NSW Electoral Commission response to Roger Wilkins' Report on the Security of the iVote system

Background

In response to a 2016 recommendation of the NSW Parliament's Joint Standing Committee on Electoral Matters (**JSCEM**),[1] Mr Roger Wilkins AO was commissioned to undertake a review of the security of the NSW Electoral Commission's (**NSWEC**) iVote system. This review was conducted to consider the security of iVote prior to next year's State General Election (**SGE19**) and provide a basis on which the NSW Government and the NSW Electoral Commissioner could assess if it was appropriate to use iVote at SGE19.

Mr Wilkins has concluded that the security of iVote remains adequate to support its continued use at SGE19, although he also points out the need for ongoing investment in the system to maintain its integrity and security. The NSWEC agrees with this assessment.

The Report recognises that all electoral information systems should be treated as critical infrastructure. It highlights the need to invest in improving the security of NSW elections overall, not only the security of the iVote system.

The NSWEC supports most recommendations in the iVote report

The NSWEC supports 25, and supports in principle 3, of the Report's 29 recommendations. The NSWEC believes that further consideration needs to be given to Recommendation 14 (compulsory vote verification) before a final decision can be made regarding its adoption. The NSWEC response to each recommendation is set out in **Appendix 1**.

Investment critical to maintaining integrity and security of systems

Several of the Report's recommendations will require additional funding to implement. Additional resourcing priorities are also likely to be identified by (i) the current COAG commissioned Australian Cyber Security Centre's review of NSW electoral processes, (ii) a PwC internal audit of NSWEC's IT contract management, and (iii) a physical and technical security risk assessment being commissioned by the NSWEC in the lead up to SGE19.

[1] Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Administration of the 2015 NSW election and related matters*, Report 2/56 (November 2016), Recommendation 6.

The NSWEC has developed a new Risk Management Framework to respond to the iVote report

The Report includes a Risk Assessment of the iVote system conducted by PwC Australia. At page 15 of its Risk Assessment, PwC observed as follows:

> PwC identified a bias toward risk ratings being assessed as Extreme or High in the model used by the NSWEC. This results in 32% of the possible results for assessment of likelihood and consequence being an 'Extreme' risk rating, while 64% of the possible assessments rate above a 'High' risk rating. This bias has been communicated to the NSWEC for future remediation.

In light of PwC's comments, the NSWEC has undertaken a review of its Risk Management Framework and has drafted a new Risk Management Policy and Risk Management Procedure. The new Policy and Procedure have been prepared in accordance with NSW Treasury Policy TPP15-03 and is consistent with ISO31000:2018, the recently revised International Organization for Standardization standard on risk management.

PwC has reviewed the updated Risk Management Policy and is satisfied that it is appropriate, and that it addresses the bias evident in the NSWEC's previous risk matrix.

Appendix 1 | NSWEC response to Mr Wilkins' recommendations

Recommendation	Response	Comment
National approach		
1. Electoral commissions in Australia should jointly develop a national platform for internet voting that could be jointly owned and maintained. The platform could be used by any jurisdiction that chooses to allow internet voting. It could be adapted in each case to accord with the law of their jurisdiction, but its core functionality would remain the same. This would be the most efficient and secure way to provide internet voting in Australia. The recommendations that follow are framed with an eye to the establishment of a national platform and could be adapted to that circumstance.	Support	All Australian Electoral Commissions have agreed to work through the Electoral Council of Australia and New Zealand (**ECANZ**) toward the creation of a national internet voting service. ECANZ has sought the support of the Council of Australian Governments (**COAG**) for this initiative.
Security		
2. The NSW Government, the Joint Standing Committee on Electoral Matters (**JSCEM**) and the NSW Parliament should, as a matter of course, always consider the security impacts of any change to electoral legislation. Those impacts are not always obvious but the question should always be asked.	Support	No comment.
3. NSWEC should put in place a comprehensive Protective Security Strategy. While many of the elements of security are being attended to, what is needed is an integrated and holistic policy that deals with:	Support	As part of its preparation for the State General Election in 2019 (**SGE19**), the NSWEC is engaging external consultants to carry out a physical and technical security risk assessment, and develop a risk management plan.

