# Report on the Security of the iVote System

Roger Wilkins AO

May 2018

# Contents

**Terms of Reference** ... v

**Introduction** ... 1

**Recommendations** ... 5

National approach ... 5

Security ... 5

Transparency, auditability & scrutiny ... 7

Resourcing and governance ... 9

**What is iVote** ... 11

iVote at the 2015 SGE ... 11

How has iVote been used by voters? ... 12

Who is eligible to use iVote? ... 14

**Security** ... 17

What are the appropriate standards for security? ... 17

Is the security of iVote appropriate? ... 18

Security: generic measures ... 21

What or who is the electoral system being protected from? ... 21

Protective security ... 22

Further observations about security and people ... 23

Governance ... 24

Storage of information ... 24

**Security: specific measures** ... 27

1 E2E verification ... 29

Other views on mandatory E2E verification ... 31

2 Monitoring and auditing ... 32

3 Scrutiny ... 32

Should the iVote source code be made public? 34

4 Testing 35

5 Response and recovery 36

6 Communications 37

7 Identity 38

Coercion and vote buying 39

8 Learning and adapting 40

9 Electoral profiling 41

**Other issues 43**

Resourcing 43

Ballot papers 44

How-to-vote material 45

**Appendix 1 International experiences with internet voting 47**

Observations about international experience 50

The 2016 American election 51

**Appendix 2 Abbreviations, list of submissions, bibliography 53**

**Appendix 3 ECANZ 'Eleven essential principles for an Australian internet voting service' 57**

**Appendix 4 PwC Risk Assessment 63**

# Terms of Reference

Following its inquiry into the administration of the 2015 NSW state election, the NSW Parliament's Joint Standing Committee on Electoral Matters (**JSCEM**) recommended:[1]

(a) the NSW Government establish an independent panel of experts to conduct a full inquiry into the iVote internet and telephone voting system to consider security, auditing and scrutineering issues well before the 2019 State Election;

(b) the panel is to contain members with expertise in at least the following areas of information technology: online voting; privacy; security; and cybercrime;

(c) iVote is only to be used for the 2019 State Election if the security concerns highlighted by the JSCEM in its report have been addressed.

The terms of reference of this report are:

(1) Whether the security of the iVote system is appropriate and sufficient.

(2) Whether the transparency and provisions for auditing the iVote system are appropriate.

(3) Whether adequate opportunity for scrutineering of the iVote system is provided to candidates and political parties.

(4) What improvements to the iVote system would be appropriate before its use at the 2019 State General Election.

I note two other recommendations of the JSCEM following the 2015 state election. Firstly, it recommended that the NSW Government does not expand iVote beyond its existing role. Secondly, that the NSW Government make the iVote source code publicly available.[2] These are matters that I will also discuss briefly.

[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.

[2] Ibid Recommendations 5 and 7.

# Introduction

I have been asked to report on iVote. In particular, I have been asked if its security is appropriate; if it allows for appropriate scrutiny; and if the auditing and auditability of iVote are appropriate.

The NSW Government has recently gone to tender to "refresh" iVote. This is a process of trying to address some of the problems the NSW Electoral Commission (**NSWEC**) has identified. It does not appear to have allowed the time, or had the scope, to radically rethink iVote.

In conducting this inquiry I have been greatly assisted by an expert panel consisting of Mr Antony Green AO, Mr Alastair MacGibbon, and Prof Rodney Smith. These people have provided me with invaluable insight and advice. But I want to make it clear that the conclusions and recommendations are my responsibility, and are not necessarily shared by any or all of the expert panel.

Mr Gareth Robson of the NSWEC assisted me as secretariat to this inquiry and writing this report. I have benefited greatly from his experience, intelligence and diligence. Once again, I should make it clear that the conclusions and recommendations are my responsibility, and not that of Mr Robson.

I have also received written and verbal submissions. I want to record my gratitude to the many busy, clever and experienced people who have taken time to give me the benefit of their views and insight.

At the outset I should make it clear that this is not an inquiry aimed at doing a cost and benefit analysis of iVote. I take it that iVote will continue. I see my job as examining certain features of iVote, notably security, and making suggestions about how those features might be improved.

However, I will say that whatever the views on the costs and benefits of internet voting, there is a trajectory of inevitability about the use of information technology (**IT**) in the whole business of voting and organising elections. As a number of Australia's Electoral Commissioners have said to me: "we need to be ready to do this efficiently and securely because it is inevitable."

Another important caveat: this is not a report that is going to be able to give detailed technological solutions. I do not have that expertise, but more importantly, any system for internet voting has to be cognisant of how dynamic information technology is. The strengths, weaknesses, opportunities and threats of any internet voting system are going to develop and shift very fast and constantly. Software and hardware technologies; business models; public expectations; threats and dangers; mitigation, defence and protections - all this will change rapidly. Accordingly, this report places more emphasis on how government might sensibly deal with internet voting in a dynamic world. I look at the sort of institutional arrangements and systems that are or should be put in place.

A word about the PwC Australia (**PwC**) risk analysis that I asked the NSWEC to commission to assist this report.[1] This was done at speed and at some points with limited or inadequate information. PwC also identified a bias in the risk assessment model used, resulting in higher risk ratings than a more balanced model would provide. Nevertheless, it is an important and constructive document. It largely confirms and corroborates the conclusions I have reached.

This type of framework is a *sine qua non* for dealing with the sorts of issues that come up for complex systems and activities. It needs to be constantly reviewed and updated. It needs to be at the centre of decision making about the internet voting system. It is a critical recommendation that NSWEC maintain a comprehensive understanding of risks.

Another thing that I think is very important, but which is not directly part of my brief, has to do with the development of a national platform and capability for internet voting. Australia has a federal system. Some of the jurisdictions are going to find it difficult to put an internet voting system in place by themselves. In any event, there are clearly efficiencies and significant advantages if internet voting were to be advanced by all the Australian states and territories and the Commonwealth collectively. This could be done in a way that does not pre-empt each jurisdiction making its own decisions whether to allow internet voting. The Electoral Commissioners could collectively develop a platform that could be used in any jurisdiction. It would be jointly owned and maintained.

One of the big advantages of this is that it allows better utilisation of knowledge at a national level about cyber security – both the threats and positive mitigation. It also has the advantage of creating national standards on security and integrity that would be observed uniformly across all Australian elections. Recent controversies around this sort of issue in the United States (**US**) have really underlined the problems of not having national standards properly observed, and implemented, across all the different state electoral systems.

Australia should be able to do this relatively easily. The Electoral Council of Australia and New Zealand (**ECANZ**), a consultative council of the Electoral Commissioners of the Commonwealth, States and Territories of Australia and New Zealand, have already articulated principles for an internet voting service at a high level. Although electoral systems vary, the variation is not so significant as to make a jointly owned "platform" infeasible.

Where is this national initiative up to?

[1] PwC's risk assessment is Appendix 4 to this report.

ECANZ has expressed the view that, with the ongoing decline in postal services and a rise in community expectations, it seems inevitable an electronic voting channel will need to be introduced for certain elector categories, for example, electors who are overseas or in remote locations, electors with blindness or low vision (**BLV**), or electors with mobility issues that make it difficult or impossible to attend a polling place. If a new voting channel is not provided for those electors they will effectively be disenfranchised and unable to exercise their democratic right to vote.

Electoral Commissioners have agreed to work together with the aim of creating a national electronic voting service. A key driver in these discussions is the need to maintain electoral integrity and efficiency. Electoral Commissioners recognise that creating a robust, secure, trusted national service will involve addressing significant technical, policy and resourcing issues. They believe the best way forward is to create a national body for electronic voting, responsible to and controlled by ECANZ. To facilitate the development of this proposal ECANZ has established an officer level Internet Voting Working Group.

Establishing this national body, and developing a national internet voting service, will require investment and cooperation from all Australian governments. Given reports of recent international threats to electoral systems, ECANZ believes there would be increased risk and inefficiency if individual electoral commissions attempted to deliver different electronic voting solutions.

At the July 2017 ECANZ meeting Australian Electoral Commissioners signed a letter to all Australian First Ministers asking that consideration be given to the adoption of a national co-operative approach to the development and security of internet voting. This letter also requested that consideration be given to enhancing collaboration between Electoral Commissioners and Commonwealth, State and Territory intelligence and law enforcement agencies, through a coordinated national focus on the issue of cyber security for Australia's election systems.

At the subsequent ECANZ meeting on 8 November 2017, ECANZ endorsed '*Eleven essential principles for an Australian internet voting service*' to guide the design and implementation of an internet voting service in Australia.[2]

The issues raised in the July ECANZ letter were considered at the 9 February 2018 meeting of the Council of Australian Governments (**COAG**). The communique released following that meeting stated:

> COAG also considered proposals from the Electoral Council of Australia and New Zealand to modernise state and federal electoral systems. COAG noted the importance of cooperation to mitigate cyber security risks, and looks forward to the Australian Cyber Security Centre's proposed cyber-security health checks of our electoral processes.

ECANZ has directed its Internet Voting Working Group to prepare a project plan which will be submitted to Australian First Ministers to outline a proposed way forward for the development of a national internet voting service.

[2] ECANZ's '*Eleven essential principles for an Australian internet voting service*' is Appendix 3 to this report.

This report has been written with an eye to this national initiative. The sorts of institutional arrangements and systems that need to be upgraded and put in place to secure iVote, would make sense to do at a national level in collaboration with all electoral commissions.

# Recommendations

## National approach

### Recommendation 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.

## Security

### Recommendation 2

The NSW Government, the Joint Standing Committee on Electoral Matters 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.

### Recommendation 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:

- Security of people,
- Security of place,
- Security of data and information.

It should also deal with governance, i.e. the clear assignment of responsibilities.

## Recommendation 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.

## Recommendation 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.

## Recommendation 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.

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.

## Recommendation 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".

## Recommendation 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 reviewed by the expert panel I have recommended (Recommendation 25).

### Recommendation 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.

### Recommendation 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.

### Recommendation 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 security this recommendation should be adopted as soon as possible.

### Recommendation 12

NSWEC should insist on the use of an identification document that may be verified by the Document Verification Service 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)).

## Transparency, auditability & scrutiny

### Recommendation 13

NSWEC should clearly set out how E2E verification is given effect in iVote. This explanation would include answers to questions including 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.

## Recommendation 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.

## Recommendation 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.

## Recommendation 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.

## Recommendation 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.

## Recommendation 18

The Joint Standing Committee on Electoral Matters 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.

## Recommendation 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.

## Recommendation 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.

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

### Recommendation 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.

### Recommendation 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 completed, the number of votes verified, and the results of the verification. This form of reporting should aid confidence in the system.

### Recommendation 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.

## Resourcing and governance

### Recommendation 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.

### Recommendation 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.

## Recommendation 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.

## Recommendation 28

Over a longer term it is likely internet voting can provide economic efficiencies, but it will require greater resources 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.

