Submission No 7

INQUIRY INTO CONDUCT OF ELECTIONS IN NEW SOUTH WALES

Name: Dr Vanessa Teague

Date Received: 13 July 2022

Submission to the Select Committee on the conduct of elections in New South Wales

A/Prof. Vanessa Teague
Thinking Cybersecurity Pty. Ltd.
and the Australian National University
vanessa.teague@anu.edu.au

July 13, 2022

This submission addresses the inquiry's fourth term of reference:

> (*d*) the use of the iVote system in the local government elections, the performance of that system and its implications, and future arrangements for use of the iVote system, including the possibility of a replacement software system,

I respectfully suggest that there are better ways to change NSW election conduct than by purchasing yet another replacement iVote software system. The system has been completely replaced at least once, following a series of serious failings in 2011. It was subsequently "refreshed" following serious security problems and some anomalous results in 2015. In 2019, the serious cryptographic errors we discovered were (at least partially) patched by the vendor during the election. In 2021, significant downtime constituted an acknowledged electoral failure, leading the NSW Supreme Court to void results in three local council elections. Please consider whether the series of failures, despite regular replacements and refreshments, has a more fundamental cause which will not be addressed by merely replacing it or refreshing it again.

The gap between substance and spin

I have written extensively about iVote in previous inquiries and will not repeat the details here, except to say that obvious failures such as those experienced during the 2021 Local Government elections are not the worst thing that could happen. iVote's most serious problem is the risk of *undetected errors or fraud* leading to an election that may seem to have progressed without incident, but actually elects representatives who are not the ones chosen by the people. The main difficulty, which does not have a known and usable solution, is allowing voters to securely verify that their electronic vote accurately reflects their intention. iVote continues to fail because it purports to solve an unsolved problem.

Even the most recent security analysis commissioned by NSWEC[1] identifies several serious problems, including hardcoded passwords, a possible opportunity

[1] `https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote\%20reports/demtech-source-code-review-report.pdf`

for deleting votes without logging, and a general overwhelming difficulty of verifying that the code being executed is working correctly. This underlines the misconception that iVote does not have security problems, merely maintenance problems. The problem of not having any maintenance to address current or future security problems, is a security problem.

Recommendation 1 *Discontinue Internet voting.*

Voting by email, phone, fax and uploaded pdfs are all forms of Internet voting and are included in the "discontinue Internet voting" recommendation. None of those options allows the voter the chance to genuinely verify that the vote recorded on their behalf matches their intended choices.

The main purpose of this submission is to encourage a complete reorientation of NSW electoral law around transparent processes, verifiable election outcomes, and secret ballots. If these principles are placed first, with cost savings and convenience as subsidiary goals, NSW elections will return to earning public trust. It might even be cheaper, because NSWEC won't have to reimburse more campaign expenses for election reruns.

Many of the ideas in this submission are derived from joint work with Prof Patrick Keyzer. [2]

Legislative change for transparent elections

Over the last decade of iVote's operation, a lack of normal electoral rules about openness, transparency and scrutiny has allowed the narrative around iVote to drift substantially away from its reality. We have been told the system was verifiable, privacy-preserving, reliable and secure, when it was never any of these things. This divergence between truth and perception is partly the fault of the NSWEC and its contractors, but also partly the fault of the NSW Parliament, who had the power to impose stronger transparency rules and more demanding security requirements, but consistently declined to do so.

A great deal of attention has focused on the three local councils that will have their elections re-run as a result of iVote's downtime. But in many other local councils, the number of voters disenfranchised by iVote was enough to change the outcome[3]—the councils that may have had their outcomes altered, but do not have the opportunity to re-vote, are more seriously adversely affected by iVote's failure. Since iVote does not produce evidence that the votes it received were accurately recorded, there may be undetected problems that altered other results. We simply do not know whether the seated councillors were all rightfully elected or not.

Here is a short list of questions that ought to have public answers.

- **Simulation of disenfranchised voters in the 2021 LGE.** Why did the NSWEC and its contractors choose the model that they did?
- **Verification failure rates.** In 2015 about 10% of verification attempts failed to retrieve any vote. What were the verification failure rates in 2019 and 2021?

[2] https://journals.latrobe.edu.au/index.php/law-in-context/article/view/119/187

[3] https://github.com/AndrewConway/ConcreteSTV/blob/main/reports/NSWLGE2021Report.pdf

- **The errors and security problems identified in the Demtech review.**[4] Which ones were corrected? Who audited the corrections?

