QON No. 31

Legislative Assembly for the Australian Capital Territory
Standing Committee on Environment, Planning, Transport and City Services

Inquiry into the procurement and delivery of MyWay+

Answer to question on notice

Asked by: Ms Jo Clay MLA

Addressed to: Minister for Transport

Reference: Minister for Transport – Transport Canberra and City Services

Hearing: 01 May 2025
In relation to: Data breaches and vulnerabilities and Credit card and password details and timings
Question received: 13 May 2025
Answer Due: 21 May 2025

In the in-camera hearing on 13 March 2025, I discussed one of the data breaches with your official Mr White, being the 'claim to extract personal identifiable information.'

Mr White said 'That vulnerability was also identified at or before go live... And it was information that could not be exploited. So again, repeating the test from the submitted claim. We were able to actually prove that, yes, the information could be shown but the person could not do anything with it thereafter... Okay. So using pretty rudimentary technology tools you could take some information out, so if you were making an inquiry of the system, using these tools, it would then pass back your credentials. So it would say, for example, if I was doing it, it would return my name. So that vulnerability was rerated [sic] not being a critical one, as it is not passing out information, not able to extract large volumes of PII. All it could do was return you very own. And we applied a mask to that almost immediately.'

I said 'That does not match up with what I read in that submission. Does anyone – like 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.'

Mr White said, 'I believe that is an incorrect assessment. Because I believe the – if this is the same vulnerability that we are talking about... Then that information only returned the inquirers credentials. What the person may have been referring to, or the reporter that researched that, may have been referring to, is that if I just change the next number, do I return someone else's? Well we did that test, and we did not get any other information. And the next number, and the next number, and the next number... 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... Which is a standard process for all ACT government to follow.'

I asked, 'Do you think there were any notifiable data breaches?'

Mr White said 'no.'

Ms Tough read onto the record from the submission our committee received from Mr Reid. "The second security vulnerability was found and fleshed out over the next two weeks. For the sake of the reader the following details are leaked on a public unauthenticated end point. Full first and last names, phone numbers, email addresses, physical home address, password hash and salt, (this is not as severe as you think). Full MyWay+ card numbers, CVV, and other info. First six and last four numbers of credit debit cards. Not only were these details on the public internet with no authentication, they were also very easy to index. All account numbers are serial small gaps, this means that within the range there are 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 recommend the usage of random identifiers. At the time of writing, we do not know if this attack has been used by 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 said, "So that is the exact PII vulnerability that we were referring to... And again, the claim of being able to index the next record, and the next record, and the next record, was unable to be repeated... so 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."

Minister, you have since provided conflicting information to the Assembly on these points:

(1) What is Mr White's role in the project?

(2) Why as recently as 13 March was Mr White's advice to a parliamentary committee wrong?

(3) Why didn't you, the Cybersecurity team, Transport Canberra and NEC understand these issues when they were clear to a member of the public and disclosed to you on 2 December?

(4) Why didn't you, the Cybersecurity team, Transport Canberra and NEC understand these issues when they were clear to a parliamentary committee made up of politicians with no technical expertise?

(5) Why wasn't testing by ACT Government and NEC able to replicate and detect the security issue that allowed one person to access another person's information?

(6) Did ACT Government or NEC contact Mr Reid after he made his first responsible disclosure? If so, what were the details of that contact?

(7) If MyWay+ followed the standard process all ACT Government digital projects follow, how can you be confident that other ACT Government systems do not suffer from the same security issues that MyWay+ suffers from?

Chris Steel MLA: The answer to the Member's question is as follows:

1. Mr White is the Executive Branch Manager, MyWay+ Program Director.

2. Mr White's advice to the Assembly was based on being informed by experts in the field of cybersecurity, include the Chief Information Security Officer (CISO) of the ACT, and his staff at the ACT Cyber Security Centre, TCCS' cybersecurity advisor, NEC Australia's Global Head of Smart Transport Solutions and their CISO and technical staff.

   Up until the NEC self-reported a data breach resulting from maintenance work by its own employees on 13 March 2025, Mr White was advised by all of these parties that there was, to that point in time, no reported data breaches.

   As reported in QTON 02 from the 13 March 2025 hearings, Mr Reid's claims were investigated by NEC, and a vulnerability was identified and corrected in 2024. At that time, NEC investigated whether a data breach had occurred as a result of the vulnerability, and concluded that there was no evidence to support declaring the incident a data breach.

   Subsequent and deeper investigations by NEC involving detailed analysis of access logs were undertaken on 9 April 2025. Based on those investigations, NEC determined that Mr Reid's claims did in fact represent a highly likely data breach. That is the first date that NEC advised TCCS that the vulnerability described in QTON 2 had resulted in a likely data breach.

3. As reported in QTON 02 from the 13 March 2025 hearings, the vulnerability was identified and addressed but the actual release of information was not identified at that time. There was no supplied evidence in Mr Reid's original disclosure, such as the extract of two or more records later provided to the Committee.

4. This is a complex technical area. Follow-up analysis by NEC was required to identify the data breach.

5. Refer to the answer to (4), where in addition to what is said here, making contact with the reporters of vulnerabilities is not a required practice, particularly where there is sufficient information provided to identify the vulnerability. In addition, the initial reports provided to the Territory did not clearly identify the reporter and their contact details.

6. As stated above, the ACT Government did not contact Mr Reid after he made his first responsible disclosure. This is not required practice and the information provided to TCCS had the reporter's details de-identified.

7. This questions is answered in full in the response provided to QON 11 from 27 March 2025 hearing.

Approved for circulation to the Standing Committee on Environment, Planning, Transport and City Services

Signature:  Date: 22/5/25

By the Minister for Transport, Chris Steel MLA