Government Response to the

9th Assembly Standing Committee on Administration and Procedure

Report 17 - Inquiry into possible structures of the committee system for the 10th Legislative Assembly for the Australian Capital Territory

Recommendation 9: Use of Zoom for Committee Public Hearings

Presented by: Chris Steel MLA
Special Minister of State
March 2021

Government response to the Standing Committee on Administration and Procedure, August 2020.

Security Risk of Zoom for Public Hearings

Introduction/Background

The ACT Government welcomes the Legislative Assembly's Standing Committee on Administration and Procedure *Report number 17 – Inquiry into possible structures of the committee system for the 10th Legislative Assembly for the Australian Capital Territory* (the Report).

The Committee inquired into the use of videoconferencing solutions to allow members to participate in public hearings from locations outside the Legislative Assembly during the COVID-19 Health emergency. In *Recommendation 9 - Use of Zoom for committee public hearings* the Report recommended that:

a. relevant ICT Security staff from Shared Services ICT to be briefed by relevant technical and Committee support staff of the OLA on how the Office configures and hosts its Committee public hearings via the Zoom platform; and
b. based on the results of that briefing, the ACT Government report to the Speaker on what, if any, particular aspect(s) of those arrangements pose ICT security risks.

Government position on Recommendations

Recommendation 9a – The Committee recommends that relevant ICT Security staff from SSICT to be briefed by relevant technical and Committee support staff of the OLA on how the Office configures and hosts its Committee public hearings via the Zoom platform.

Government response

Agreed. The Government supports the recommendation and notes that Shared Services ICT coordinated responses from the vendor (Zoom) technical staff and OLA Committee support staff on how the Office configures and hosts Zoom meetings.

On 25 October 2020, ICT Security met with the Executive Manager, Business Support to the OLA, to ascertain how Zoom was currently licensed, governed and configured.

ICT Security participated in technical discussions with vendor staff to confirm specific security mitigations implemented, including validating the vendor's responses to a standard security questionnaire.

In November 2020, ICT Security staff analysed these responses in a Security Risk Assessment report. Some aspects of this report were undertaken under Non-Disclosure Agreement (NDA) with the vendor and therefore cannot be tabled or released publicly.

Recommendation 9b – The Committee recommends that, based on the results of that briefing, the ACT Government report to the Speaker on what, if any, particular aspect(s) of those arrangements pose ICT security risks.

Government response

Agreed. The assessment finds that the Zoom platform, as assessed in December 2020, is a medium security risk and SSICT believes this is an acceptable risk for the OLA to host its Committee public hearings, which was the specific scope of use identified by the Committee.

The Security Risk Assessment was conducted on the Zoom platform as offered by the company in December 2020. This differs from the one that was used for the original Public Committee Hearings. Early in 2020 there was a significant number of high-profile security shortcomings of the Zoom platform. On 1 April 2020 Zoom acknowledged security issues in their platform and pledged to make a number of enhancements to address security and privacy. Zoom completed this security uplift in June 2020 and included:

- Introduction of 256bit AES encryption, in-line with industry standards.
- Transparency on the data routing, so users can tell where the call has traversed as well as providing customers the ability to control the call routing to specified regions.
- Significant enhancements to the password and meeting ID security, to stop external parties being able to guess meeting IDs.
- Better control for meeting owners to lock meetings and remove participants as required.
- Updates to their privacy policies to meet European and US standards.

In total, the security assessment identified 16 risks. Four risks are considered inherently low, with the remainder risks rated medium, which results in an overall medium rating. Risks related to confidentiality were not considered, given the content of the meetings is made publicly available.

In accordance with the ACT Insurance Authority Risk Management Policy (the standard used by Government), low and medium risks can be accepted with minimal further treatment however they should be monitored and reviewed periodically to ensure they remain tolerable. ICT Security recommended ten security risk treatments for OLA to consider, which, if addressed would:

- Reduce two risks from medium to low; and
- Reduce the likelihood of seven risks, primarily from possible to unlikely.

Four risk treatments were considered higher priority by ICT Security:

- Password enforcement to meet Cyber Security Policy requirements;

- Multifactor authentication to meet Cyber Security Policy requirements;
- Encryption to meet Cyber Security Policy requirements; and
- Enterprise licenses to ensure the solution is hosted in Australia and OLA can access all Zoom security controls.

The implementation of these recommendations would further improve the integrity and security of the system should the OLA decide to implement them.

The OLA currently has Zoom "Business" licenses. To further increase the cyber resilience of the platform, ICT Security recommends upgrading these licences to "Enterprise" at a total additional cost of approximately $1400 per year, any costs incurred to upgrade licencing would be absorbed internally.