- **The cause of the 2021 downtime.** Was it the same as the cause of the apparently very similar downtime in the last days of polling for the State General Election in 2019?

My guess is that the Committee's answers to these questions will be, "We don't know." The fact that these details are generally not made publicly available, and are not generally even the focus of scrutiny or attention, allows a continuing divergence between reassurance and reality.

Whether Internet voting is continued or not, the iVote enabling legislation should be repealed entirely and replaced with legislation oriented around improving transparency and security.

I know of no other democracy that criminalises the sharing of source code related to elections. Switzerland mandates openness of the source code, as every democracy should. If the source code is so embarrassing that its publication would undermine trust in NSW elections, then it should not be used.

As well as mandating openness of all the system details, source code and documentation, the new legislation should require:

- privacy of the votes, in a reasonable threat model that cannot be attained easily by a small number of officials or providers;

- verifiable outcomes, so that the system must be designed to provide evidence to scrutineers that the election outcome is correct, without having to trust the software.

Recommendation 2 *Regardless of the exact use of computers in elections, there should be specific, detailed regulations that emphasise transparency, vote privacy, and verifiable outcomes.*

The current iVote enabling legislation gives the NSWEC great leeway to build a system and deliver an election electronically in any way they choose—this strategy has not been successful. By contrast, the older legislation for paper-based elections is quite detailed and prescriptive, constraining the NSWEC to follow processes that are transparent and verifiable by scrutineers. This strategy works much better, and it is notable that Switzerland (which paused Internet voting following the cryptographic errors we identified) has much more detailed and specific requirements, which were strengthened when problems occurred.[5]

Detailed regulations setting minimum standards for transparency, privacy and verifiability are the responsibility of the NSW Parliament—NSWEC cannot be expected to write their own rules, and it is clear that they have (quite understandably) not succeeded in the effort to do so. This will take substantial time, effort, and expert input. The same is true for any use of computers in elections.

[4] `https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote\%20reports/demtech-source-code-review-report.pdf`

[5] `https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-89020.html`

More transparent and trustworthy alternatives

This section briefly outlines alternative uses of technology in elections, which are much more consistent with a secret ballot and verifiable election outcomes. In all cases, the details matter, and I am not necessarily advocating any of these without further careful examination of the pros and cons. My point is simply that there are numerous other ways of meeting the needs of voters, without sacrificing election integrity. Some of these approaches might work well, if they were designed with transparency, verifiable outcomes, and ballot secrecy as primary goals.

Electronic voting in a polling place with a voter-verifiable paper record Voters with disabilities could use a computer in a polling place as an aid to fill in their ballot. The computer could then print out a human-readable paper record of the vote. Although not all voters with disabilities are able to check this printout directly, many could, and the overall opportunity to verify the result would be much better than nothing. These printouts could then be included in the normal scrutineered counting process.

Delivering candidate information electronically; returning a paper vote by mail Another alternative for those who miss the postal voting deadline for reasons beyond their control (such as a covid diagnosis) could be the opportunity to print out a ballot at home and return it by mail. This is clearly a last resort, but compares favourably to iVote because at least voters could see that their ballot accurately reflected their intention.

Secure drop boxes to reduce dependence on the post Many US jurisdictions provide special secure drop-boxes for ballot return, so that voters do not need to rely on the postal service.

No-excuse early voting This would allow people to vote early without a specific reason, hence reducing the pressure on polling day and increasing each person's opportunity to vote while well.

Rigorous audits of electronically counted ballot papers Even if people vote on paper, there is scope for security problems or software errors to effect outcomes when the ballots are digitised and counted electronically. NSWEC does a good job of publishing digitised vote preferences, so that the actual count can be double-checked—we have been able to identify and help to correct errors in the counting code in the past. The main gap is in ensuring that the paper ballots are accurately digitised—for this, a rigorous audit of a random sample of ballot papers against their corresponding digitised preferences should be required by law. The recently-passed Assurance of Senate Counting Bill (2021)[6] could be a good model to adapt.

Recommendation 3 *Mandate an audit of the ballot papers in the Legislative Council to verify that the digitised preferences are accurate. Consider adapting wording from the Assurance of Senate Counting Bill (2021).*

[6] `https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6810`