NEC response to questions on Notice from the MyWay+ Inquiry hearings on 26 March 2025

Question 17

The Committee received a number of submissions suggesting the system was hackable from during user testing until it was patched.

(1) How can you be sure that personal information of other users was not accessed during this time?

During the period leading up to and through user testing into the period of initial go live, NEC and the ACT govt performed ongoing penetration testing of the MyWay+ system which did expose some potential exploits of the solution which were addressed during this period. In addition, NEC was informed of potential vulnerabilities in the solution as reported by TCCS from public "responsible disclosure" of cybersecurity issues, which were investigated at the time and any issues addressed including software releases to address any potential vulnerabilities. This included a disclosure from Shaun Fulham received on the 13th of December through TCCS via the ACT Government Cyber Security Governance Centre, which highlighted potential issues with legacy API's.

At this time, based on our initial analysis of the data available, NEC did not see any indications of data breaches that indicated unauthorised data access, and confirmed the same to TCCS. Updates were made on the 14th of December 2024 to block APIs that were not used in the production system, but formed part of the solution – including those accessed by Mr. Fulham. However, recently due to information provided through this inquiry, NEC has further investigated logs from December and has identified that fare media list information for user's personal details was accessed, and we have shared this discovery and implications with TCCS.

(2) Can NEC demonstrate it had complied with the terms of Part 8 of the NGT Contract and the security-related requirements of the Statement of Work?

We are fully compliant with all access control and identity management requirements as outlined in the NGT Contract. Our systems implement unique user IDs for each staff member accessing Territory systems, with no shared or generic accounts permitted as specified in clause 70.6(c)(i). All passwords meet the ACT Government Password Standard, and multi-factor authentication has been deployed for privileged access in accordance with clause 70.6(c)(ii). All Operator users are authenticated from ACT Government Active Directory.

The same rigorous access controls have been extended to the customer portal, ensuring that all customers receive unique user IDs and must adhere to the MyWay+ password policy. All public users are either authenticated by ACT Government Digital Account or from MyWay+ Ticketing application based on user account type, created by public user. Password policy in MyWay+ Ticketing

application replicates policy of ACT Government Digital Account. This approach guarantees that customer access is appropriately restricted to only their own data and functionality within the system, maintaining the confidentiality and integrity of Territory Data across all user types.

We acknowledge that there was a lapse in controls affecting a subset of APIs which allowed logged-in customers to view other customers' data by manipulating data requests sent by the customer's browser. Exploitation of this vulnerability required non-standard technical knowledge and deliberate manipulation of requests beyond the scope of regular user activity. Upon identification, this issue was addressed with urgency, demonstrating our commitment to promptly resolving security incidents as required by clause 70.6. During this period, NEC implemented heightened security monitoring across the environment to ensure comprehensive detection of any potential issues.

This security breach occurred where a user was able to access unused API's, which was reported to NEC on 13th of December and remediated on the 14th of December 2024. In accordance with clause 70.6, we immediately implemented all necessary remediation measures as directed by the Territory. This included conducting a comprehensive security assessment, implementing additional protective measures, and preserving relevant evidence in line with clause 70.6(n)(b). Our incident response fully complied with the Territory's directions per clause 70.6(a-d).

Our access control measures ensure that only approved personnel with appropriate security clearances can access Territory Data, with such access strictly limited to the minimum necessary for performing contract obligations as required by clause 70.6(d). We maintain comprehensive audit logs that automatically record all system access attempts, ensuring each action is traceable to a specific individual user or account as mandated by clause 70.13.

(3) If yes then how can this be claimed when Canberrans personal and payment information was accessible?

Following the breach, we implemented enhanced mitigation strategies as specified in clause 70.6(c) to prevent similar incidents. This included implementation of rate limits for specific API calls, removal of unused APIs that were not meant to be available in the production environment, and stronger validation of API requests. Since 14 December 2024, no further breaches or successful attacks have occurred, demonstrating the effectiveness of our remediation efforts.

As required by clause 70.37, we have provided detailed security reports to the Territory documenting the incident, our response actions, and ongoing security improvements. We continue to maintain heightened security monitoring across the environment and have worked proactively with the Territory to identify and implement additional security procedures in accordance with clause 70.3, further strengthening the security posture of the system.

(4) Why did you set up a system that did not follow API structure (like REST), as recommended standard practice indicated by other witnesses such as Mr Patrick Reid.

NEC can confirm that all newly developed API sets within our Ticketing product are REST-based and follow modern best practices.

However, the ticketing system in question was built on top of an existing set of APIs that were originally structured to support our existing microservice architecture and the Customer Portal. These APIs were developed prior to our current REST-first approach and use an architectural style consistent with the platform and services available at that time.

While they are not RESTful by today's standards, these APIs aligned with the platform architecture in use at the time and supported internal integration requirements.

All APIs invocations were authenticated using a valid access token which is generated corresponding to a user session post user authentication process from MyWay+.

Question 18

Mr Sean Fulham stated in the 26 March hearing that he had accessed not only his own data, but also that of Mr Patrick Reid. Mr Reid stated that he also made data requests of the MyWay+ system that involved other users.

(1) Does NEC or the ACT Government have logs of all of these attempts to access other users personal and payment information?

NEC retains logs of all access to API's for a period of at least 6 months, which includes details of what data has been accessed in the system. Upon receiving this request from the Inquiry, NEC has further investigated this claim and reviewed the logs available; we have seen evidence of a spike of enquiries from single IP addresses/users against the API associated with retrieving Cardholder details based on sequential account IDs between the 5th of December and 10th of December, which is consistent with harvesting of data through repeated queries against incremental account IDs as per the claim.

This spike of API requests was against an unused API that did not have appropriate protections to prevent access of data other than for the registered user, which created a vulnerability that has resulted in a data leak as noted by Mr. Fulham and noted earlier, addressed on the 14th of December 2024, at which time this API, along with other similarly undocumented APIs, were blocked at the API gateway for the ticketing system, preventing further access.

In terms of data exposure, NEC's analysis shows there was personal data exposure on accounts in the account range #0 to #5830 on the 5th and 6th December; and then on the 9th and 10th December for accounts in the range #5929 to #9284. Further to this, log analysis has identified that a small subset of accounts with personal details linked to them were harvested. The reason this figure is smaller than the quantity of account records accessed is because not all accounts were either not registered as a user account or did not have registered fare media corresponding to the account which results in no data being returned to the query.

Investigations to date indicate that above instances are the only exposures of this type.

(2) Did NEC or ACT Government log Mr Fulham and Mr Reid's access of each other's data?

The logs have evidence of single IP address per occurrence harvesting data for other user accounts through repeated queries, which would be consistent with the claims from Mr. Fulham.

(3) If yes please provide this proof.

As per our obligations under our contract with TCCS, NEC will share this detail with TCCS, who will follow their own responsible disclosure and reporting processes in determining how this information is shared.

(4) If not, why?

Not applicable.