Submission No 21

ADMINISTRATION OF THE 2019 NSW STATE ELECTION

Name:	Dr Roland Wen
Date Received:	15 October 2019

Submission to the Inquiry into the Administration of the 2019 NSW State Election

Dr Roland Wen Professor Richard Buckland

Security Engineering and Cyber Governance
School of Computer Science and Engineering
The University of New South Wales

Executive Summary

Election systems are critical sovereign infrastructure. Worldwide attacks on elections have occurred and are occurring at increasing rates. Such attacks are a relatively low cost and simple way to bring about substantial impact on the target country for economic, political or disruptive purposes. Electronic voting systems are particularly vulnerable targets and Internet based electronic voting systems even more so.

Cyber attacks by nation states have successfully compromised Australian government agencies and public institutions. There is clear evidence that such attacks are increasing globally, as are foreign attempts to influence and interfere with democratic processes. As a member of the Five Eyes Australia is a high profile target. A national approach to building and operating electronic and Internet voting as critical sovereign infrastructure is needed to address these threats as a matter of national security.

The NSW iVote Internet voting system is not fit for the purpose of electronic voting at scale. Originally envisioned as a small scale system for assisting small groups such as vision impaired voters, the system has been built quickly and at low cost. The subsequent three NSW state elections and one WA state election in which iVote systems have been used have experienced multiple incidents and vulnerabilities, and there have been numerous published failings in its security, reliability, scrutiny and transparency.

It is important to note that these vulnerabilities and failures are symptoms of the problem rather than being the problem themselves, and fixing and patching them as they are discovered will not provide electoral security and safety. Rather they are an indication, like foreshocks before an earthquake, that the system is not fit for purpose and it has been designed, built and deployed at the quality and security standards of commercial software systems rather than as critical sovereign infrastructure.

Using iVote for voting at scale exposes elections to serious risk of

- attack,
- error,
- system failure,
- foreign interference,
- voter privacy breaches including voter coercion and vote buying (due to the loss of the secret ballot),
- loss of public trust in the electoral commission,
- loss of public trust in election outcomes,
- incorrect election outcomes.

Recommendation 1. *The current iteration of the iVote system should not be used in future elections beyond small numbers of targeted groups such as vision impaired voters. In particular the use of iVote should not be expanded to other jurisdictions as a de facto national electronic voting system.*

Recommendation 2. *A new e-voting system should be developed based on a national approach. This e-voting system should be designed to be suitable for secure long-term large-scale use. Close and ongoing engagement with experts and federal agencies with advanced capabilities (such as the Australian Cyber Security Centre) should be harnessed to ensure the new system is designed, built, tested and operated according to four pillars of best practice for election technology [BTW11; CORE11]:*

1. *failure-critical engineering,*
2. *risk management,*
3. *transparency, and*
4. *a culture of scrutiny.*

Recommendation 3. *Strong, specific, upfront requirements must be mandated for transparency and scrutiny. Any e-voting system must be able to satisfy these requirements before being used in an election.*

Recommendation 4. *That there be public education and discussion about e-voting and in particular about the importance or otherwise of voter influence, privacy, coercion and retaining the secret ballot.*

1 Electronic Voting Security Risks

Australia and New South Wales have a world class record of conducting fair and free elections. Australian electoral processes, electoral commissions, and announced election outcomes have traditionally enjoyed high levels of public trust envied worldwide. However the continued use of iVote is placing this at risk. Electronic voting (voting by device rather than using pen and paper) including Internet voting (voting by device remotely and unsupervised) are uniquely susceptible to foreign and malicious attack for the following reasons:

- Election systems are used rarely but intensely.
- Failure or attack can be invisible due to vote privacy.
- Electoral outcomes often are affected by a very small number of votes, and so change can be affected by small targeted attacks.
- Democracy is vulnerable to loss of public trust in election outcomes.
- Recovering from errors can be hard particularly if it prevents people from voting in the eligible period or if discovered after some time has passed.
- Electronic voting can provide a relatively simple and cheap way of exerting significant national influence.
- Unlike traditional attacks on elections, the attacker is not required to attend in person or even to be in the same country.

Internet voting also introduces serious risks from the loss of the traditional Australian principle of the Secret Ballot. One risk is the possibility that outside attackers or insiders (the electoral commission and its suppliers) could learn the votes of all voters who used Internet voting. Another risk is large-scale voter coercion and vote buying.

