting of these proceedings.

All witnesses making submissions or giving evidence to committees of the Legislative Assembly for the ACT are protected by parliamentary privilege.

“Parliamentary privilege” means the special rights and immunities which belong to the Assembly, its committees and its members. These rights and immunities enable committees to operate effectively, and enable those involved in committee processes to do so without obstruction, or fear of prosecution.

Witnesses must tell the truth: giving false or misleading evidence will be treated as a serious matter, and may be considered a contempt of the Assembly.

While the committee prefers to hear all evidence in public, it may take evidence in-camera if requested. Confidential evidence will be recorded and kept securely. It is within the power of the committee at a later date to publish or present all or part of that evidence to the Assembly; but any decision to publish or present in-camera evidence will not be taken without consulting with the person who gave the evidence.

Amended 20 May 2013

The committee met in camera[1] at 10.15 am.

STEEL, MR CHRIS, Treasurer, Minister for Planning and Sustainable Development, Minister for Heritage and Minister for Transport
McHUGH, MR BEN, Deputy Director-General, Transport Canberra and Business Services, Transport Canberra and City Services
WHITE, MR MARK, Executive Branch Manager, Transport Canberra and Business Services, Transport Canberra and City Services
KONTI, MS BETTINA, Chief Digital Officer, Chief Minister, Treasury and Economic Development Directorate

THE CHAIR: Good morning and welcome to this in-camera hearing of the Standing Committee on Environment, Planning, Transport and City Services for our Inquiry into the procurement and delivery of MyWay+. This morning the committee will hear from the Minister for Transport and officials. Thank you all for coming.

The committee wishes to acknowledge the traditional custodians of the land we are meeting on, the Ngunnawal people. We wish to acknowledge and respect their continuing culture and the contribution they make to the life of the city and the region. We would like to acknowledge and welcome any other Aboriginal and Torres Strait Islander people who may be attending today's event.

For the benefit of broadcasting and Hansard, please note that this hearing is being held in-camera. Given the private nature of this hearing, the proceedings will not be broadcast to the public, but they will be recorded and transcribed. Anyone participating via video conference—Ben—please ensure that only those required for the hearing are present in the room with you.

Please note that evidence given in a private hearing can be authorised for publication at a later date, either by the committee or by the Assembly, but this would be done in consultation with the relevant witnesses. We had a brief chat about this. We would, obviously, talk to you first. We gather that in the possibly 100 in-camera hearings that have been held only once was evidence published. So it is probably pretty unlikely, but we cannot give you any guarantee at this stage.

The hearing is confidential to the committee and the witnesses present at this stage. Minister, can I please ask you to confirm that everyone present is authorised to be here in attendance? Thank you.

If anyone takes a question on notice, please say, "I will take that on notice." That helps our secretariat.

First of all, we welcome Mr Chris Steel MLA, Minister for Transport, and officials. We have several witnesses for this session. I remind you of the protections and obligations afforded by parliamentary privilege and I draw your attention to the privilege statement. Witnesses must tell the truth. Giving false or misleading evidence will be treated as a serious matter and may be considered contempt of the Assembly. The first time you

[1] After consultation with the witnesses who provided evidence at the hearing, the committee resolved, on 5 June 2025, to make this transcript publicly available.

speak, please confirm you understand the implications of that statement and that you agree to comply with it.

We are not inviting opening statements. Our job here today is to ask the questions we need to ask to get the information we need to help us decide what to do in terms of publishing submissions. We may then have some other questions afterwards. But it is really important for us to get to that decision point, so we can make a responsible decision.

I will kick off, and my colleagues will make sure that we are asking those directed questions. Minister, we received David Pryce's submission. There are a number of submissions that talk about cybersecurity. At this stage, we have held back from publication of all of those. There is one in particular—did you receive that one that we sent?

Mr Steel: I do not recall seeing it, but I am happy to check that after this. I think the line of questioning is about the protocols. Firstly, I just wanted to say, with your indulgence, thank you for having an in-camera hearing. I think there has been—

THE CHAIR: Can I just get you to confirm the privilege statement?

Mr Steel: Yes. Sorry. I confirm and acknowledge the privilege statement.

THE CHAIR: Thank you.

Mr Steel: Over recent years, quite a lot of work has been done between states and territories and the commonwealth around cybersecurity protocols and how we manage incidents that come up. Playbooks have been developed for managing incidents, as well as a greater understanding of protocols around information that is shared publicly about cybersecurity.