## Recommendation 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.

# What is iVote

iVote is an electronic voting system. Electronic voting systems may be implemented for voters who attend a polling place on election day or for so-called early voting prior to election day, also known as "pre-poll" or "convenience voting". However iVote is a remote system, an internet voting system, intended for use from any device that is connected to the internet and has a web browser.

Primarily this report will concern the use of iVote via the internet. However, iVote also provides an option for voting entirely via telephone, using either an automated "interactive voice response" system or talking with a human operator, who is in fact using the iVote system on behalf of the voter.

iVote was first implemented for the NSW state general election (**SGE**) in 2011. A tender was conducted to procure a suitable system, which was won by Everyone Counts, an American company. The iVote system developed for the 2011 SGE was comprised of three sub-systems that the NSWEC refer to as:

- The "registration system" developed by the NSWEC.
- The "credential management system" developed by the NSWEC.
- The "core voting system" provided by Everyone Counts.

That version of iVote was used for the 2011 SGE and subsequent by-elections for the NSW legislative assembly prior to the 2015 SGE.

## iVote at the 2015 SGE

The NSWEC again went to the market to procure the iVote system to be used for the SGE in 2015. The key difference to 2011 was the introduction of a fourth sub-system, referred to as the "verification system". This enabled voters to choose whether to verify that their vote had been recorded correctly, using a separate telephone service. Verification in this sense means that the voter could verify that their vote was cast as intended (**cast-as-intended**) and that all voter's votes had been included in the count for the election (**recorded-as-cast**). A technical difference was that the votes cast were encrypted "in" the web browser before being transmitted. The votes remained encrypted when transmitted throughout the constituent systems and then "stored" prior to the close of polling.

The NSWEC intended to procure replacements for two of the iVote sub-systems. Firstly, the core voting system for which the successful tender was entered by Scytl, a Spanish company. Secondly, the new verification system for which the successful proponent ultimately withdrew. The NSWEC determined that it would internally develop the verification system, that is, along with the registration and credential management systems it was already committed to delivering.

Thus, the iVote system used at the 2015 SGE had four components:

- The registration system developed, operated and hosted by the NSWEC.
- The credential management system developed, operated and hosted by the NSWEC.
- The core voting system developed by Scytl, operated by Scytl and the NSWEC, and hosted by Secure Logic, an Australian company.
- The verification system developed by NSWEC and operated and hosted by AC3, an Australian company.

## How has iVote been used by voters?

Albeit from a low base, there was a very large increase in the number of votes cast using iVote in 2015 when compared with 2011:

| **Eligibility basis** | **2011** | **2015** | **% increase** |
|---|---|---|---|
| Outside NSW on polling day | 43,257 | 257,730 | 496% |
| Live 20km from polling place | 1,643 | 8,407 | 412% |
| Disability | 1,296 | 12,714 | 881% |
| BLV | 668 | 4,818 | 621% |
| **TOTAL** | **46,864** | **283,669** | **505%** |

Another measure of the increased use of iVote is as a proportion of total votes cast at those elections, and as an element of the growing use of early voting options:

| | **% OF TOTAL VOTES** | |
|---|---|---|
| **VOTING TYPE** | **2011** | **2015** |
| **Early voting** | | |
| Pre-poll in-person | 8.2% | 14.1% |
| iVote | 1.1% | 6.2% |
| Postal | 5.7% | 4.5% |

| | | |
|---|---|---|
| Declared institution[1] | 0.3% | 0.3% |
| | **15.4%**[2] | **25.1%** |
| **Election day voting in-person** | | |
| Polling place | 74.3% | 67.4% |
| Absentee[3] | 9.5% | 6.3% |
| New enrolment[4] | 0.5% | 0.9% |
| Silent and others[5] | 0.3% | 0.3% |
| | **84.6%** | **74.9%** |

It is normal practice for the NSWEC to engage a third-party to survey electors following an election. Voters were generally satisfied with the experience of voting at the 2015 SGE.[6] Notably satisfaction was highest among iVote users, with 97% satisfied by the service. The next most satisfied were postal voters at 95%, and voters who attended a pre-poll in-person at 93%. Among those who voted in-person on election day 87% were satisfied.

| **Form of voting** | **Satisfied** | | **Dissatisfied** | | **Neither** |
|---|---|---|---|---|---|
| | **Very** | **Fairly** | **Very** | **Fairly** | |
| Pre-poll in-person | 70% | 23% | 1% | 4% | 2% |
| iVote | 80% | 17% | 0% | 1% | 1% |
| Postal | 73% | 22% | 4% | 2% | 0% |
| Election day voting in-person | 49% | 37% | 4% | 6% | 4% |

[1] A vote cast at a nursing or convalescent home, hospital or similar institutions at which election officials attend before election day.

[2] Percentages do not total 15.4% due to rounding.

[3] A vote cast at a polling place outside of the district in which a person is enrolled.

[4] A vote by a person who is enrolling at the time of casting their vote.

[5] A silent elector's address has been omitted from the electoral roll. Others includes votes by persons who appear to have already been marked off the roll in a polling place, and persons whose name does not appear on the roll who claim that to be an error.

[6] Ipsos Social Research Institute, *New South Wales State General Election Research: Prepared for the NSW Electoral Commission* (June 2015).

# Who is eligible to use iVote?

The bases for eligibility to use technology assisted voting at the 2015 state election under the *Parliamentary Electorates and Elections Act 1912* (NSW) (**PE&E Act**) were:

> **Section 120AB of the PE&E Act**
>
> (a) the elector's vision is so impaired, or the elector is otherwise so physically incapacitated or so illiterate, that he or she is unable to vote without assistance,
>
> (b) the elector has a disability (within the meaning of the *Anti-Discrimination Act 1977*) and because of that disability he or she has difficulty voting at a polling place or is unable to vote without assistance,
>
> (c) the elector's real place of living is not within 20 kilometres, by the nearest practicable route, of a polling place,
>
> (d) the elector will not throughout the hours of polling on polling day be within New South Wales.

## Eligibility at the 2019 state election

The *Electoral Act 2017* (NSW) (**Electoral Act**) will ultimately repeal the PE&E Act. The Parliament has broadened the bases for eligibility to include:

> **Section 152(1) of the Electoral Act**
>
> (a) the elector has a disability (within the meaning of the *Anti-Discrimination Act 1977*) and because of that disability he or she has difficulty voting at a voting centre or is unable to vote without assistance,
>
> (b) the elector is illiterate and because of that he or she is unable to vote without assistance,
>
> (c) the elector's residence is not within 20 kilometres, by the nearest practicable route, of a voting centre,
>
> (d) the elector is a silent elector,
>
> (e) the elector will not throughout the hours of voting on election day be within New South Wales,

(f) the elector is a registered early voter (technology assisted voting),

(g) in relation to a by-election—the elector will not throughout the hours of voting on election day be within the electoral district concerned,

(h) the elector meets such other eligibility requirements as may be prescribed by the regulations.

### *Silent electors*

A silent elector is an elector whose address has been omitted from the authorised roll or list of electors.[7] A person may request their residential address be omitted if they consider having that address on a roll would place their personal safety or that of their family at risk. While such a request is provided for by the new Electoral Act, a person will also be taken to be a silent elector if they have their address omitted from the roll kept under the *Commonwealth Electoral Act 1918* by the Australian Electoral Commission (**AEC**). There are currently over thirty-one thousand silent electors in NSW.

### *Registered early voter (technology assisted voting)*

'Registered early voter' is a new status granted under the Electoral Act. It is of two classes: 'registered early voter (postal)' and 'registered early voter (technology assisted voting)'.[8]

An application may be made to the NSW Electoral Commissioner (**the Commissioner**) to be a registered early voter if:

**Section 37(1) of the Electoral Act**

(a) the elector's residence is not within 20 kilometres, by the nearest practicable route, of a voting centre, or

(b) by reason of being seriously ill or infirm, the elector is unable to travel from the place where he or she resides (other than a hospital that is a voting centre), or

(c) because he or she will be at a place (other than a hospital that is a voting centre) caring for a person who is seriously ill or infirm, the elector is unable to travel from that place to a voting centre, or

[7] Electoral Act, ss 4 and 36. These provisions are fundamentally the same as the PE&E Act.

[8] Electoral Act, ss 4 and 37.

(d) the elector is enrolled pursuant to an application made under section 32(6) (which contemplates the provision of a registered medical practitioner's certificate), or

(e) a registered medical practitioner has certified that the elector cannot physically sign the elector's name, or

(f) the elector is a silent elector, or

(g) the elector is a person with a disability (within the meaning of the *Anti-Discrimination Act 1977*), or

(h) because of his or her religious beliefs or membership of a religious order, the elector:

(i) is precluded from attending a voting centre, or

(ii) for the greater part of the hours of voting on an election day, is precluded from attending a voting centre.

A person retains the status of 'registered early voter' until it is withdrawn by the Commissioner. Accordingly, the reasons for registration as an early voter do not include illiteracy, or not being within the state on election day (or district for a by-election), as circumstances that would not necessarily apply in future elections.

The new Electoral Act expands the existing role of iVote. Silent electors and, in relation to by-elections, electors who will not be within their electoral district on polling day are the immediate examples. The 'registered early voter' status also has the potential effect of expanding eligibility for iVote to people who previously may have used postal voting. The Parliament has also provided that it may in future prescribe further eligible electors by way of regulation.

### *Indefinite registration for people who are blind or have low vision*

As noted, registration as a registered early voter (technology assisted voting) is indefinite. This will likely be welcomed by electors with permanent blindness or low vision or physical disability. When I met with representatives of Vision Australia they advocated that people with permanent blindness or low vision should not be required to re-register for iVote prior to every election. They noted that this would provide equity to people who would otherwise be required to complete an extra requirement to exercise their right to vote, by comparison with many who face little challenge in attending a polling place at each election.

# Security

## What are the appropriate standards for security?

For protective security I have used the Australian Government's Protective Security Policy Framework (**PSPF**). This deals with what I have called "generic measures" for dealing with the security of people, places and information and data.

Cyber security is essentially part of the protective security, but given its prominence and high profile a separate set of standards has been developed by most organisations, including the Australian Government. So that, as part of protective security, agencies are expected to have a Cyber Security Strategy. In the Australian Government the essential requirements are set out in the Australian Government Information Security Manual (ISM), produced by the Australian Signals Directorate.

ISO/IEC 27001 'Information technology - Security techniques - Information security management systems – Requirements' is the key international standard. The "specific measures" discussed below are to some extent a function of the peculiar features of electronic voting and specifically, internet voting. A lot of ink has been spilt on this subject. There are standards promulgated by the Council of Europe, the European Commission, the Organisation for Security and Cooperation in Europe, the Organisation of American States and a variety of think tanks and organisations in the US. As well, there has been a lot written in academic literature on the appropriate standards. I have used the 'eleven essential principles' promulgated by the ECANZ. Although these are high level principles, they embody or refer to key standards such as voter privacy, verification, software independence, and transparency.

I have also identified some key principles that I believe electoral commissions should bear in mind. These have emerged in the course of my inquiry and I think they are worth setting out.