For example, members of a family or organisation such as a church or union could be pressured to vote openly and so along co-ordinated lines. Furthermore, under such a system voter credentials can be handed over or sold to allow others to vote for you. Although current elections may have a low risk of large-scale voter coercion and vote buying, using a system with weak privacy safeguards can not only rapidly increase the risk of this occurring, but also increase the risk of damaging public trust in the outcome simply by allegations of this occurring.

Elections are obvious and increasingly exploited targets for attack. To defend against sophisticated, highly-skilled and well-resourced attackers such as state actors, e-voting systems need to be designed and deployed as critical sovereign infrastructure incorporating a high level of security and assurance by design.

The NSWEC does not have sufficiently advanced capabilities to address the problems with iVote. The iVote system has grown from a small pilot in 2011 to a large-scale Internet voting system that has overtaken postal voting and was used by more voters than in any other public election worldwide. But despite procuring an almost entirely new version of iVote each time for every NSW state election, serious fundamental problems have persisted, and essential improvement measures have not been implemented effectively, or at all. As a result iVote has fallen further behind international best practice. In certain respects regarding transparency and scrutiny, iVote 2019 was more problematic than 2015, even though "[a] key driver for [the significant refresh for iVote 2019] was to increase transparency to the voters and the political party scrutineers" [PWC19].

These fundamental problems are not isolated to the NSWEC. They apply to election technology used by all state and federal electoral commissions. But of course the risks and consequences are far greater for Internet voting at scale.

We have previously written about best practices for electronic voting and election technology [BTW11; CORE11], problems with NSW iVote [WB18], and also problems with Victoria vVote [WB16], which shared the same fundamental failings as iVote in the practices followed for engineering, risk management, transparency and scrutiny. In the remainder of this submission we give some brief examples of problems with iVote in the 2019 NSW State General Election, based mainly on the limited published documentation.

2 Problems with Engineering

The security and quality assurance program for iVote had substantial shortcomings and was not appropriate for critical sovereign infrastructure.

Testing plans did not have a strong focus on security testing. For example the roadmap in the iVote tender requirements allocated only one week for penetration testing (a key part of security testing) before going live [NSWEC17]. We pointed this out in our submission to the iVote Inquiry [WB18] in the hope that security testing would be expanded significantly. In our experience, it is standard practice for organisations and government agencies with a rigorous supplier security assurance program to conduct much more thorough penetration testing for common business applications, let alone for complex, specialist applications with such critical and unique security requirements as iVote.

Key components of iVote were excluded from critical assurance activities. For example the Registration and Credential Management System was out of scope of the iVote source code review by DemTech [HS19]. This system experienced multiple failures and extended outages during the election.

The iVote system did not undergo any small-scale real world testing before going live at scale on a full state election. PWC's post-election findings [PWC19] reveal operational failings due to missing and weak security controls for iVote operations. Such failures should have been identified and remediated during small-scale trials to ensure that comprehensive, mature operational controls are in place before going live at scale. For example:

- "Finding 4: Voter information was not deleted from the registration system." This was discovered incidentally when analysing another issue.

- "Finding 13: Undocumented configuration changes were made to the Registration and Credential Management System in production." Changes to the production system were not documented or tested before being made, which is a symptom of weak change management controls.

- "Finding 15: Deficient password practices followed for the iVote platform." Some iVote systems were not compliant with the NSWEC's password policy. (The details are redacted from the report.) Furthermore the password policy is weak, for instance the minimum password length is eight characters. This fails to comply with the Australian Government Information Security Manual, which requires a minimum password length of 10 characters.

- "Finding 16: User-IDs were not disabled during the lockdown procedures." Users were were not properly locked out of the system during the election.

- "Finding 17: [Redacted] on air-gapped (offline) computers was not disabled." It appears that Wifi was not disabled on two critical computers that were supposed to be completely isolated. (The details are redacted from the report.)

- "Finding 18: Lack of review of firewall rules to ensure only authorised network traffic is allowed." The firewall did not block all unauthorised traffic, and this was not detected until the firewall configuration was reviewed after the election.

- "Finding 25: Lack of adherence to the removable media procedures at one of the data centres hosting iVote." It appears that voting data was not securely erased by a third party supplier. This a symptom of weak controls for supplier management.

3 Problems with Risk Management

Risk management and governance frameworks for iVote are not robust or mature. The approach to iVote has been high risk without effective controls needed to achieve key objectives, in particular in the areas of transparency and security. (We discuss these two topics in the following sections.)