I will hand over to the Bettina to talk a little bit about that, because that goes to David's letter and the nature of submissions that you might be receiving. But I guess the key point is that when vulnerabilities are identified we do not want to provide public information about those vulnerabilities, in case a threat actor uses them.

THE CHAIR: We understand. I might just jump back a bit though. I actually do not mind, Minister, if it is you or if it is your officials; we are not fussed. We just want to check: have you read, and do you understand, the two major vulnerabilities that have been described to this committee? One vulnerability is where people could go onto the website and get money that is not on their balance. That is described as the 'endless money loop vulnerability'. That is one major vulnerability. The other major vulnerability described was that people's personal information—including their names, their addresses, their credit card numbers and their passwords—may have been leaked to the internet.

Are we all on the same page? Have you seen the submissions that describe those two vulnerabilities?

Mr Steel: I have not, but—

Ms Konti: I have read and acknowledge the privilege statement. No, we have not seen the submission, but we are aware of those vulnerabilities because they have been disclosed to us. Those vulnerabilities—working with Transport Canberra and City Services, as well as their vendor, NEC—have been shut down.

THE CHAIR: Okay. So, with those two major vulnerabilities that I just described, you have not seen the submission.

Ms Konti: No.

THE CHAIR: That is a shame. I believe we sent it, but it sounds like we are talking about the same ones. Have those two vulnerabilities been addressed? Are those weaknesses—

Ms Konti: They do not exist anymore, as far as I understand.

THE CHAIR: They no longer exist? Okay. Are there any other major security vulnerabilities that have been identified by you, or by anybody else, that have been reported to you so far?

Mr Steel: Do you want to go back from the beginning of the program?

Mr White: Sure.

Mr Steel: I think there is quite a lot of discussion to be had about what actually occurred prior to launch date and then after the launch date, in terms of identification of vulnerabilities.

Mr White: Yes. Thank you, Minister. I confirm and agree with the privilege statement. Going back to that, as the minister referred to, cybersecurity vulnerabilities are ever-present. We need to understand that with the classification of them—you mentioned them as 'major'—there is a protocol that we follow to assess them. When they are in fact reported as a vulnerability, we investigate them and find out if they are a repeatable vulnerability—if we can also repeat the same process. So, they can be reported to us, but then we go and test that. When I refer to 'we', that is either TCCS or DDTS with the vendor. Then we check to see if the vulnerability does equate to what was reported. We then see what actions are required.

You mentioned two vulnerabilities. The "endless loop" is actually technically better described as an SQL injection, which is where you would establish a database and have that database set on automatic and start feeding in a piece of information and get that information to respond out of the system. That vulnerability was identified very early. It was actually identified in our community-based testing period—

THE CHAIR: Do you have a date for that, or a month?

Mr White: I believe it was 14 November.

THE CHAIR: Thank you.

Mr White: When other members of the public did report this, through responsible disclosure, we were able to know that that type of vulnerability was already addressed. So it was identified on the 14th, and—

THE CHAIR: Had it been exploited? Has that one been exploited?

Mr White: No, it has not.

THE CHAIR: Excellent. Great. Good going.

Mr White: On the 16th, it was remediated out of the system. With the other one, which is a claim to extract personal identifiable information, that vulnerability was also identified at or before ‘go live’. It was information that could not be exploited. So, again, by repeating the test from the submitted claim we were able to prove that, yes, the information could be shown, but the person could not do anything with it thereafter.

THE CHAIR: I do not understand that. I am not sure if my colleagues do? What do you mean—somebody could see the information, but they could not exploit it?

Mr White: Using pretty rudimentary technology tools, you could take some information out. If you were making an inquiry of the system, using these tools, it would then pass back your credentials. For example, if I were doing it, it would return my name. So that vulnerability was re-rated as not being a critical one, as in: it was not passing out information and was not able to extract large volumes of PII. All it could do was return you very own. We applied a mask to that almost immediately.

THE CHAIR: Mr White, you have not seen the submission that we sent across either?

Mr White: I have not.

THE CHAIR: That does not match up with what I read in that submission. It was described to us that it would not simply release to Mark White Mark White’s information; it would release to Mark White lots of other people’s information. And it was indexed in such a way that made it quite easily hackable. It was described to us as easily used in a phishing scam or a mass data theft. It is difficult because you have not read the submission. Are you saying that that is an incorrect—

Mr White: I believe that is an incorrect assessment. If this is the same vulnerability that we are talking about—

THE CHAIR: Here’s hoping!