Electoral commissions should always bear in mind that the ultimate arbiter of election results is a court. In designing systems for elections, including internet voting, electoral commissions therefore need to have the sort of evidence that would enable a court to conclude that the system produces a reliable outcome and, if a problem has occurred, its effect has been identified. Their test should be: would a court say that this system is fair and reasonable? Can we demonstrate that to the satisfaction of a court?

The Parliament, the JSCEM and the Government should bear in mind that ad hoc decisions that impact on the electoral system may effect the security of the system. Security is the property of a system and "fiddling" with the system should be discouraged. Before making decisions to change or alter the electoral system in some way there should be the discipline of thinking through the implications for security generally. Government should always consider how changes to the electoral system have implications for security which on their face have nothing to do with security. This is going to be ever more relevant in a cyber future.

Having said that politicians should try not to make ad hoc decisions about the electoral system, it needs to be said that the iVote system will need to be continuously reviewed and updated in the light of experience. In this report I suggest that the NSWEC have the benefit of advice from a panel of experts. The idea is not to tinker with the electoral system, but rather to ensure that the hardware, software and systems that support the electoral system are "patched" or adapted to mitigate emergent threats and risks.

The Commissioner has considerable discretion to make these changes under the power to approve procedures for technology assisted voting.[1] This type of "adaptation" or "patching" is critical to security. The NSWEC should keep the JSCEM updated on this (sometimes through confidential briefs).

## Is the security of iVote appropriate?

The short answer is this: given the relative insignificance of the numbers currently involved in internet voting, and given the intention of tightening current practices through the iVote Refresh Project, security is adequate.

But the prospect of increased numbers of people using internet voting and the prospect of jointly establishing a national internet voting platform makes it imperative to lift security to a higher level.

The risk assessment carried out by PwC and my own conversations and observations confirm this assessment (PwC uses the phrase "security by obscurity"). It is not that security is not currently being attended to. Rather, it is not attended to as systematically and comprehensively as it needs to be, given the emerging threat environment and the fact that internet voting is now becoming "critical infrastructure". This is partly because of lack of resources and capability constraints. Developing a platform nationally would mean that resources could be pooled and critical capabilities at the Commonwealth level could be accessed.

Unpacking this assessment a bit more:

(1) The likelihood of successful tampering with iVote can be thought of as a product of a number of probabilities:

- Probability that someone wants to tamper with iVote,

[1] PE&E Act, s 120AC; Electoral Act, s 155.

- Probability that someone is able to tamper with iVote,
- Probability that any such interference would not be discovered and rectified.

(2) The assessment that I have come to after consulting with a range of people and discussing with PwC and intelligence officials is that the probability of each of these events is fairly small. Its product, or the probability of all the three events, is obviously much smaller.

(3) A lot of attention, particularly from cryptographers, is concentrated on the probability that someone could tamper with iVote. That is understandable from their point of view. And steps should be taken to deal with those risks, bearing in mind that no system will ever be riskless. But the probability that anyone will actually be motivated to interfere with iVote, given its current relative insignificant electoral impact, is very low. It would likely be very hard to change the outcome of an election currently by tampering with internet votes even if someone could. Also, provincial and local elections have a relatively low profile. Any propaganda effect is likely to be small or negligible. Although it may serve to damage the reputation of the system used for internet voting; and that may have national or international repercussions.

(4) It is important also to consider how elections actually work. In this context it is important to remember that Australia has a system of compulsory enrolment and compulsory voting unlike many other jurisdictions. Talking with experts and officials, if there were a large discrepancy between iVote outcomes and other outcomes in similar demographic areas, officials and political parties would be “put on inquiry”. They would look to see whether the results are “right”. That is one reason why I have emphasised the criticality of “end-to-end verification” (**E2E verification**), monitoring, auditing and also the use of profiling in this report. Tampering would have to be very clever and subtle to “get under the radar”. If it is that subtle, its ability to make large differences in electoral outcomes is likely limited. Although Australia’s penchant for preferential voting makes that more feasible than systems that do not allow for preferences.

The argument against internet voting that caused me most concern was put by the submission of Dr Vanessa Teague et al and suggested by some of the issues raised by Dr Roland Wen and Prof Richard Buckland.

The premise of the argument would be conceded by most experts in the area of encryption and cryptography. That is the contention that there is no electronic voting system that cannot in theory be penetrated and manipulated. It may not always be practical to do this. It may not be probable or likely. But it is always possible or conceivable that a system could be penetrated and manipulated.

A more troubling premise might also be conceded as well. That is the contention that any system could in theory be penetrated and manipulated without the penetration and manipulation being detected. Once again, while it may not be likely, it is possible or conceivable that this might happen.

We know that this sometimes does happen with physical voting systems. There are documented cases of penetration and manipulation with physical voting systems. In Australia this has been rare and small in scale. But in the case of electronic voting things could be different. Penetration and manipulation of an electronic voting system could occur on a very large scale and could be carried out remotely.

Hence the argument is that, in the case of electronic voting, penetration and manipulation could have significant consequences and impacts, because of the scalability of penetration and manipulation.

This argument does give me cause for concern. But on balance I am not persuaded. The key difficulty I have with this argument is that it places too much weight on theoretical possibility and not enough on empirical likelihood, or probability of things occurring.

Let me set out my reasons:

(1) As indicated in this report, I consider that on the current scale of internet voting it is unlikely that people will want to intervene to try to alter the election result. In any event, this is a matter of intelligence and it is an empirical question. The level of realistic risk is an empirical matter, and a key recommendation of this report is that electoral commissions should get very serious about integrating that intelligence into the way elections are run.

(2) In theory, while penetration and manipulation of results may not be detected, as a matter of fact it is highly likely that intervention that changed results would be detected. Psephologists, political parties, pollsters and other experts would most likely query and question outcomes that are inconsistent with expectations.

(3) If the mere theoretical possibility of intrusion and manipulation were sufficient to stop doing things, then we would not be flying in aeroplanes, using mobile phones, and engaging in electronic commerce and banking.

It could be contended that there are no "riskless" or "relatively riskless" alternatives to using aeroplanes or mobile phones or electronic banking, but that there is a relatively riskless alternative to internet voting – stick to the traditional method of physical voting with physical ballot papers.

However, for some people, it is not clear that there is this alternative: those with a disability, those who are living a long way from a polling place, those who are out of the jurisdiction (more or less, those who are entitled to use iVote under the current law).

To use more technical jargon, decisions are a function of probability and utility or the consequences of events occurring. Neither function is straightforward. The probability of intrusion will vary with circumstances and context, including time, geography, events, etc. Utility will also vary with the circumstances and context, with the prominence and significance of the election, the size of the cohort, the marginality of the electorate, etc.

Also, in the end, judgements and decisions are "political". Not in a "party political" sense, but in the sense that someone has to decide on the basis of

> evidence and information what is the best thing to do. Experts can provide information and empirical knowledge, but are in no better decision-making position to make trade-offs and value judgements than anyone else.
>
> For example, there seems all the difference in the world between running internet voting systems in local or provincial elections with a restricted or confined number of voters, and running internet voting for the US Congress in a highly charged geo-political context. Both the likelihood that something might occur and the significance of the consequences are going to be very different.

What seems to me to be reasonable from both a security and a social policy perspective is the current relatively confined ambit of internet voting. As I indicate in this report, going beyond that substantially requires a more systematic and ramified approach to security, including intelligence assessments, intrinsic design and extrinsic protective security.

## Security: generic measures

When analysing the effectiveness of security it is essential to understand what is being kept secure and safe, and what it is being kept safe from.

In this case what is being kept safe and secure is a system or process of decision making. It needs to be kept secure so that citizens can be certain that those elected really are their legitimate representatives. The stakes are high. This is critical infrastructure because it can affect what attitude citizens have to the legitimacy of their representatives, the Government and the decisions the Parliament and the Government make.

### What or who is the electoral system being protected from?

In one sense the answer is simple: people who might want to tamper with or manipulate or sabotage the system. There is a long list of possibilities:

- Other sovereign states which may want to create embarrassment or uncertainty or mistrust; or, which may want to change the result of the election covertly and secretly.
- Political parties or activists who may wish to change or manipulate the outcome of the election.
- Companies or organisations who may be trying to promote their interests generally or in a particular electorate.
- Terrorists who may see their cause advanced in fact, or symbolically, by attacking the heart of the democratic process.
- Professional "hackers" who may have been paid to tamper with the election.

- "Hacktivists" who may want to sabotage the election as a form of protest about internet voting, or another issue of debate. Other hackers may wish to do so "just for the heck of it".
- "Trusted insiders" who may be bribed or coerced into manipulating outcomes or sabotaging an election.

These characterisations are very broad. It is possible at any point in time that there would be much more specific and actionable intelligence about threats of interference. It is important for all electoral commissions to have a standing arrangement with Australia's criminal intelligence and national security agencies for regular threat assessments. There needs to be regular guidance on potential threats and the efficacy of mitigation. Without a proper understanding of threats it is not possible to put in place any sort of sensible system of risk management.

Before turning to the question of protective security and how that might be dealt with, it is worth pausing to think in a little more detail about what exactly this "electoral system" or "electoral process" is. I am centrally concerned with the iVote system, but that is part of a larger and more complex system, or systems.

The iVote system and the electoral system have complex relations with a number of other actors, corporations and systems. They do not exist in a vacuum, and nor should they. But protective security needs to understand and map the connections and relationships. For example, we know that data and intellectual property (**IP**) of corporations have been compromised through cyber intrusions into systems that sit at the margins. They might belong to the corporations' lawyers, accountants, or contractors.

A quick look at the current iVote system. There is Scytl, a private software provider; a variety of private providers of software and hardware – some contracted to the NSW Government, some to the NSWEC; private and public sector storage of data; academic and private sector advisors; telecommunications carriers. This is without looking at any intersection with the wider "electoral system" and a range of other services such as cleaning, maintenance, finance and administration.

It may seem forbidding to think about security on such a broad canvas. But it is important to look at threats and risks holistically, otherwise it is pretty much a waste of time. And protective security properly done should be integrated into core business models and management systems. It is not some arcane "add on".

## Protective security

Protective security is usually seen as encompassing three aspects:

- Security of places and premises.
- Security in relation to the people who work for an organisation.
- Security of information.

A good approach to protective security starts with a risk analysis of "the business". That includes an understanding of some of the key issues described above – the key relationships and dependencies, the key assets, the key threats and the key vulnerabilities (the key risks).

For example, in relation to data or information, an organisation needs to decide what critical information it has that needs to be secured. It needs a scheme for “classifying” information and a scheme for access to that information. It also needs to think about the best way to store and transact with the information, including physical storage and access. All of that will also involve the structure of the organisation and system of governance and decision making in the organisation. The organisation will also need to think about the procurement of goods and services. How much control they want to retain? What security requirements it wants to require of these services and equipment?

