



**LEGISLATIVE ASSEMBLY**  
FOR THE AUSTRALIAN CAPITAL TERRITORY

---

STANDING COMMITTEE ON JUSTICE AND COMMUNITY SAFETY

Mr Peter Cain MLA (Chair), Dr Marisa Paterson (Deputy Chair), Mr Andrew Braddock MLA

## Submission Cover Sheet

### Inquiry into Electoral and Road Safety Legislation Amendment Bill 2023

**Submission Number: 004**

**Date Authorised for Publication: 02 August 2023**

# Submission to the Inquiry into Electoral and Road Safety Legislation Amendment Bill 2023

Dr. Thomas Haines  
The Australian National University



July 27, 2023

There is no known way to construct an internet voting system which is secure enough for government elections. Furthermore, developing secure IT systems is notoriously hard and we see widespread vulnerabilities in internet voting systems in Australia and overseas; the existence, and time till discovery, of these vulnerabilities should temper the confidence of any legislative body or electoral commission in any internet voting system.

The Electoral and Road Safety Legislation Amendment Bill 2023 proposes to amend the Electoral Act 1992 to allow internet voting for overseas voters. This would allow internet voting to be used in the ACT on an ongoing basis rather than as a specific response to the COVID crisis, as in 2020.

Ensuring the possibility of voting for overseas voters poses an increasing challenge as the mail systems, on which the current postal voting solution relies, become increasingly unpunctual; this decline in postal services is the stated reason for the introduction of internet voting.<sup>1</sup> The increasing disenfranchisement of these voters certainly warrants changes to the Electoral Act. However, it remains dubious if internet voting is the best way to address this issue. I am very pleased to see 136H.3.b restricts the use of the internet system to overseas voters; however, other options still seem preferable (See Recommendation 1).

In the unlikely situation that the Inquiry is satisfied that no alternative—other than disenfranchisement—exists to an internet voting system, the legislation should still require that:

- the system meet established standards (Recommendation 2),
- the system is well audited (Recommendation 3), and the security limitations clearly communicated (Recommendation 4).

---

<sup>1</sup>Overseas e-voting, page 42, Report on the ACT Legislative Assembly Election 2020 - ACT Electoral Commission

## Recommendations

1. Carefully consider other alternatives to internet voting; if the stated reason is “the large number of votes that were rejected due to being received after the legislated deadline for receipt of postal votes”<sup>2</sup> then an obvious solution would be to move back the legislated deadline. Other alternatives to consider would include mailing the ballots to local embassies rather than directly to Australia.
2. Enshrine security requirements in legislation to protect against system being declared “secure” with minimal analysis. Specifically, we suggest following the Swiss model<sup>3</sup> of requiring at least the following before allowing the system to be deployed:

Authorisation is required for each individual ballot; it is granted if the following requirements are met:

- (a) The system is designed and operated so as to guarantee verifiable, secure and trustworthy electronic voting.
  - (b) The system is easy to use for the voters; account must be taken of the special needs of all voters wherever possible.
  - (c) The system and the operational procedures are designed and documented so that the details of the technical and organisational procedures can be checked and understood.
  - (d) The public have access to information appropriate to the addressees on how the system works and its operational processes, and there are incentives for experts among the public to participate.
3. Require that all significant attack surfaces of the system have been appropriately audited before the system is deployed. This analysis should include:
    - the system design,
    - the software,
    - the infrastructure and operations, and
    - penetration testing of the deployed system.

The scope, methodology, and high level findings of these audits should be public information.

4. Require the security limitations of the system be clearly communicated. For the public to make informed decisions about the trade-offs of having an internet voting system they need to be aware of the limitations of the system; the current propensity towards talking about the security of the system publicly in glowing and nebulous terms does not serve to inform the key stakeholder (the electorate) of the choice being made.

---

<sup>2</sup>page 43, Report on the ACT Legislative Assembly Election 2020 - ACT Electoral Commission

<sup>3</sup>Federal Chancellery Ordinance on Electronic Voting - Swiss Federal Chancellery - <https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsbedingungen.html>