Mr White: Then that information only returned the inquirer’s credentials. What the person—the reporter or the researcher—may have been referring to is: if I just change the next number, do I return someone else’s?

THE CHAIR: Yes?

Mr White: Well, we did that test—and with the next number, and the next number and the next number— and we did not get any other information.

THE CHAIR: It’s difficult, because we did try very hard to make sure we were all looking at the same information—

Mr White: Certainly.

THE CHAIR: How did you discover this? Where did you get this information? I just want to make sure—

Mr White: This was part of testing, and it was either reported in through the ACT Cyber Security Centre or through the Federal Government Cyber Security Centre—

THE CHAIR: Okay.

Mr White: Which is a standard process for all ACT government to follow.

THE CHAIR: I would have asked you if there was a notifiable data breach, but, based on what you have told me, I—I will ask you anyway: do you think there were any notifiable data breaches?

Mr White: No.

THE CHAIR: That sounds like it matches what you have described. Does anyone else want to jump in on this? What I have heard is that the categorization on this side of the table was different from what has been presented in submissions.

MR CAIN: The submission was on behalf of the ACT government, was it not?

THE CHAIR: We received a submission on behalf of ACT government from David Pryce, which I am certain everybody has seen. We received a submission from Patrick Reid, and there are a number of other submissions—

MS TOUGH: That go into it too.

THE CHAIR: Yes, that actually describe a similar thing. I think Patrick Reid’s was probably the best description. Patrick Reid has described it quite differently from that.

MR CAIN: Did any of the witnesses before us have involvement in any of those submissions from Mr Pryce and Mr Reid?

THE CHAIR: They did not—

Mr White: Mr Pryce is the Director-General of TCCS, and I—

MR CAIN: I know. My question was: did any of you have involvement in those submissions, with drafting or approving?

Mr Steel: No. I was certainly made aware that Mr Pryce was going to get in touch with the committee with some information about how, generally, cybersecurity vulnerabilities could be handled to make sure that they are not presented in a public way that would enable a threat actor to exploit those vulnerabilities.

MR CAIN: So, Minister, you are aware of that submission?

Mr Steel: I am aware of the fact that he was going to get in touch with the committee.

MR CAIN: Did you approve that submission?

Mr Steel: No, I was simply made aware of the fact that it was coming forward.

MR CAIN: And the content of it? To what degree were you aware of the content of that submission?

Mr Steel: Yes, I was aware of it.

MS CARRICK: And how could an actor—

Mr Steel: It is coming from government and from the director-general of the directorate that I have direct responsibility for, yes.

MR CAIN: And you were comfortable with the accuracy of that submission?

Mr Steel: From Mr Pryce?

MR CAIN: Yes.

Mr Steel: From what I recall of the submission, the nature of the content was around providing information about the handling of cybersecurity vulnerabilities. It was not necessarily presenting evidence, so to speak.

Ms Konti: I have awareness of that submission from David Pryce. If we are talking about the same one, it is the one where it is asking the committee to exercise a protocol or to refer submissions that talk about cybersecurity vulnerabilities to ACT government for review before you choose to publish them. That is the one that I am aware of. Most of the drafting of that came from my staff in the ACT Cyber Security Centre, within DDTS. So I have awareness that—

MR CAIN: So is it of concern to you that, as described, Mr White thinks the submission has made a misdescription?

Mr Steel: No. I think we are talking about different submissions. Sorry, Mr Cain.

THE CHAIR: I will just jump in. We have checked our records on the 6th. We did send to the Steel inbox and the DLO the submission from the member of the public. I am not sure why that has not been received. We will probably just get you to check your processes, because we were very much trying to have a conversation in which we had all looked at the same thing.

I reckon that the submission from David Pryce is pretty straight forward, and it does just ask us to check before publishing any reports of major cybersecurity.

MR CAIN: Okay. Thank you.

THE CHAIR: It does not confirm that there are any outstanding; it just asks us to check in. So we are all on the same page. The difference is the ones reported by members of the team.

Can I ask a couple of procedural questions? If this committee chose to send cybersecurity submissions to the ACT cybersecurity team—the name of which I temporarily forget—what would be the time period you would take to tell us whether those breaches had been fixed and it was now safe to publish, if we chose to do that?

Ms Konti: Pretty quickly.