You can imagine that a lot of this has to do with “cyber security”, but it is important not to think of cyber security as something “special” or “separate” from protective security. It is not. It is an important new part of the way we do business and interact with each other. Some of the most significant breaches in cyber security have had to do with bad personnel practices, bad management practices and bad supervision – all to do with “trusted insiders”.

I do not intend to set out a protective security policy for the NSW electoral system here. Indeed, in my experience, the process of actually thinking through and developing a policy is as important and salutary as the product itself. But I do recommend that a comprehensive protective security policy for the NSWEC be developed, put in place and maintained.

## Further observations about security and people

For the NSWEC a lot of the issues around the vetting, recruitment, supervision and management are conventional. But at election time the staff of the NSWEC expands dramatically, and most of this staff is directly involved in the election. One of the things widespread internet voting would do is to virtually eliminate this added risk – but that is not likely to happen any time soon.

For the NSWEC, because of this dramatic “seasonal” expansion, well-designed protocols, training and “culture” are extremely important. Culture is an overused term these days but for the NSWEC it is very important. Openness and transparency are not natural attributes of the public service. For electoral systems, however, this is critical and needs to be part of the way officials “look at” and “think about” things. This is essential for trust and trust is essential to the proper functioning of the system. But openness and transparency are not an invitation to indiscipline.

An example of what I am getting at here is the issue of education and communication about iVote and internet voting. I will have more to say about this shortly. But as it is critical the citizens understand how to use iVote and how to do so securely, it is also important that staff in the NSWEC understand iVote. It should not be a “black box” to the officials responsible for managing elections in NSW. During previous elections iVote has largely been operated by the team of IT managers and developers who were responsible for implementing the system. In other words, the system has been managed by the IT experts separately from the election officials managing all of the other voting methods.

The NSWEC has restructured these arrangements. A new operational model will incorporate iVote in overall election management and provide for better separation of functions and duties. During future elections iVote will have an operations staff, rather than its managers and developers. It is important that the NSWEC review the effectiveness of this new approach.

Another feature of iVote is the complexity of the legal arrangements and the number of "players" involved. Maybe this is part of the design for security, but it certainly raises questions about the number of people who may have access to critical aspects of the system and whether the vetting, controls and supervision have been adequately thought through. More importantly, the NSWEC needs to have control over these people and services for the purposes of delivering iVote. It is not clear that it does. This is probably partly a matter of contract and partly a matter of internal government instructions. By "control" here, I mean that the NSWEC needs to have the power, knowledge and ability to direct things be done or not done, and to ensure compliance with the directions they give.

I note the NSW Auditor-General has recently been critical that many public service agencies do not adequately manage contracts for IT services, particularly in relation to cyber security monitoring and reporting.[2]

## Governance

Governance will also figure as a key element in security. Risks need to be dealt with at the right level of an organisation. Much of what is in the PwC risk assessment presupposes that governance has been well-designed and is efficient and agile. Many of the risks that need to be dealt with are dynamic. They will shift and morph over time. Whether it has to do with external threats of technological change or opportunities for mitigation, there needs to be the ability to make quick and well-informed decisions, and to implement these decisions. These are not always attributes of the public service.

I recommend the institution of a panel of experts that can be used to quickly give the NSWEC advice on a range of issues relating to iVote and internet voting. Whether this has to do with changes in the system, changes to policy and guidance on procurement. The panel should include expertise in protective security, cyber security, government and electoral issues and technology.

## Storage of information

Storage of information about voters is not strictly something for this report. Information about voters is collected and stored by the AEC and shared with

[2] NSW Auditor-General, *Report to Parliament: Detecting and responding to cyber security incident* (March 2018).

electoral commissions in the States and Territories, pre-eminently through the electoral roll. The NSWEC also collects information about voters.

We know that in the US presidential election of 2016 there were attempts to access and probably tamper with this sort of information. It is also clear that destroying or altering this sort of information is a possible way of interfering with elections.

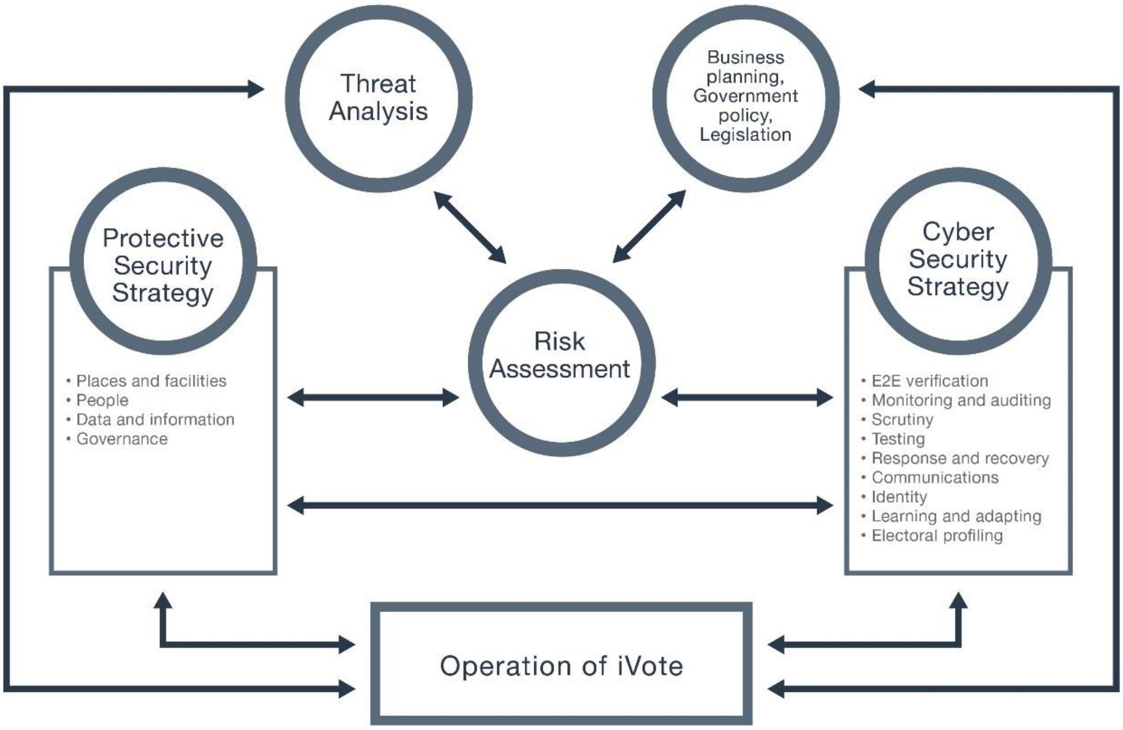
There are a range of techniques and facilities for securing and checking the integrity of storage of information. These techniques and facilities are employed by a range of agencies and businesses.

The NSWEC, and the AEC, need to ensure that they are employing state of the art techniques and facilities and are regularly reviewing and testing the integrity of their systems for storing information. This should be central to any cyber security strategy.

It should also conform with privacy laws and policies.

# Security: specific measures

We have looked at a number of security measures, threat analysis, risk assessment, protective security in respect of premises and facilities, in respect of people and in respect of data and information. The general scheme of security for the system set out in this report is shown schematically in the diagram below.



Traditional voting carries risks of manipulation or tampering that cannot be excluded. However, with internet voting the theoretical scalability of manipulation or tampering is much greater.

This heightens the importance of mitigation measures such as E2E verification and monitoring and auditing. The great virtue of E2E verification is that it enables individual voters to assure themselves that their vote has not been manipulated or tampered with. It is direct experience that the system is working reliably.

If we consider specifically an internet voting system like iVote, what are the key security measures over and above those generic measures?

Unsurprisingly, the submissions received have focussed on the cyber security aspects of iVote.

There are a range of views that may be broadly classified as follows:

- Pessimists: those who say that there are vulnerabilities with iVote which mean that citizens should not trust iVote, and these vulnerabilities probably cannot be fixed; at least, not now.
- Optimists: those who say that no system can be guaranteed, that the vulnerabilities of the iVote system are not significant, and, in any event, the vulnerabilities can and should be addressed. On this view voters should trust the iVote system, but it needs to be constantly updated and improved.
- Agnostics / Qualified Optimists: those who say that iVote has vulnerabilities which do need to be attended to, but given the comparatively small scale of its use currently, voters should view security as adequate. But going forward there needs to be a more radical reconsideration of the design and operation of the system. This will take time and resources and the marshalling of expertise.

Interestingly, among these three approaches there is considerable agreement about the general nature of key vulnerabilities:

- E2E verification: iVote does not adequately incorporate E2E verification.
- Monitoring and auditing: iVote does not adequately monitor and audit transactions. Hence, there is increased risk of undetected intrusion.
- Scrutiny: There is not adequate openness and scrutiny of the iVote system for political parties, experts and the public generally.
- Open source code: The source code for iVote is not public and subject to examination and critique, as is the code in some other jurisdictions.
- Testing: The testing regime around iVote is neither regular enough nor robust enough.

It is important to say that it is not being contended that NSWEC does nothing on these issues. Rather it is contended that what is currently being done can be improved upon and needs to be improved upon.

PwC's risk assessment of iVote also identified these as key risks that require further mitigation. I also note that iVote Refresh Project documentation identified these as areas for attention.

Based on the submissions, the literature, PwC's analysis and my own observations and conversations with my panel members, I consider the following are the specific features requiring attention:

1. An internet voting system should exhibit E2E verification while maintaining the secrecy of the ballot.

2. There should be a robust way of monitoring and auditing the system so that errors or intrusions can be detected and rectified.

3. There should be independent scrutiny and interrogation of the system by experts, political parties and citizens.

4. There should be a regimen for testing the system.
5. There should be plans for response to and recovery from “attacks” and these should be subject to a regimen of “exercises”.
6. There should be an active strategy of communicating with stakeholders and citizens about internet voting, including issues of cyber security and “cyber hygiene”.
7. There should be a system of electronic mark off and due diligence for registration.
8. There should be institutional design and encouragement of a culture of learning and adapting.
9. Electoral polling and profiling should be used to help identify discrepancies.

I will elaborate on each of these features.

# 1 E2E verification

Protective security is not peculiar to the NSWEC and iVote. The observations and suggestions in the previous sections are more-or-less generic. They would apply to most systems and organisations.

A key difference between voting systems and other internet systems is the way in which these key principles are in tension and even, in a sense, inconsistent. Transparency and openness are key requirements of an electoral system. But so is the secrecy and privacy of the individual vote. No one should be able to find out how someone else voted. And then there is the requirement of security where the vote needs to be secured and “seen” to be secure even though no one is allowed to know how anyone else voted.

These tensions explain why analogies with systems like internet banking are not exactly relevant. We allow our bank to look at our accounts and transactions. Indeed we encourage that up to a point. But we do not allow electoral officials to do that with our votes until they are “depersonalised” or “anonymised”. Bank transactions can be verified by my banker, but I am the only person who can verify that my vote as cast is the vote I intended to cast.