For example the timeframe for the iVote 2019 refresh was overly ambitious and high risk: a completely new system was to be procured in less than 12 months from signing contracts to the execution of the election. This system had to be complex as it was intended to provide strong verifiability, which requires sophisticated cryptographic techniques. While incorporating verifiability has the benefit of mitigating certain risks, the trade-off is that the increased complexity also increases a range of risks across security, reliability, performance, transparency and scrutiny. These risks were not well managed, and in the end the objectives and potential benefits of a verifiable system failed to be realised.

On top of this further risks were introduced by considering increased scope for iVote, for instance expanding the scale to potentially one million voters, along with the potential to support NSW Local Government Elections as well as elections in other jurisdictions [NSWEC17].

In addition, risk assessments of iVote have often downplayed the risks. For example in determining that there was a low risk that vote tampering in iVote could change the election outcome without being detected, one of the reasons given was that “psephologists, political parties, pollsters and other experts would most likely query and question outcomes that are inconsistent with expectations” [Wil18]. However this assumption is flawed in the current political climate where opinion polls and political analysis are frequently inaccurate. Unexpected outcomes have become more regular, for instance in the 2016 Brexit Referendum, the 2016 US Presidential Election, and closer to home in the 2019 NSW State Election and the 2019 Federal Election. Such errors in risk assessments can result in missing or ineffective controls to mitigate the risks.

4 Problems with Transparency

The iVote 2019 system has similar transparency failings to previous iVote iterations despite published intentions to improve transparency. Material planned to be released before the election to allow scrutiny and pre-emptive error detection was either published well after the election or not at all.

The only technical documents for iVote published by the NSWEC were released in July, after the election: the iVote Source Code Review by DemTech [HS19], and the responses by the NSWEC [NSWEC19b] and Scytl (the vendor) [Scytl19].

Plans to publish other key material were not followed through. For example the iVote Refresh Project Report [NSWEC19a] stated that:

- “During the 2019 State election the NSW Electoral Commission will publish key data to provide insight into the progress and functioning of the iVote channel. [...] key verification data will also be published alongside other iVote data. As well as publication of the verification data, we will publish the results of the mixnet processing”, and
- “The NSW Electoral Commission will publish information on the design and operation of the iVote channel in the public domain.”

None of these were published. Instead a confidentiality agreement was required to access the verification data and the specification documents for writing software to verify that data. (We were invited to participate in the verification.)

This absence of published material means that iVote did not in fact provide verifiability. It defeats the very purpose of using a system that has very high complexity in order to provide verification features. These transparency problems also make it difficult to uncover the full extent of the problems with iVote, including potential flaws in its verification mechanisms.

5 Problems with Scrutiny

Key scrutiny measures for iVote were not carried out or were not effective. This was due to problems in planning and execution. Rather than putting in place mechanisms to support broad and effective scrutiny, barriers were created that made scrutiny infeasible or discouraged potential scrutineers. These barriers included inadequate transparency, inadequate time, and imposing conditions that excluded potential scrutineers.

Inviting scrutineers to write software to verify the iVote verification artefacts was not well organised and was done too late. The process began less than three weeks before election day, and a week out we still had not received sufficiently detailed specifications to allow verification software to be written. In comparison, iVote 2015 involved much more straightforward software to verify fewer and simpler artefacts, but several weeks was still needed to clarify gaps in the specifications to ensure full and robust verification was performed. (Our verifier was the only one to detect subtle errors in the iVote data in that instance.) Based on our experience, it is highly unlikely that in the very limited time available, independent verifier software would have been able to be written to fully and correctly verify all the iVote 2019 artefacts. Again, it largely defeats the purpose of using a highly complex system that provides verifiability if the verifiability is not used.

The public invitation for iVote source code review was a positive initiative in principle but was similarly problematic in practice, and we are not aware of any meaningful findings from this exercise. The code review period started in January 2019, only two months from going live. This did not consider the extensive time and effort needed for reviewers to perform a comprehensive code review on a large, highly complex system (as volunteers, so potentially in their spare time) and report the findings, then for the NSWEC to verify the findings, implement remediations and rigorously test the updated system.