THE CHAIR: Like a day, like an hour, like a month? Like sometimes we get eight months?

Ms Konti: A day or three, at most.

THE CHAIR: One to three days. That is a good range. Okay.

MS TOUGH: I have just found the submission. If everyone is happy, I am happy to read this.

Mr Steel: Yes.

MS TOUGH: It said:

> The second security venerability was found and fleshed out over the next two weeks. Shaun goes into detail on the timeline and scope—

That is another attached document—

> For the sake of the reader, the following details were leaked on a **public, unauthenticated** endpoint:
> • Full (first and last) names
> • Phone numbers
> • Email address
> • Physical (home) address
> • Password hash and salt (this is not as severe as you think [4])
> • Full MyWay+ Card number(s), CVV(s), and other info
> • First 6 and last 4 numbers of credit/debit card(s) (see [3] for risk evaluation)
>
> Not only were all of these details on the public internet, with no authentication, they were also very easy to index. All account numbers are serial (with small gaps). This means that within the range [600, 800], there is at least 30 users information. Scraping this is very easy. Just ask for user 1, followed by user 2, and so on until you have every registered user. This is why the federal government recommends the usage of random identifiers [5]. At the time of writing, we do not know if this attack has been used by a malicious actor. The information laid out above could,

> at the very least, be used for a very convincing phishing scam. At worst, there is a chance it could be used for mass identity theft.

Mr White: That is the exact PII vulnerability that we were referring to.

MS TOUGH: Yes.

Mr White: Again, the claim of being able to index the next record, and the next record, and the next record, was unable to be repeated.

MS TOUGH: Cool. Perfect.

Mr White: Subsequent to that as well, we also changed the encryption on those API endpoints. Therefore, that information could not be read without significant hacking of the encryption.

Ms Konti: The concerning thing about what you just read out to me was that there is a claim in there that has been found on the public internet—that information?

MS TOUGH: Yes, it was leaked on a public, unauthenticated endpoint.

Ms Konti: All of the information that we have says that there was no evidence that that information had actually made it anywhere outside of the MyWay system. That is my understanding of the vulnerabilities.

Mr White: Yes. And I do believe that if that is the information then it is the information of the researcher themselves, because they can only return their own record—or rather, they 'could' only return their own record, at that time.

THE CHAIR: We have come up with a list of documents that would assist our inquiry. It would help us if we can run through those and confirm that you could table or provide those shortly, before we see you again.

Mr Steel: Yes.

THE CHAIR: We would like to see them. You will set your mind as to whether they are public documents or not public documents, but these are documents that would help us. We are after the procurement plan, the evaluation plan and the original business plan—the BSR—of the scoping. Are these documents that our committee can receive?

Mr Steel: We would have to check the business case.

Mr White: That is right.

Mr Steel: It would usually be cabinet in confidence, but we can certainly check.

THE CHAIR: Can you check for each one of those, and if any of those cannot be provided please explain very clearly why.

Mr Steel: Sure, yes.

THE CHAIR: And can get them dated—

Mr Steel: Yes.

THE CHAIR: Please get them labelled and dated when they come. Were there any other documents on our list? The risk assessment!

MR CAIN: Yes. Make sure that is in there somewhere.

THE CHAIR: Yes.

Mr Steel: Yes. Absolutely.

MR CAIN: I would like to view that one—the risk assessment.

Mr White: Any particular risk assessment? Because, as I say—

THE CHAIR: We would like the first one—the dated first one.

Mr White: Yes.

THE CHAIR: And then we would probably like a description of how you changed, revisited and amended it. Obviously, risk assessments change over time. So we want to see the first one, and then we want to know what your processes were for maintaining it and applying it. Is that possible?

Mr White: It is an exceptionally large ask. I just remind the committee that going through a procurement—

THE CHAIR: Yes.

Mr White: At the beginning of the procurement we would undertake a risk assessment. At the midpoint of the procurement we would probably do another risk assessment. At the conclusion, and around the periods of contract signing and execution et cetera, there would be another risk assessment. Then, for the life of the program, there is an initial risk assessment and then it is almost updated monthly, if not weekly. I would also point out, when it comes to dealing with cybersecurity, which I believe is the remit of this session, that is a separate risk assessment.

THE CHAIR: Sure. Is it possible to provide us with those first initial risk assessments? And then the description you have just given us, if that was what was applied during the life of the project: here is how we updated and used this. Is that too big an ask?