On the other hand, we also want to maximise openness and transparency. The election system needs to be seen as reliable and trustworthy. In a democratic system of government that is of the essence. To the extent things in the system are obscure or hidden or secret there is a danger that citizens will begin to question its reliability and trustworthiness. Indeed, it would be useful for electoral commissions and governments to work with a maxim or presumption in favour of transparency and openness. I would go further and say that openness and transparency is not enough. Electoral commissions and governments also need to ensure that the electoral system is understood by, and intelligible to, voters. There needs to be active communication.

The “gold standard” for voting systems is E2E verification:

- Every voter should be able to verify that his or her vote has been cast-as-intended.
- Anyone should be able to verify that all and only valid votes have been collected-as-cast.
- Anyone should be able to verify that the votes as collected have all been counted (referred to as **counted-as-cast** or **counted-as-recorded**).

This is a key standard for internet voting. Think of it as the equivalent of the standards for the securing of ballot boxes in physical elections, the protocols around sealing, storage, delivery, opening of boxes and counting of ballot papers. If these protocols are properly adhered to then we can have confidence in the result. Similarly if an internet voting system adheres to E2E verification then we can be confident in the result.

In terms of security, the NSWEC should employ a system for iVote that adheres to this standard.

Scytl says that its current system does adhere to this requirement. Some critics contend that it does not. The iVote Refresh Project documentation indicates a number of aspects for improvement that have to do with E2E verification.

In this report I do not intend to get involved in a detailed technical critique of current or future iVote systems. I will, however, make a number of observations and suggestions.

First, as I say, E2E verification is an important standard and should be central to the design and procurement of an internet voting system. That is acknowledged by the ECANZ in their eleven essential principles, and is also advocated by expert submissions to this inquiry.

Second, E2E verification, although critical, is not the only consideration. As I pointed out above, and as the ECANZ note, the "usability" of the system is also critical. There is no sense in having a perfectly secure system that no one can understand or use.

Third, technology is constantly developing. There are already a variety of ways in which E2E verification might be delivered, and there are a variety of emerging technologies (such as blockchain) that might do even better. There is also the discovery and development of new vulnerabilities and techniques for tampering and intruding. All of which underlines the importance of having flexibility and agility as part of the way these systems are deployed.

Fourth, E2E verification is normally interpreted as a standard that says voters should be able to verify that their vote was cast-as-intended. Most internet voting system give voters the option of verifying. They do not make it mandatory to verify. Given how critical verification is to security, and given that the individual voter is the only person who can verify the content of their own vote, I think electoral commissions should seriously consider making verification mandatory. In other words, to cast a valid internet vote there would be two steps – cast the vote and verify or confirm the vote. We already do this 'two step' process for certain banking transactions, to authenticate a range of consumer transactions, or to access remote computer networks. It would greatly enhance security.

## Other views on mandatory E2E verification

Some of my panel members and some commentators have raised issues in relation to mandatory E2E verification.

The issues include:

- Mandatory verification would create a requirement that is additional to compulsory voting. That is, if an elector votes but does not verify, have they voted or not?
- 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. Voluntary verification will achieve this.
- Mandatory verification may to lead to "false positives" as voters will misremember their 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 monitoring and auditing and scrutiny measures for iVote discussed in this report. 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.

First, it is true that voters cannot rummage through ballot papers to check that their vote remains as intended. For physical voting, the NSWEC has procedures in polling places and the places where votes are counted to mitigate the risk that a vote can be changed. With internet voting there is also a possibility that a vote could be altered by a malicious actor after it has been "transmitted" to the "virtual ballot box". I have referred to various measures that mitigate that risk, of which E2E verification should be effective. Hence my advocacy of mandatory verification by individual voters.

Second, E2E verification is not only about the statistical adequacy of verification. It is about individual voters being psychologically assured, or trusting, that the system works. They know it works because they have checked it, and they know that everyone voting has to check it is working. E2E verification is not only about statistics, it is about individual perception and trust.

Third, it is true that only NSWEC officials and not just anyone can currently verify that ballot boxes have been properly sealed, stored and delivered for counting. But that does not mean that if it is possible to be more transparent with internet voting we should eschew that possibility because we do not do it for the physical ballot paper voting. The thrust of my argument is that greater transparency in electoral systems is always a good thing.

# 2 Monitoring and auditing

Monitoring and auditing is really an aspect of E2E verification. In concept this should be something that electronic records make more possible and easier to do.

Scytl, for example, has a system that enables anyone to see that only “signed” or “certified” valid votes have been collected in the “virtual ballot box”. Movements and transactions involving these “votes” or at least the “virtual envelopes” that contain the votes are logged.

In the iVote system developed for the 2015 SGE these encrypted votes are duplicated so that two “envelopes” containing the same vote go into different virtual boxes: the ballot box proper, and a box that can be accessed by voters for verification purposes. This illustrates the sort of functionality available in internet voting. But this functionality needs to be properly used to identify any possible problems. It should be possible to be quite targeted and specific about the locus of any issue.

Auditing is more than monitoring. It is an authorised process of checking to see that things are in order. Typically, it is carried our ex post facto. But it need not be. Currently, PwC carries out a procedural audit in the course of an election. It checks to see if the authorised procedures have been followed. It does not monitor or check for discrepancies or issues with the collection or counting of votes per se.

Elsewhere I am suggesting that the NSWEC establish an expert panel to consider the outcome of election and advise the NSWEC on issues, problems, and “learnings” that come to light. I do not suggest any further “real-time audit role” for this panel, although its deliberations would clearly benefit from such a function.

I am also suggesting a different and augmented role for political parties in monitoring and interrogating the system. That is an important function, but not a substitute for real-time audit.

Clearly monitoring should make use of electronic “tools” to identify possible problems and issues. But over and above that I think there should be a person or persons whose job it is to monitor and audit the system in real-time and bring an assessment of problems and discrepancies to the attention of the NSWEC.

I also think the role of “procedural” auditor currently fulfilled by PwC should be expanded to include a report on the adequacy of the system including the process of monitoring and dealing with problems and discrepancies for each election.

The sort of skills required in relation to these roles would ideally include experience in cyber security as well as a knowledge and understanding of electoral process.

# 3 Scrutiny

Scrutiny in the electoral system has a specific meaning. It is a process where political parties watch and interrogate the administration of an election, especially the counting of votes. It has the advantage of sorting out a number of potential problems and uncertainties quickly and efficiently and without resort to formal process.

The role of scrutineers in traditional, physical elections is to add an additional level of surety that there are no errors or political bias in counting the votes. More importantly, so it is seen that there is no political bias. Should a particular vote be admitted? How should a particular ballot paper be interpreted? Because the interests of the different parties balance each other there is a "rough fairness" in this and a check on the processes.

In the case of internet voting, there is effectively no scrutiny of this sort, and there really cannot be. Most of the discrepancies and issues that arise in physical voting contexts are not going to arise with forms of electronic voting or internet voting. In fact, that is one reason for having electronic and internet voting. There is no ambiguity about ballot papers, and counting can be done rapidly. It is much more efficient.

So what is the role for scrutiny in this "new world"? The problems and the sorts of decisions that will need to be made by electoral officials are more likely to involve the malfunctioning of the system or possibly signs that the system has been illicitly manipulated in some way. To assess these sorts of judgements and to provide relevant input or objections and justify them is going to require a different kind of scrutineer. As I remarked to one party official, "you are going to need someone who is a 'tech nerd' but with 'political savvy'".

In one way there is really no special role party representatives can play in monitoring internet voting. There is no role that could not be played by anyone else who understands internet voting systems and has access to the logs or records of transactions.

Political parties could and should make sure they have people with that experience, and make sure they do monitor and interrogate the process. There seems to me no reason why political parties should not have virtually uncontrolled rights to monitor the system from "lock-down" to count. And, importantly, to interrogate the system. We will come back to the limits and constraints. There may be limits to access some aspects of intelligence and operational security.

Political parties could and should be part of the process of educating the public about internet voting and security. Political parties could and should use their knowledge of electorates and voting profiles to watch for discrepancies and possible issues. This is a skill and knowledge that most other people do not have. It is an important check on the system, and I recommend elsewhere that the NSWEC should encourage research into electoral profiling.

One of my themes is the importance of openness and transparency. Except for the secrecy of the content of votes, it is good to have a presumption in favour of openness and transparency. Physical voting is, after all, a public process. The NSWEC should consider whether there is any good reason why political parties, experts and any citizen who is interested should not be able to "see" or view the process of collecting and counting internet votes. After all the content of those votes is encrypted until the count, so what else is there that needs to be secret?

There is an area where political parties may still need to be involved in pragmatic decision making – where some problem arises with the system that needs to be quickly resolved. These things happen with all systems. The NSWEC will need to make a decision about what is a reasonable way to proceed. Perhaps in that context it would be sensible to consult with political parties in some circumstances.

One further measure I will be recommending is that the JSCEM needs to stay across the emerging issues of internet voting, and there will no doubt be some very significant issues. Keeping law and policy abreast of developments in cyber is not easy, and is not going to become easier. The cyber world moves at any entirely different speed to governments and parliaments. I suggest that the JSCEM have technology assisted voting as a standing item on its agenda. I also suggest that the JSCEM consider the best way to permit the NSWEC to make urgent decisions to deal with emergent threats and issues, which may require expenditure of funds or changes to law or policy.

The Court of Disputed Returns has developed a jurisprudence that minimises its involvement as far as possible. This is mainly because the Court places a premium on getting an outcome, and also because it does not want to encourage endless litigation. The Court has therefore taken the view that it will generally only worry about disputes that could impact the outcome of an election. The time limits for bringing an action in the Court are also very short.

There is however the prospect of different sorts of issues or disputes arising under a system of internet voting. Political parties or members of the public might think that the system does not work in such a way that the results should be trusted. That may be because it is not “tamper proof” or because it is contended there is evidence of tampering. The Court would presumably apply an onus of proof based on the balance of probabilities. Is there evidence to show that it is likely the result has been tampered with? But the Court may also take the view that the NSWEC should take reasonable steps (a) to ensure that the system is “tamper proof” and (b) to demonstrate that it is tamper proof. In other words, the NSWEC must have the capability of monitoring and securing the system to some sort of “reasonable standard”, and must be able to bring evidence from its program of logging and audit. And the Court must have the capability to make this sort of assessment.

## Should the iVote source code be made public?

Let me touch on the issue of the constraints on transparency and openness. I said above that there should be a presumption of transparency and openness. A number of submissions have strongly advocated that the software code for internet voting should be made public.

The arguments for doing that seem to have two limbs:

(1) By making the code open you allow the widest possible community to test that code, to identify problems and solutions and to optimise the efficiency and effectiveness of the code.

(2) It is a piece of critical infrastructure that is essential for the proper functioning of the democratic process which should, as far as possible, be transparent and open.