There were further problems with the code review process including:

- The Registration and Credential Management System was excluded from the review.
- Participation was restricted to individuals on the electoral roll with demonstrated expertise in electronic voting. This excluded overseas experts and severely limited the pool of participants (we estimate in the order of 10 individuals were eligible).
- The code was likely to be missing dependencies and also to include code not used in iVote, which was the case for the DemTech code review.
- The code was not likely to be production ready as key components were still under development, which was the case for the DemTech code review. This increased the risk of significant changes between the code reviewed and the code used in the live system.
- Confidentiality agreements were required, which discourages participants. While we did not view this particular agreement, we have spent extensive time and effort in negotiating to remove unacceptable conditions from previous agreements. For example, the confidentiality agreement initially proposed for iVote 2019 scrutiny (which is likely to be less onerous than the code review agreement) included unreasonable conditions such as “Any copyright or other intellectual property arising from the exercise of your functions and the provision of your report vests in the NSW Electoral Commission”. (In other words, all testing software, documentation

and reports created by any volunteer scrutineer would belong to the NSWEC and be controlled by them.)

In contrast to the iVote scrutiny approach, Swiss Post's Internet voting system had broad public scrutiny well in advance of being used, through both public code reviews and public penetration testing. The code review did not have conditions to exclude participants or require confidentiality agreements to access the code. This allowed a substantial number of international experts to participate. While not perfect, this was a much more effective scrutiny process and as a consequence a number of serious security vulnerabilities were identified and remediated in time.

References

[BTW11] Richard Buckland, Vanessa Teague and Roland Wen. "Towards Best Practice for E-election Systems - Lessons from Trial and Error in Australian Elections". In: *E-Voting and Identity - Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers*. Ed. by Aggelos Kiayias and Helger Lipmaa. Vol. 7187. Lecture Notes in Computer Science. Springer, 2011, pp. 224–241.
URL: http://dx.doi.org/10.1007/978-3-642-32747-6_14.

[CORE11] Roland Wen, Vanessa Teague and Richard Buckland. *Best Practices for E-election Systems. Computing Research and Education Association of Australasia (CORE) Supplementary Submission to the Inquiry into the 2010 Federal Election*. Submission 101.1, Inquiry into the 2010 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia, 2011.
URL: https://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=em/elect10/subs/sub101.1.pdf.

[HS19] David Hook and Carsten Schürmann. *Review of the iVote 2.0 System*. DemTech Group, Jan. 2019.
URL: https://www.elections.nsw.gov.au/getmedia/341fa362-e859-4f36-89d5-1b7385e195b7/Code-review-report_NSWEC-7-Redacted.

[NSWEC17] New South Wales Electoral Commission. *iVote Voting System RFP Requirements*. 1st Dec. 2017.

[NSWEC19a] New South Wales Electoral Commission. *iVote refresh project for the 2019 NSW State election*. Feb. 2019.
URL: https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/iVote-Refresh.pdf.

[NSWEC19b] New South Wales Electoral Commission. *NSW Electoral Commission iVote Project — Code Review Report*. 29th July 2019.
URL: https://www.elections.nsw.gov.au/getmedia/3f78bda3-56e0-4ca5-b0e6-8d588c28babc/iVote-CodeReviewResponse-v1-0.

[PWC19] PricewaterhouseCoopers. *Post Election Report — 2019 NSW State Election iVote Review*. June 2019.
URL: https://www.elections.nsw.gov.au/getmedia/b2280c43-a129-47ca-bd75-f9c98887736b/2019-State-Elections-iVote-review-(post-election-report)-June-17-2019-redactions-v2-3-draft-Copy_Redacted(1).

[Scytl19] Scytl. *Scytl iVote 2.0 System — Response to NSWEC-7 Final Report*. 11th June 2019.
URL: https://www.elections.nsw.gov.au/getmedia/d6955cf1-7103-48e5-b30e-44cbf18064f2/Scytl-iVote-responses-to-NSWEC-7-Final-Report-release.

[WB16] Roland Wen and Richard Buckland. *Submission to the Victorian Inquiry into Electronic Voting*. Submission 23, Inquiry into Electronic Voting. Electoral Matters Comittee, Parliament of Victoria, 2016.
URL: http://www.parliament.vic.gov.au/images/stories/committees/emc/Inquiry_into_Electronic_Voting/Submissions/No_23_Dr_Roland_Wen_and_Associate_Professor_Richard_Buckland.pdf.

[WB18] Roland Wen and Richard Buckland. *Submission to the iVote 2019 Inquiry*. Submission 10, iVote Inquiry. 2018.
URL: https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/Sub10-20180112-Roland-Wen-and-Richard-Buckland.pdf.

[Wil18] Roger Wilkins. *Report on the Security of the iVote System*. May 2018.
URL: https://www.elections.nsw.gov.au/About-us/Public-interest-information/Commissioned-reports/Report-on-the-iVote-system.