Mr Steel: So you are interested in the procurement side? Because that is the earliest—obviously it starts with procurement and then moves through. Is that what you are talking about?

THE CHAIR: We would like to see the original documents. I think the information we are after is: what did you originally think the project was going to look like, and what documents did you have in the original procurement? We are not asking for the contract at this stage, because I reckon that is going to be pretty complicated. But we are trying to get a sense of what the project was at the beginning, who was responsible and who turned their minds to these things. And then just a description of how these things work. We can come back if there are more documents. Have I got that right?

MR CAIN: One thing I know that would help me—and it may help my fellow committee members—is some sort of document that tracked how you dealt with risks and evaluated them and re-evaluated them and what actions were prompted by evaluating your risks as you went on the journey. I do not know if you have a summary document of that. It would kind of make sense to have something like that so you can keep track of the management of those risks.

Mr White: Yes. Certainly all procurements and delivery of major programs, like MyWay+, fall under the ACT Risk Management Framework. There are very robust policies, procedures and frameworks in place that were adhered to. Effectively, in response to your request, we would be providing that. We followed that.

MR CAIN: Okay. So what went wrong?

Mr White: Sorry, I do not know what the—

THE CHAIR: Yes, I reckon that is a—

Mr Steel: I guess the point is that the procurement risk assessment will have different information in it than other risk assessments throughout the project lifecycle. In the submission, we referenced that the project team had engaged the services of CyberCX to undertake the cybersecurity threat risk assessment. So that is a specific assessment that was undertaken, looking at cybersecurity matters. For each different risk assessment, depending on when it is undertaken, we will be assessing the different types of risks, depending on where you are at with the project. So the one that relates to procurement is not going to include all the risks of the project implementation, because it is done at a particular point in the cycle.

THE CHAIR: I reckon an excellent way forward would be for you to write an index of the things that you think we have asked for. Before you go off and do the work, send it to our secretariat, who will check. We do not want to make you waste your effort. You can give us a one-line description of what each thing does, so we are not wasting anyone's time. That might be a useful way forward.

MS TOUGH: Yes.

Mr White: Yes.

THE CHAIR: Did you conduct an independent security evaluation of MyWay+?

Mr White: Yes, we did.

THE CHAIR: Can we see the certificate? Is that—

Mr White: It does not come with a certificate. It does come with a report. If we are referring to the same artifact, what we have got is the CyberCX report on the project assurance—or the cybersecurity assurance.

MS TOUGH: It sounds like the same kind of thing.

THE CHAIR: Was it conducted by someone different from the contractor?

Mr White: Yes, it is independent—absolutely—and was conducted by CyberCX, who are a world-leading cyber authority.

THE CHAIR: Great.

MS TOUGH: Yes, that sounds like the same thing—the reports.

THE CHAIR: Do we want to get that?

MS CARRICK: Yes.

MS TOUGH: Yes.

THE CHAIR: Is that possible?

Mr White: I am going to have to take that on notice.

THE CHAIR: Yes. If you cannot, you will come back and tell us why.

Mr White: Yes.

THE CHAIR: That will be alright. We will accept that.

Mr Steel: That might relate to whether there are any ongoing vulnerabilities that are identified, so we will check.

THE CHAIR: We are genuinely trying to avoid exposing unaddressed cyber security risks.

Mr Steel: Yes.

Mr White: Yes.

THE CHAIR: We are interested in the composition of the decision-making groups on this project—

MR CAIN: Yes.

THE CHAIR: by role or by name—the key decision-makers.

Mr White: Are you describing the governance structure of the program delivery?

MR CAIN: Yes.

THE CHAIR: Yes. Can we get a list of that?

Mr White: You certainly can.

THE CHAIR: I am going to stop talking and just check to see if there is any other critical information that we need to make decisions.

MS TOUGH: Going back to Ms Konti, if we were to re-provide the submission I read from, you would be happy to just triple check that it is exactly the same vulnerability that Mr White identified—

Mr Steel: Perhaps if we take it on notice?

MS TOUGH: Yes.

Mr Steel: I do not know whether the answers on notice are in-camera or not. But—

Unidentified speaker: They are.

Mr Steel: They are. Okay, yes. We might just respond to the entire submission and provide some feedback on, particularly, whether the vulnerabilities that were identified in that submission have been addressed or whether they are new, particularly in relation to the matter around whether it is available on the public internet.