The arguments against this type of openness are roughly of three kinds. First, this type of openness is relatively useless and very time consuming given the limited number of experts and the ability to get their advice and views anyway. Second, it provides useful information to possible malicious actors. Three, it creates potential problems around IP for commercial providers. It might also be argued that the way discussion around internet voting and electronic voting has developed a degree of antagonism has arisen. To some extent the discussion, or debate, is "ideological" on both sides. It certainly is in danger of creating "more heat than light".

In my view IP is not really a consideration here. Private companies can still take steps to patent their IP. They are unlikely to turn down a lucrative contract for the reason that code will be made public. Also, suppliers already work in open source jurisdictions overseas.

The real arguments here have to do with balancing security with scrutiny and testing. Undoubtedly there are systems where security considerations would be overwhelming, for example, defence systems; where there could be no question of allowing code to be available publically. Electoral systems are now seen as critical infrastructure, certainly since attempted intrusions into the US electoral systems. But a good deal of the workings of these systems is and should be public because it is essential to their critical function.

The choice is not a simple binary one between 'open' and 'closed': there are degrees of openness. The solution to this problem could lie somewhere between these poles. Perhaps giving some experts access under conditions of non-disclosure or even under conditions of firstly disclosing to the NSWEC any problems discovered. My own view is that the code should be made public, and that IP issues should be sorted out through commercial negotiation. I note that the JSCEM has also reached this view and the NSW Government has accepted in principle the JSCEM's recommendation in this regard.

# 4 Testing

Proper testing of systems such as iVote is a key measure for securing the system.

There is a variety of ways in which this can be done and a variety of agencies and companies that can do it.

It can involve simply testing the robustness of the technology. Or it can have the broader scope of testing the electoral system as such to see how difficult it is to manipulate or tamper with.

The NSWEC needs to have a regimen for testing at regular intervals and also an arrangement for "surprise testing" or "unannounced testing" of some aspects of the system.

The results of the tests need to be considered by the NSWEC and by the expert panel I have recommended. The results need to be considered at the top level of management.

This is also the one area where openness and transparency may be problematic. In my experience in government, penetration tests always succeed in penetrating. It often requires considerable skill and craft, but penetration occurs. It is not always sensible to reveal the outcomes or learnings of testing, except in a limited and confidential way. That there has been testing and how and when it occurred can be made public. But to reveal the outcome or result of testing can provide dangerous intelligence to possible malicious actors, even if steps are being taken to address vulnerabilities. It can also reveal not only weaknesses in systems, but very often capabilities, techniques and modus operandi of the "attackers".

# 5 Response and recovery

There needs to be a plan about what to do if things go wrong with the system. There are very different sorts of things that can go wrong. There will also be things that go wrong that were not envisaged or anticipated. So "response plans" or "recovery plans" are not simple.

Nor can you simply "set and forget". Plans need to be constantly reviewed and updated in the light of experience. And not only the experience in NSW or Australia – there needs to be a good research base about what is happening internationally.

"Resilience" is a key property of a system when we consider response and recovery to incidents. Prevention is obviously a better thing to do – avoid the incident or problem in the first place. A lot of the recommendations in this report have to do with preventing breaches of security. But it is necessary to have a plan about what to do, if despite best efforts, there is a breach of security.

A resilient system is one that can recover rapidly with minimal negative impact. For example, we might discover that a limited number of votes have been affected by malware. If we can be sure that the malware is quarantined to a few votes and we can be sure that those votes are not going to have an impact on the election, then it might be reasonable to continue with the election. But even in that case there would need to be a carefully documented decision, consultation and good communication. How all of that is handled and sequenced is the substance of a response and recovery plan. Typically such a plan will need to encompass governance, coordination, and decision making. It will need to encompass technological and logistical issues, communications, and legal issues.

There also needs to be a regimen for "exercising" these plans. Given the similarity of systems around Australia there would be merit and efficiencies in coordinating the process of planning and exercising. Under some scenarios it will probably be necessary to include other agencies such as the police or Departments of Premier and Cabinet, or Departments of Finance.

It is quite possible to run "desktop" exercises to test a variety of scenarios. These types of exercises are employed very effectively by the Commonwealth Department of Defence. They have the advantage of being relatively cheap to carry out and of being able to involve extreme and complex scenarios with a high level of confidentiality. Desktop exercises will not normally be able to test operational preparedness.

So issues of design, verification and monitoring have a bearing on resilience. But so does governance, training and communications. Resilience can be seen as a function of good risk identification and appropriate mitigation. Except, there is a residual risk – what we might describe à la Rumsfeld as "unknown unknowns" – which really defines resiliency. It is the capacity of a system to adapt rapidly and handle novel and unexpected circumstances.

## 6 Communications

One of the key risks identified by PwC has to do with communications with voters and citizens.

The Federal Constitutional Court of Germany has made the point that democracy is a public process and needs pre-eminently to engage the public. To engage citizens the electoral system needs to be transparent and intelligible. I have discussed processes of verification and how important that is for security. But it is also important for political engagement and the legitimacy of the process.

It cannot be a "black box". People need to understand internet voting, how it works, what their rights and obligations are in using it, and what they can do about cyber security and cyber hygiene.

For example, a very important cohort of potential users are people with disabilities, especially people who are blind or have low vision. I have had extremely useful discussions with a variety of peak organisations. It would be good to mount an information campaign through these peak organisations. The campaign should not shy away from issues of cyber security and cyber hygiene. In fact it would be sensible to involve telecommunications companies to get out messages about cyber hygiene in particular.

Communications needs to be more than sending out information to people. It needs to be a strategic process of communications. It needs to be interactive, two-way communication. It needs to involve telecommunication companies, and it may need to involve schools, aged care and disabilities facilities, and perhaps local government in the future.

The content needs to be well thought through. Cyber security is a problem that is not peculiar to voting systems. So there are obvious synergies here with messaging from other companies and agencies, up to a point. It may be possible, for example, to encourage cyber hygiene by making it a precondition for internet voting.

Website applications are able to detect the "version" of the browser and operating system a visitor to the site is using. A blunt approach might ultimately be taken to block access to those using what the NSWEC determine to be outdated or vulnerable software. However it is vital that from the point of registration iVote users are encouraged or "nudged" to not only check their software and be given information about how to do so, but also educated about the reasons why such measures are encouraged.

The NSWEC should also not shy away from the issues of cyber security as people have been inundated with reports about Russian interference in the US elections. Rather, this is an opportunity to explain the importance of using the verification system, for example, and to explain how the system works and what voters can do themselves to enhance security.

The NSWEC should think about how to use social networking to communicate on these issues, including providing interactive content such as "webinars". Feedback and criticism is an important way of understanding issues that need to be addressed.

Political parties are key for communication. They have asked for periodic presentations to their staff on how iVote works. In Australia, where voting is compulsory, there is little need to encourage people to vote. But there is a growing number of channels for voting. Political parties have an incentive to make sure that voters understand those options. That also gives them an opportunity to advocate.

If parties were able to facilitate registration for internet voting in the way they do for postal voting, then they would have the incentive to make sure people understand how the system works and be an important part of "educating" the electorate. This is something that requires serious examination; detailed discussion is probably beyond the scope of this report.

# 7 Identity

Identity is important here. Impersonating someone or creating a fictitious voter needs to be excluded. Governments in Australia have taken limited action in relation to this issue. Mostly because it does not appear to have led to any discernible problem of any significance.

Prof Rodney Smith produced a research report for the NSWEC concerning multiple voting and voter identification.[1] He found that a large number of apparent but ultimately false multiple votes are created by NSWEC "mark-off data", that is, human error by the polling place workers when crossing off voters names in the polling place. Once the false multiple votes are removed, the evidence is that multiple votes form a very small proportion of overall voters – only 0.08% or less than one vote per thousand - and is too small to determine the winner in any seat. What multiple voting exists is not strategic, and is not directed at marginal seats. Rather, it is strongly related to demographic factors such as fluency in English.

But internet voting could change that. And governments will need to tighten up the enrolment and authentication and verification of voters. It is something that is becoming increasingly simple to do. And with multiple voting channels, more important.

[1] Rodney Smith, 'Multiple Voting and Voter Identification: A research report prepared for the New South Wales Electoral Commission' (February 2014)

The JSCEM 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.[2] I would reinforce that recommendation. From a security perspective this should be a priority. There are now a range of voting channels. Voters need to be sure that their vote cannot be duplicated or replicated. That is critical for trust in the system.

With iVote it should be possible to identify any duplicate vote and cancel it. But if there were no electronic mark off, the NSWEC would not be aware of this duplication until it was too late to remove the duplicates. If voting is compulsory and there is electronic mark off, there is a little prospect that there could be duplication or replication of voting of any significance.

When a person enrols to vote they need to provide either a driver's licence or passport number or the endorsement of another person enrolled to vote. The authenticity of these other forms of identification is checked by the AEC against a database of passport numbers and driver's licences to confirm such a document has been issued to a person by that name. In other words, such a check goes some way to preventing the enrolment of fictitious persons.

In my view the provision allowing a currently enrolled voter to endorse a person's identity for the purpose of enrolment constitutes a considerable weakness in the system of authentication and verification of identity. It should not be allowed.

When a person registers for iVote there is a check to ensure that the person is on the electoral roll. That should ensure that it is not possible to register fictitious voters to use iVote. But it does reinforce the importance of strengthening the enrolment procedures so that documents must be produced and verified. Eventually, one would hope that biometric verification is used.

Currently the NSWEC sends letters to some voters who have registered to use iVote. It does not, however, send a letter to those who have provided identity documents, such as a driver's licence or passport when registering. Those documents are verified through the Document Verification Service (**DVS**) at the point of registration for iVote. The DVS is a Commonwealth facility that confirms such a document has been issued to a person by that name. This is very important to protect the security of the system by ensuring that duplicate or fictitious votes cannot be created. It would be better to insist on the use of identity documents for all registrations.

Not only would that obviate the need to send out letters, it would also remove a weakness in the security of the system which might allow fraudulent voting.

## Coercion and vote buying

Internet voting is voting outside a polling place. In theory, it therefore lends itself to greater potential for coercion of voters or bribery of voters to "buy" votes.

[2] 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 1.

Prof Smith has carried out extensive research on this topic in relation to conventional voting. His conclusion is that in the current physical voting system there is little coercion or bribery. His contention is that this is simply not part of the culture or social mores of Australian elections and has not and is not likely to be an issue.[3] To the extent that voter interference might exist at all in Australia, Prof Smith found it is likely to be extant small-scale "expressive" voter coercion (such as family voting or sect voting that seeks to affirm the identity or values of the group through their actions), rather than the large scale activity necessary to affect the outcome in a particular electoral district.

Will internet voting change that? I think it is unlikely to for a number of reasons:

(1) The penalties under electoral legislation and under the Crimes Act are substantial.[4]

(2) The reputational risk for political parties is extremely high.

(3) The funds of parties are largely a matter of public record. Questionable use of these funds would quite possibly come to light.

(4) There probably are instances of coercion in certain communities of the sort identified in the United Kingdom in the Pickles Report.[5] This is probably relatively rare and isolated. And it is usually better dealt with as part of a deeper social issue.