Recommendation	Response	Comment
• Security of people, • Security of place, • Security of data and information. It should also deal with governance, i.e. the clear assignment of responsibilities.		In addition, the Australian Cyber Security Centre (**ACSC**) has commenced its engagement with the NSWEC pursuant to the 9 February 2018 COAG decision to undertake cyber security health checks of Australia's electoral processes. It is anticipated that additional resourcing requirements will be identified by this ACSC review. If so, the NSWEC will develop a funding proposal for consideration by the NSW Government.
4. Many aspects of iVote will be delivered by external parties. NSWEC should ensure it has the in-house capacity to properly understand and control what is expected of third parties providing hardware, software and services, and ensure that arrangements and contracts with third parties and other government agencies also mandate appropriate security requirements.	Support	NSWEC acknowledges the need, and is taking steps, to raise its capability and capacity in this area and improve its contract management processes.
5. NSWEC should ensure that arrangements with the private sector to provide software for internet voting are sufficiently flexible to allow changes to be made to meet new threats and exigencies.	Support	Contracts for the iVote Refresh project have improved flexibility to address evolving security threats and exigencies.
6. NSWEC should put a Cyber Security Strategy in place as part of protective security. While elements of such a strategy exist, what is required is a comprehensive strategy that deals with both the prevention and detection of intrusions.	Support	As part of the 2018-19 Budget the NSWEC received $100,000 in 'seed funding' for information security and data governance. This seed funding will be used to initiate development of a Cyber Security Strategy. The NSWEC is working with the

Recommendation	Response	Comment
The strategy should encompass more than iVote and include all assets and facilities managed or controlled by NSWEC, including, for example, the storage of information about voters.		Department of Finance, Service and Innovation and the Department of Premier and Cabinet to develop a tactical plan for improving its cyber security capabilities. This work will take into account findings of the ACSC review of the NSWEC's electoral processes. If additional resourcing requirements are identified during the development of this Strategy, the NSWEC will develop a funding proposal for consideration by the NSW Government.
7. NSWEC should enter into arrangements with key Commonwealth agencies (perhaps in concert with the Australian Electoral Commission) including the Department of Home Affairs, the Australian Signals Directorate, CERT Australia, the Australian Cyber Security Centre, the Australian Federal Police, and the Australian Security Intelligence Organisation to ensure that it has a good and up-to-date understanding of threats. Ideally, such an arrangement should involve all Australian electoral commissions given the technological developments in electoral systems and other international developments. Electoral systems should be treated as "critical infrastructure".	Support	The NSWEC will strengthen its existing links with Australia's intelligence and law enforcement agencies regarding security threats. NSWEC is engaging with the NSW Government GCISO (Government Chief Information Security Officer) to leverage whole of government relationships.
8. NSWEC should make use of the Risk Assessment for iVote carried out by PwC. NSWEC should manage the risks identified, noting that many of these risks are addressed by recommendations in this report. More importantly, it should treat risk assessment as a dynamic process and constantly review and update the Risk Assessment. That Risk Assessment should be regularly	Support	The risk categories identified by PwC will be included in the NSWEC risk assessment and management process for SGE19.

Recommendation	Response	Comment
reviewed by the expert panel I have recommended (Recommendation 25).		
9. NSWEC should put in place arrangements for systematic vulnerability testing. This should be more than penetration testing. It should test for whether the system can be "gamed" or "manipulated". As with any critical infrastructure, regular exercises and testing need to be incorporated into business planning. Once again, doing this with other electoral commissions and involving the Commonwealth would be sensible from a cost and benefit perspective.	Support	The iVote system, and other key election systems, will undergo a series of external vulnerability assessments as part of testing prior to SGE19. This will include technical penetration testing at various stages of development and implementation. NSWEC is considering more comprehensive external 'Red Team' (attack emulation) reviews to test detection and response capability. The scope and resourcing required for regular vulnerability testing across all the NSWEC's election systems (including iVote) is also being assessed.
10. NSWEC should establish response plans for possible intrusions and tampering. With electronic voting it should be possible to find out more easily what has gone wrong and what to do about it.	Support	Previous response plans are being re-developed as part of the iVote Refresh project, to reflect the new systems and infrastructure. The prevention of, and monitoring for, intrusion or tampering is included in the project and will inform the new response plans.
11. It is noted the NSW Parliament's Joint Standing Committee on Electoral Matters has recommended that the NSW Government expand the trial of electronic roll mark-off of electors at pre-polling and election day polling booths, with a view to a full rollout over the next few elections. With the increased number and use of alternative voting channels and emergent issues around	Support	The NSWEC will submit a funding proposal to the Government, with the aim of introducing an electronic roll-mark off system in time for SGE23.