MS TOUGH: It sounds like it probably is what Mr White identified, but this is just so that if we publish this it is easy to say, 'No, actually this never occurred,' or whatever the correct answer is.

Mr Steel: 'The vulnerability has been patched,' or—

MS TOUGH: Yes, the vulnerability has been patched.

THE CHAIR: Is there anything else on the cybersecurity issue that we need to—

MR CAIN: Obviously we are going to have public hearings on this. What do you think should have happened differently for this project to have been rolled out much more smoothly than it was?

Mr Steel: From a cyber point of view?

MR CAIN: Yes.

Mr White: Like with all major projects—and also in an evolving technology landscape—we constantly learn new things. Some of those learnings would be applied to this project if we were commencing it tomorrow. That would include perhaps a larger devotion of resource towards a cybersecurity assurance. It would perhaps include slight changes and improvements and upgrades to the risk assessments and different protocols being exercised in that space. Then the roll of independent assurance would be more prominent, rather than just part of the program itself. It would actually be part of the critical decision-making in going live.

That being said, I would also say that we followed and probably exceeded the governance guidelines on what was needed.

MR CAIN: Well, maybe they need reviewing. Obviously, tapping onto a bus, travelling on it and tapping off again happens around the world and has been happening for a long, long time. Why did the government not just implement something that had proven itself and worked, whether in this country or otherwise? Given that there are so many operating systems that have been operating for decades everywhere in the world, how could you not get this done much more smoothly and efficiently?

Mr Steel: The question probably goes beyond the cybersecurity matters—

MR CAIN: It does—

Mr Steel: Ben McHugh might be the best person to talk about that. But, actually, in Australia, we had a travel-card-based system with the previous MyWay system, where we were enabling tapping on and tapping off public transport. That is similar to other systems around Australia, including those—like myki, for example, in Victoria— that do not offer the capability and have systems where debit and credit cards cannot be used. Although Victoria are also looking at implementing that system, as we have done.

I will hand over to Ben McHugh. The ACT government's submission outlines NEC's previous involvement in some other ticketing systems around the world that have provided this capability. We have been trying to leverage off that with the program partner to deliver that system here—which is functioning as we speak. I will hand over to Ben McHugh.

Mr McHugh: Thanks, Minister. Thanks for the question, Mr Cain. I have read and understood the privileges statement.

I guess there are a whole range of reasons why we embarked on introducing a new interface with our public transport system. Ticketing is one of the components, but it was all focused on improving the customer experience and attracting more people to use public transport in our city over time.

Like all things, evolution occurs. In the technology space, that is definitely the case. The system that was replaced—the original MyWay system—was, from a technology perspective, very much past its use-by-date and its functionality. Our ability to even maintain and manage that system was compromised by the age of the technology. So the commitment to replace that was multifaceted, but the customer experience and the attracting of more people to public transport was at its core.

In procuring a partner to deliver that system we did require a demonstration of experience in delivering similar systems in other jurisdictions. NEC were able to do that, and there are references to those systems and that experience in our submission to the inquiry. We would be happy to pass that question onto NEC for them to demonstrate their experience.

The commitment to providing the best possible experience for our customers in Canberra on public transport was there. We think providing modern, account-based functionality in that engagement—and through payments and through journey planning and a whole range of other improved technologies—is the best way to encourage more people to use public transport in Canberra.

MR CAIN: Why not just use New South Wales's system?

Mr McHugh: Minister, I am not sure if you want to respond?

Mr Steel: No. I'm happy for you to respond.

Mr McHugh: Because that technology in itself, Mr Cain, is already outdated. It will need to be replaced. I am aware that New South Wales are already embarking on replacing that system themselves.

Mr Steel: I think it is also about the contract that that particular proprietor has with Transport NSW and the New South Wales government; it is not as simple as just being able to tap into that contract. That would require agreement with the proprietor, which is effectively a procurement activity that would have to be undertaken.

As outlined in the submission, a range of procurement activities were undertaken by Transport Canberra in developing a next generation ticketing system for Transport Canberra. The initial series of procurements were not successful, because they did not provide value for money based on the valuation of those tenders. That is why the last tender process went out, which had a revised scope, which was, particularly, not to include cash payments for public transport. We think that elicited a wider range of tenderers that were able to come forward.

Transport Canberra then secured the services of NEC through that process, for a contract of $64 million over 10 years. When you look at ticketing systems around Australia—noting that the size of this is smaller—it is a considerably smaller amount of money than other jurisdictions have procured ticketing systems for which provide similar functionality.