(5) Voting in Australia is mandatory, so that some of the issues about "getting out the vote" do not arise as they do where voting is voluntary.

(6) The iVote system itself allows a voter to change their vote and cancel their previous vote. There is no receipt that reveals the content of the vote, although it would be possible to use the verification process to reveal the content of the vote.

(7) It would be difficult for someone to be sure that they had successfully coerced or successfully bribed a voter. Arguably it would be easier to simply require a physical voter to take a photograph of their ballot paper with a mobile phone.

While coercion and bribery cannot be excluded, that possibility does not constitute sufficient reason to rule out internet voting. Nevertheless, there should be vigilance and any evidence of coercion or bribery should be thoroughly investigated.

[3] Rodney Smith, 'Internet Voting and Voter Interference: A report prepared for the New South Wales Electoral Commission (March 2013).

[4] The Electoral Act provides a maximum penalty of 200 penalty units or imprisonment for 3 years, or both.

[5] Sir Eric Pickles, *Securing the ballot: Report of Sir Eric Pickles' review into electoral fraud* (August 2016).

# 8 Learning and adapting

Another important risk that PwC identifies is having the capability to learn and adapt on a continual basis.

To some extent this has to do with the flexibility of the arrangements the NSWEC enters into with providers. It also has to do with the institutional arrangements in place for testing, researching, keeping abreast of the threat environment and having a robust process for feedback and review.

But pre-eminently it has to do with “culture”, a much abused term. By that I mean the attitude of top management in particular.

The cultural values that are important in this context are a firm presumption in favour of being open and transparent about policy and process unless there is a good reason why not. An electoral system does not only have to be efficient and trustworthy, it needs to be seen and believed by citizens to be efficient and trustworthy.

As for institutional arrangements, I have suggested a range of measures above. It is important to understand these suggestions systematically, not as individual modules. There are, of course, different ways of approaching security and its different aspects. But one thing that really must be done is to think about security systematically or holistically and as part of core business.

# 9 Electoral profiling

By “electoral profiling” I simply mean the process currently carried out by pollsters, parties and academics of polling sections of the electorate.

The reason why this is important from a security point of view is that it gives an indication of what voter intentions are. It is a check on the integrity of the internet voting system that is independent of the electoral system. Of course, it is not authoritative or definitive, but it is an indication. If there are significant discrepancies then there is probably a case for further inquiry and investigation, to see what the cause of the discrepancy might be.

As a matter of security, the NSWEC should take a close interest in polling, its methodology and credibility. Longitudinal and sectional analysis of voting intentions and even more sophisticated analysis should be part of that.

For example, while it may offend the convention of not beginning to count votes until the close of polling, it should be possible for the NSWEC to analyse iVote results in real-time during the election period against previous election results and current polling.

# Other issues

There are some other issues that were raised in submissions that I want to deal with.

## Resourcing

This is not a cost and benefit study, but it should be obvious that internet voting has both costs and benefits.

The benefits include access and convenience. In some cases this amounts to the difference between being able to exercise a right to vote and not being able to.

Accuracy and speed of counting votes is also a benefit. The laborious process of ferrying ballot papers would be completely avoided, and the vagaries or handwriting and the intention of voters would disappear as an issue of contention. Every vote could be brought to the count almost instantaneously.

The cost and dependability of postal services and human judgement, interpretation and supervision, would become less relevant.

On the other hand, there will be costs. Some of these costs will be capital expenditure. This capital cost is likely to be "lumpy" and "up front", as opposed to recurrent savings which may occur further down the track, with the decreasing need for a large casual workforce.

The design and development of a robust national voting platform, for example, will need dedicated funding and people. This could take up to four years according to the submission of Dr Roland Wen and Prof Richard Buckland. The team would need to be taken "off line" as it is impossible given the crowded nature of the electoral cycles in NSW, and elsewhere in Australia, to rely on people who are also involved in administering elections. If the national internet voting platform is to proceed, then increased resourcing is imperative. That expenditure can be shared between jurisdictions.

My own observations and PwC's analysis lead to the conclusion that the skills and capabilities and numbers of people supporting internet voting in the NSWEC are going to need to increase substantially. This report outlines a range of areas where greater effort and resourcing is going to be needed.

While iVote has been small and relatively insignificant in terms of electoral impact, now is the time for a “step change” in the arrangements for internet voting and that will take money, though not only money. One aspect of resourcing is making sure political parties are properly equipped and trained to play the important scrutiny role I address in this report. This is a function that is in the public interest. It is not just a “hand out” to political parties. It is very important to get parties to properly participate in this system. Nor, as I have described, is this a simple “information” campaign. It needs to be much more strategic than that, and will require the “harnessing” of key sectors and organisations (telecommunications companies, for example).

Similarly, a communications strategy to the community and particular sections of the community such as people with a disability is not just “nice” or “useful”. It is essential to the integrity and utility of the system. Resourcing peak representative and community organisations as part of this strategy would make a lot of sense.

## Ballot papers

The tractability and comprehensibility of ballot papers has been an issue in Australia. That is not likely to change. Preferential voting complicates what is required of voters. It has also been raised in submissions to this inquiry.

How to render ballot papers in electronic form so they are understandable, useable and fair to candidates is an issue that was raised with me by both parties and potential voters. There is no easy answer to that. But it is clear that simply translating physical papers into electronic form may not be the best thing to do.

“Randomisation” of the columns in which the parties appear on the ballot paper was not favoured at all by parties because it impacts on the production of how-to-vote material. The requirement to “click” at the ends of the virtual ballot paper before it could be submitted was suggested by some. This would, at least, force voters to “scroll” through the entire ballot paper. The option previously proposed by the NSWEC is randomising the initial “view” of the ballot paper, rather than always firstly presenting the top left of the paper. This measure should also address the apparent bias in iVote results favouring leftmost groups on the Legislative Council ballot paper at the 2015 SGE due to “donkey voting”.

My own suggestion, which will be viewed as heretical by many, is that what voters need is an “auto-fill” device. So that if a person wanted to voter for party “X”, and in accordance with that party’s suggested preferences, they simply press the “auto-fill” button for party X and the ballot paper is automatically completed.

One of my panel members believes this would not be a good thing to do, and may reintroduce “preference whispering” which Commonwealth reforms have recently sought to prevent.

In any event, it is clear that work needs to be done on the design of virtual ballot papers and the law needs to be framed to allow more lateral solutions.

## How-to-vote material

How-to-vote material is sent to people who register for postal votes. Should it also be sent to people who register for internet voting? Should it be sent by mail or by email? Should how-to-vote material be accessible directly from the iVote system?

Some of the potential voters were not happy with the idea of having their email inbox filled up with electoral material. Still, provided there are clear protocols around the quantity and frequency of material, it seems to me that how-to-vote material should be provided.

Since all this material has to be registered with the NSWEC, there may be some way in which the NSWEC can forward relevant material to voters once it is registered. Although, parties explained to me, that sometimes material is amended up until "the last minute".

Parties can facilitate the registration of voters for postal votes. This obviously enables the party to provide electoral material to the voter. There seems to me no reason why parties should not be able to facilitate voters to register for iVote. In fact that would give political parties the incentive to ensure that voters had a better understanding of iVote and how to use it safely, that is, securely.

One of my panel members believes that the role of political parties in facilitating the registration of voters to use iVote is a controversial issues that requires careful deliberation and discussion. It is certainly something that could be abused with remote voting – whether iVote or postal voting – although there is no evidence that it has been abused with regard to the latter. If political parties are to have a role in facilitating registration there should be clear limits and protocols that safeguard the freedom of choice and secrecy of voting remotely.

# Appendix 1 International experiences with internet voting

In 2009 the Federal Constitutional Court of Germany (Bundesverfassungsgericht) held that the use of "voting machines" was unconstitutional.[1] These were electronic voting machines deployed in polling places, not an internet voting system. However I consider the principles discussed in the decision are relevant to the implementation of an internet voting system.

The Court found that the public nature of elections emerged from the German constitution, a principle that required it to be possible for the public to examine all the essential steps in the electoral process, and in the reliable ascertainment of the results, without special expert knowledge unless other constitutional interests justified an exception. The Court stated:

> The major scope of the effect of possible errors in the voting machines or targeted election falsifications requires special precautions to be taken in order to comply with the principle of the public nature of elections.[2]

The Court did not rule out the use of voting machines:

> The legislature is not prevented from using electronic voting machines in the elections if the constitutionally required possibility of a reliable correctness check is ensured … Whether there are still other technical possibilities which create trust on the part of the electorate in the correctness of the proceedings in ascertaining the election result based on verifiability, and which hence comply with the principle of the public nature of elections, need not be decided here.[3]

Internet voting has been introduced in twenty countries, particularly for equivalent levels of Australia's state and local governments. The introduction of internet voting has often been characterised as a trial, and has often been for specific purposes such

[1] BVerfG, Judgment of the Second Senate of 03 March 2009 - 2 BvC 3/07, www.bverfg.de/e/cs20090303_2bvc000307en.html

[2] Ibid [120].

[3] Ibid [123], [124].

as military personnel – Australia has also trialled such a system - or for other citizens based abroad. Internet voting has also been introduced as a measure to increase voter participation or "turnout" in countries where voting is not compulsory. In Australia, NSW's iVote system has also been used at the 2017 state election in Western Australia for people who could not vote without assistance because they are insufficiently literate, are blind or have low vision, or are otherwise incapacitated.[4]

In the United Kingdom, several local authorities conducted internet voting trials in 2003 and 2007. Following the latter, the UK Electoral Commission reported that there was an unnecessarily high level of risk and that insufficient testing, security and quality assurance had been adopted. It also reported that there was a general lack of transparency around the internet voting system implemented.[5] Similar criticisms were levelled at postal only voting. It should be noted that electoral management in the UK is based on a model of "precinct" voting, where voters have a fixed polling place at which they can vote. Electoral authorities appear resistant to any move away from this system of management.

Norway discontinued internet voting in 2014, following trials at local elections in 2011 and general elections in 2013.[6] The trials were popular, with the internet voting system used for 26 per cent of the total votes cast in 2011, and between 33 per cent and 37 per cent in 2013. The trials were also considered to have had a high level of trust, with recorded-as-cast verifiability available on both occasions. In addition to the lack of political consensus (the government that introduced the trials was defeated at the 2013 election by a coalition of parties that was returned at the 2017 elections), factors in the decision to end the trials included that voter participation did not increase, and concerns for voter confidence should a security incident occur.

France determined that internet voting would not be permitted for its parliamentary elections in 2017,[7] having provided such a service for its citizens abroad since 2012. The government announced the advice of its information security agency ANSSI (Agence nationale de la sécurité des systèmes d'information) was that the risk of

[4] *Electoral Act 1907* (WA), s 99C.