Recommendation	Response	Comment
security this recommendation should be adopted as soon as possible.		
12. NSWEC should insist on the use of an identification document that may be verified by the Document Verification Service (**DVS**) before a person may register to use iVote. This approach should take account of the circumstances of electors with a disability (within the meaning of the *Anti-Discrimination Act 1977* (NSW)).	Support in principle	82.6% of electors who registered to use iVote for SGE15 provided either driver licence or passport information to be verified by the DVS. For iVote electors who identified as having a disability the use of DVS was 59.2% and for electors who identified as blind or low vision it was 51.1%. It could be argued that the introduction of compulsory identification verification for iVote users would be inconsistent with voter identification requirements for people who use other voting channels, such as postal or in-person voting. There is also the risk that mandatory identification verification could disenfranchise some iVote users. On the other hand it could be argued that, having regard to cyber-security concerns relating to electronic voting, to maintain confidence in the integrity of elector identification, DVS verification should be made mandatory for electors using the iVote system. In the lead up to SGE23, the NSWEC will undertake public consultation regarding this recommendation and its potential impact on eligible electors' use of iVote.
Transparency, auditability & scrutiny		
13. NSWEC should clearly set out how end-to-end verification (**E2E verification**) is given effect in iVote. This explanation would include answers to questions including	Support	NSWEC will publish an iVote Strategy document later this year that will set out details of the refreshed iVote system and

Recommendation	Response	Comment
what functionality supports verification? What is the process for monitoring? What is the process for auditing? Who is completing these processes, and when? Currently these processes are opaque. Clarity and transparency around this is absolutely critical.		its intended operation for SGE19. One of the elements to be addressed in that Strategy is E2E verification.
14. NSWEC should consider making it part of casting a valid vote via the internet to also verify that vote. Because votes are secret, only the voter is in a position to verify that the vote as collected reflects their intention.	To be further considered	The new iVote system will offer simpler, smartphone-based verification. In the lead up to the election, the NSWEC will undertake awareness raising activities to promote the availability and use of this verification facility. The introduction of mandatory verification runs the risk of disenfranchising voters who are unable to verify their vote (for example, electors using operator assisted voting and electors who do not have a smartphone or cannot download the verification app). In his report, Mr Wilkins notes that some members of his expert panel and some commentators raised issues with mandatory E2E verification, including: • Mandatory verification would create a requirement that is additional to compulsory voting. • Mandatory verification does not apply to any other type of voting channel. • Mandatory verification is unnecessary as only a sample of verified votes will indicate whether the system is working or not. • Mandatory verification may to lead to "false positives" as voters will misremember their

Recommendation	Response	Comment
		preferences. It may also lead to "false negatives" if voters do not take verification seriously and simply verify an incorrect ballot as correct. • The process for verifying other voting channels is more akin to the iVote monitoring, auditing and scrutiny measures. Those measures are more appropriate for iVote than mandatory verification. • There is no current requirement for voters to verify that all votes have been collected-as-cast and counted-as-cast. While the NSWEC is currently of the view that verification of every vote is not required to achieve an appropriate level of assurance that the votes counted reflect those votes as cast, it agrees that consideration should be given to the development, and potential impact, of a mandatory verification requirement.
15. As part of monitoring and E2E verification NSWEC should develop systematic profiling and identification of discrepancies or anomalies in voting patterns as a way of detecting possible intrusions or tampering.	Support	The NSWEC already monitors voting patterns across all voting channels (including iVote) to detect anomalies, and will assess how that monitoring can be enhanced for SGE19.
16. NSWEC should consider opening up the process of E2E verification to political parties and other interested parties so that they can see for themselves and monitor how the process is working. This will promote trust and confidence, and could be a further source of scrutiny and potential intelligence.	Support	The NSWEC plans to improve transparency regarding the use of iVote for SGE19. An initial measure will be the publication, in near real-time, of data on the performance of the iVote system. This will be outlined in the iVote Strategy to be released later this year. The Strategy will also outline improvements to facilitate scrutineers observing the operation of iVote.

Recommendation	Response	Comment
17. NSWEC should have an active communications policy to explain iVote and cyber security to political parties and potential voters. This will not only promote trust and confidence, it will also make the process more efficient.	Support	The NSWEC is currently implementing a new Integrated Communications and Engagement Strategy which will include providing a greater understanding of the iVote process to electors and political participants.
18. The JSCEM should have iVote as a standing reference, and should hold NSWEC to account in the development of a systematic approach to security as outlined in this report.	Support	No comment.
19. The NSW Government should consider assisting political parties to develop people who are knowledgeable or expert in information technology and cyber security so that they can properly participate in the electoral system and intelligently interrogate process and decisions. This scrutiny is important to the efficacy of the electoral system. This assistance could be provided via the public funding regime available to eligible political stakeholders.	Support	No comment.
20. The Court of Disputed Returns should be briefed on iVote, including issues on security, to consider what effect this mode of voting may have on disputation. The development of internet voting may well change the types and timing of disputes that come before that Court or other courts and tribunals.	Support	Prior to SGE19 the NSWEC will offer the NSW Supreme Court a briefing on the operation of iVote.
21. Since the ultimate arbiter of electoral disputation will be the courts, in making decisions about the use of internet voting and the system that supports it, it is important that the NSWEC keeps in mind the test of "reasonableness"	Support	See response to Recommendation 20.