MS CARRICK: If NEC has demonstrated it has provided robust ticketing systems, presumably the cybersecurity is robust in those systems that they have delivered. So where were the vulnerabilities introduced in this system? Was it additional functionality that introduced vulnerabilities? My question is: if NEC delivers robust ticketing systems, how were these vulnerabilities introduced?

Mr White: Do you want me to answer that, minister?

Mr Steel: Yes.

Mr White: I think I made the point before that there is a rapidly evolving technology landscape around us, including a rapidly—probably a more rapidly evolving—cyber threat that is occurring. Those who are protecting are running slower than those who are attacking, simply put.

The challenge for a company like NEC—again, I cannot speak on their behalf, and I am happy to take this question on notice so that we can get NEC to respond to it. But any global technology company has the same challenge, which is: their existing technology base over time becomes vulnerable. It was not vulnerable yesterday; it is today. It is just the nature of it, because, as I say, the attackers are evolving and running faster than the defenders.

Of the vulnerabilities that have been identified, they are being managed, being assessed, being treated and being mitigated in a very judicious manner. That is being done with the speed and haste that I have expected from my 35 years of experience in being involved with technology. So I actually see NEC as a very active partner with us in addressing anything related to cybersecurity.

MS CARRICK: If vulnerabilities were to be published now, you would be able to say the ones that have been identified have been corrected—have been fixed. There is always ongoing monitoring, but the ones so far that have been identified to date have been fixed—

Mr White: For those that we are aware of, absolutely.

MS CARRICK: Thank you.

Mr Steel: Just in terms of understanding the system, I think there is a misunderstanding that may be prevalent in the community about the procurement of the system and what the system actually does. I think the misunderstanding is that it is a totally customised system for ACT government. Our submission goes into a little bit of detail on how that is actually not the case.

Having said that, there are always integrations that are required with ACT government systems. One of those was the ACT Digital Account. I might hand over to Bettina to talk about those integrations and what we brought in. That did evolve over the project's development.

Ms Konti: It did. There were two sub-projects that were led by my group as part of the MyWay+ program. The first was the ability to integrate the MyWay system into the ACT Digital Account, so that people in the ACT who had a digital account could use their digital account to buy tickets. And there is future intention for people who are entitled to a concession to be able to get concession prices for tickets, automatically, because we know who they are and know that they are entitled to a concession. So that was the vision behind getting the ACT Digital Account in for use with MyWay.

We understand now that 60 per cent of people who use MyWay are using it through the ACT Digital Account. That is good. Importantly, the ACT Digital Account has very high and very robust security around it. When that vulnerability—one of the two that you were talking about in that submission—was identified, NEC brought their system down and we disabled connection to the ACT Digital Account immediately. We did not put it back together until that vulnerability was confirmed as corrected.

The other sub-project that we led was the integration of the MyWay system into the core finance system of the ACT. Obviously, the ticketing system collects money from tickets, and that needs to find its way through to the back end of the financials of the ACT government to put into bank accounts and those kinds of things. They were two projects that we led as part of this program.

THE CHAIR: Thank you for your time. You may be asked some of the same questions again. That is because this is an in-camera hearing, and sometimes we need to get things on the public record. So do not get frustrated if you get asked the same questions in a public hearing as you have just been asked.

We will deliberate, and we will be in touch shortly, I would imagine. On behalf of the committee, thank you for your attendance today. I do not think we had any questions on notice, but we have got a number of documents on notice.

Mr White: Yes.

THE CHAIR: Actually we did have some questions on notice! James is paying attention!

We are very happy to see that index before we see the extensive document search, to make sure that we get the right documents. We would love those answers within five business days, which I think is your statutory requirement in the standing orders. We would love you to please adhere to that very strictly. We are trying to get evidence in before the hearings. If we cannot resolve that quickly, we may have to go back to parliament and get an extension of time. If we can get things quickly, we can stick to our statutory timelines.

A transcript of proceedings will not be distributed in the usual manner, due to the confidential nature of this hearing, but arrangements to view the transcript can be made if required by contacting the secretariat. I imagine you might want someone in your team to have a look at it, so get in touch and do that.

Thank you to our witnesses, who have assisted the committee through your experience and knowledge. Thank you broadcasting and Hansard. We are now closed.

The committee adjourned at 10.56 am.