Recommendation	Response	Comment
that might be applied by a judge, and how the reasonableness of key arrangements and decisions might be demonstrated to a court.		

22. The iVote system software should be made public. At the very least it should be made available and assessed by the community of experts. As internet voting becomes more significant there are more dangers in not making things public and open.	Support in principle	As part of the iVote Refresh project NSWEC has negotiated the public release of elements of the system source code. The following source code will be released:
		• Voting client (JavaScript)
		• Verification application (mobile app)
		• Voting service
		  ○ Validation of the encrypted vote
		  ○ Validation of the cryptographic proofs
		  ○ Digital signature of the receipt
		• Verification service
		  ○ Validation of the encrypted vote
		  ○ Validation of the cryptographic proofs
		• Counting service
		  ○ Vote decryption
		  ○ Digital signature
		
		The iVote contract stipulates that the release will not occur until after the system has been used for SGE19.
		
		As was the case for SGE15, in the lead up to SGE19 and subject to confidentiality arrangements, individuals will be able to seek access to examine all of the iVote source code.

23. NSWEC should publish statistics after the use of iVote at any election that includes the number of registrations, the number of votes cast, the number of votes that were not	Support	See response to Recommendation 16.

Recommendation	Response	Comment
completed, the number of votes verified, and the results of the verification. This form of reporting should aid confidence in the system.		
24. NSWEC should make the method of electronically counting votes for elections public so that, effectively, political parties or members of the public can check the count. This should not be controversial given open publication of vote data by NSWEC.	Support in principle	In its response to the JSCEM report in 2017 on preference counting in local government elections (LGE),[2] the NSW Government accepted in principle Recommendation 6 (minimum levels of data, including full preference data, to be released following LGE) and Recommendation 7 (source code of counting software used in LGE be subject to external audit at least every five years). Existing NSWEC policy for both SGE and LGE is already consistent with these recommendations. Prior to each major release of counting software, NSWEC publishes the functional specification for the 'PRCC', a computer system that completes both the proportional representation count and the optional preferential count. This functional specification defines the method of electronically counting the votes. NSWEC also publishes a test certificate from an external software certifier prior to each major election confirming that the software used for the count conforms to the functional specification and legislation governing vote counting. Interested individuals or organisations are able to review the functional specifications, and the legislation, to develop their

[2] Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into preference counting in local government elections in NSW*, Report 3/56 (November 2017).

Recommendation	Response	Comment
		own count software. As the NSWEC publishes complete vote data (preference files) for each election, the individual or organisation can check the distribution of preferences and the election results using their own software. This analysis has been carried out by academics and political commentators for previous elections.
Resourcing and governance		
25. NSWEC should appoint a standing panel of experts to help implement this report and review and maintain the currency of arrangements and policies recommended in this report. That panel should probably include people who have expertise in cyber security, electoral policy and practice, and protective security. Emergent problems and issues could also be dealt with by this panel. The panel should conduct a review following every election event to see how iVote performed and advise NSWEC on possible changes.	Support	The NSWEC will establish this panel in time to conduct a post-SGE19 review of iVote's performance.
26. NSWEC should review the staffing and resourcing of the "iVote team" to ensure that it is adequate to the growing use and significance of iVote. This will likely require increased resources.	Support	The NSWEC will continue to monitor and review the potential staffing and resourcing impact of the use of iVote.
27. NSWEC should consolidate the organisational restructure that has integrated the iVote team into its election operations as a whole, and undertake ongoing review of the effectiveness of that integration.	Support	The NSWEC has recently finalised an organisational restructure. This structure will be reviewed in light of the Report's recommendations.
28. Over a longer term it is likely internet voting can provide economic efficiencies, but it will require greater resources	Support	The NSWEC will continue to monitor and review the potential resourcing impact of the use of iVote.

Recommendation	Response	Comment
upfront. Security is of the essence, and the various measures and institutional arrangements recommended in this report need to be properly and adequately resourced by the NSW Government.		
29. NSWEC should consider requiring registered electoral material, particularly "how-to-vote cards", to be provided in formats that are accessible to voters who are blind or have low vision by means of assistive technologies such as screen readers and Braille devices. The NSW Government should consider supporting this requirement through the public funding regime available to eligible political stakeholders.	Support	For SGE19 the Electoral Commissioner will be required to make registered 'how-to-vote' material available on the NSWEC website. The NSWEC will encourage political participants to register electoral material which meets Australian 'accessibility' standards but cannot compel them to do so.