[5] Electoral Commission, *Summary: Electronic Voting May 2007 electoral pilot schemes* (August 2007) <https://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0008/13220/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf>

[6] Organization for Security and Co-operation in Europe, *Norway, Parliamentary Elections, 9 September 2013: Final Report* (January 2014) <https://www.osce.org/odihr/elections/109517>; Government of Norway, *Internet voting pilot to be discontinued* (Press Release May 2014) <https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/>; Government of Norway, *Expert Study Mission Report The Carter Center Internet Voting Pilot: Norway's 2013 Parliamentary Elections* (March 2014) <https://www.regjeringen.no/globalassets/upload/krd/kampanjer/valgportal/valgobservatorer/2013/rapport_cartersenteret2013.pdf>

[7] Government of France, French Abroad - Voting Procedures in Legislative Elections (March 2017) <https://www.diplomatie.gouv.fr/fr/services-aux-citoyens/actualites/article/francais-de-l-etranger-modalites-de-vote-aux-elections-legislatives-06-03-17>

cyber attack was extremely high, hence the government considered it preferable to take no risk at all.

Finland conducted a feasibility study into internet voting in 2017.[8] It was their view that the benefits of the technology were not yet greater than its risks. The report identified the most significant risk to be voter confidence, concluding that confidence in internet voting could be harmed by false information and rumour as much as technical failure, and that electoral managers were yet to possess the means of having “concrete” evidence that an election result was indisputable and that no manipulation had taken place.

Switzerland has trialled internet voting for referendums and parliamentary elections at various levels of government since 2004. In 2017, its Federal Council determined the next steps for the broad introduction of internet voting, including public disclosure of the source code and progressing from trials to regular operation. At the same time, the Conference of Cantonal Chancellors adopted a memorandum of understanding concerning strategic objectives for the implementation of internet voting. Objectives to be achieved by the end of 2019 include implementation of general security requirements and the certification of systems, fostering confidence in electronic voting, an assessment of trials conducted between 2012 and 2017 trial period to evaluate implementation of the new security requirements, and that cantonal internet voting projects will be reviewed on an annual basis, including arrangements for federal financing of the projects.

Estonia introduced internet voting for local elections in 2005. “I-voting” has been conducted eight times in total, including subsequent local elections in 2009 and 2013, parliamentary elections in 2007, 2011 and 2015, and European Parliament elections in 2009 and 2014.[9] All voters are permitted to use the system, and its use is relatively high:

| | **2013 local elections** | **2014 European Parliament elections** | **2015 parliamentary elections** |
|---|---|---|---|
| Eligible voters | 1,086,935 | 902,873 | 899,793 |
| Voters turned out | 630,050 | 329,766 | 577,910 |
| I-votes counted | 133,662 | 103,105 | 176,329 |

Internet voting is only permitted from the tenth day prior to election day until the fourth day prior. Voters are permitted to cast their vote again using the internet

[8] Government of Finland, *Working group: Risks of online voting outweigh its benefits* (Press Release December 2017) <http://oikeusministerio.fi/en/article/-/asset_publisher/tyoryhma-nettiaanestyksen-riskit-suuremmat-kuin-hyodyt>

[9] Estonian National Electoral Committee, *Internet Voting in Estonia* <http://www.vvk.ee/voting-methods-in-estonia/>

voting system or at a polling place. Once internet voting closes, records are prepared for use in polling places to indicate whether a voter has used internet voting, and if it is determined that a voter has voted twice the electoral manager cancels the internet vote. When using the internet voting system, voters are required to identify themselves either by using an “ID card”, requiring a “smart card” reader to be connected to the computer from which they are voting, or by an “out-of-band” identification check using a mobile device that has a SIM card with a security certificate and two PIN codes.

The source code of the Estonian internet voting software has been made public since 2013.

## Observations about international experience

International experience is not conclusive or definitive. There is evident caution and circumspection about electronic voting and about internet voting specifically. In these examples there is little evidence of intrusion into the voting system; and no evidence I am aware of that an intrusion has changed the outcome of an election.

On the other hand, it is the perception and belief of the voting public that is the significant factor here. If people believe that their system of voting is subject to manipulation, or the threat of manipulation, that is almost as important as whether or not it is fact open to manipulation. If people have that belief they will cease to trust the system and cease having confidence in the results.

This psychological factor is more important where voting is voluntary because it influences the decision whether or not to vote. But it could also be important even where voting is mandatory in “colouring” the way people perceive the legitimacy of electoral outcomes.

Security is critical. Much of this report deals with what that means and how it should be put in place and maintained.

But equally critical is that people understand how the system works and how to use it safely and securely. Hence my insistence on E2E verification, transparency and openness, and the importance of a strategic communications program that goes beyond simply giving people the usual information. The decision of the German court referred to above makes the point very clearly.

It is probably also important to approach internet voting incrementally, as NSW has done. Its introduction was in a relatively small and confined way that targets those sectors of the community where there are clear benefits over and above the benefits of convenience – people with disabilities, voters in remote locations and people out of the jurisdiction on election day.

What is also evident from the local and international experience is this: irrespective of whether or not jurisdictions opt for remote internet voting, most electoral systems are effectively “hostage” to IT systems. Modern electoral systems hold data in electronic form; carry out enrolment and registration in electronic form; carry out vote counting in electronic form. The US experience shows that those functions are also vulnerable.

## The 2016 American election

The assessment of the American intelligence community is that Russia conducted a multifaceted campaign to influence the 2016 US presidential election, including covert espionage activities and overt public messaging.[10] This campaign comprised three elements.

Firstly state actors allegedly conducted "cyber operations" against targets associated with the major political parties, and other organisations of influence in relation to policy. Cyber operations in this context are also often referred to as "hacking", and involve unauthorised access to an information system or network through exploitation of weaknesses in security, typically cyber security. The well-known example is the intrusion into the electronic systems of the Democratic National Committee, and subsequent unauthorised public disclosure of emails from that system.

Secondly, state actors allegedly also conducted cyber operations against numerous state and local electoral management organisations. This reportedly involved emails masquerading as if from an election-related service provider being sent to officials of the electoral management organisations. Such conduct, known as "spear-phishing", attempts to have recipients inadvertently access a website or open a file that executes malicious code. It is not known how effective this campaign was, or what its objectives were. The assessment of the US Department of Homeland Security (**DHS**) in January 2017 was that systems used for vote tallying were not targeted or compromised. In September 2017, the DHS reportedly contacted election officials in 21 states to notify them that they had been targeted. What is known to have been compromised are voter databases, containing names, dates of birth, genders, driver's license numbers, and partial Social Security numbers. Reportedly there is evidence that attempts were made to delete or alter that voter data.

Thirdly, state actors engaged in propaganda in support of particular candidates and negatively against another. An influence campaign centred on large scale, highly organised social media activities allegedly involved:

- Procurement of domestic computer infrastructure in order to mask the international origin and control of the activities.
- Creation of false personas for social media accounts.
- Production and distribution of political advertising.
- Use of stolen identities to conduct transactions such as payments for political advertising.
- Organisation of political rallies.

[10] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D (January 2017).

Investigation of these events continue, with prosecutions pending in some instances. More broadly these events demonstrate the continued use of propaganda to influence public opinion, and relevant to this report, that propaganda may not be distinguished by the media or the public generally from issues of “hacking” and cyber security.

# Appendix 2 Abbreviations, list of submissions, bibliography

## Abbreviations

| | |
|---|---|
| **AEC** | Australian Electoral Commission. |
| **BLV** | Blind or low vision. |
| **COAG** | Council of Australian Governments. |
| **Commissioner** | The NSW Electoral Commissioner. |
| **DHS** | US Department of Homeland Security. |
| **DVS** | The Commonwealth's Document Verification Service. |
| **E2E verification** | End-to-end verification. |
| **ECANZ** | Electoral Council of Australia and New Zealand. |
| **Electoral Act** | *Electoral Act 2017* (NSW). |
| **IP** | Intellectual property. |
| **IT** | Information technology, but it is used generically herein to embrace concepts including information and communications technology, information systems, information management, etc. |
| **JSCEM** | The NSW Parliament's Joint Standing Committee on Electoral Matters. |
| **NSWEC** | The staff agency led by the Electoral Commissioner generally known as the NSW Electoral Commission that enables the three person Electoral Commission and the Electoral Commissioner to exercise their functions. |
| **PE&E Act** | *Parliamentary Electorates and Elections Act 1912* (NSW). |
| **PSPF** | The Australian Government's Protective Security Policy Framework. |
| **PwC** | PwC Australia. |

| | |
|---|---|
| **SGE** | State general election. |
| **US** | United States of America. |

## List of submissions

1. Dr Vanessa Teague, Dr Chris Culnane, Dr Aleksander Essex, Prof Rajeev Goré and Prof J. Alex Halderman
2. Mr Mark Eldridge
3. Physical Disability Council of New South Wales
4. Smartmatic Australia
5. Mr Ian Brightwell
6. Mercury Information Security Services
7. Australian Election Company
8. Scytl Australia
9. Mr Ralph McKay
10. Dr Roland Wen and Prof Richard Buckland

## Bibliography

Australian Signals Directorate, *Australian Government Information Security Manual: Controls* (2017).

Australian Signals Directorate, *Australian Government Information Security Manual: Principles* (2016).

Dr Richard Adams, ‘IT External Audit Report: Final Report for the iVote system as implemented by the Western Australian Electoral Commission for the March 2017 State Election’ (June 2017).

Bundesverfassungsgericht, Judgment of the Second Senate of 03 March 2009 - 2 BvC 3/07.

*Commonwealth Electoral Act 1918* (Cth).

*Electoral Act 2017* (NSW).

*Electoral Act 1907* (WA).

Electoral Commission (United Kingdom), *Summary: Electronic Voting May 2007 electoral pilot schemes* (August 2007).

Electoral Council of Australia and New Zealand, *Eleven essential principles for an Australian internet voting service* (November 2017).

Electoral Matters Committee, Parliament of Victoria, *Inquiry into electronic voting* (May 2017).

Feng Hao and Peter Y A Ryan (Eds.), *Real-World Electronic Voting: Design, Analysis and Deployment* (December 2016).

The Greens, Submission No 8 to Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into the Administration of the 2015 NSW State Election and related matters* (August 2015).

The Greens (WA), Submission 10 to Community Development and Justice Standing Committee, Parliament of Western Australia, *Inquiry into the Administration and Management of the 2017 State General Election* (August 2017).

Ipsos Social Research Institute, *New South Wales State General Election Research: Prepared for the NSW Electoral Commission* (June 2015).

International Organization for Standardization, *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirement*s (October 2013).

Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Administration of the 2015 NSW State Election and related matters*, Report 2/56 (November 2016).

Liberal Party of Australia (NSW Division), Submission No 22 to Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into the Administration of the 2015 NSW State Election and related matters* (September 2015).

Organization for Security and Co-operation in Europe, *Norway, Parliamentary Elections, 9 September 2013: Final Report* (January 2014).

Robert Krimmer, Melanie Volkamer, Jordi Barrat, Josh Benaloh, Nicole Goodman, Peter Y.A. Ryan and Vanessa Teague (Eds.), *Electronic Voting: First International Joint Conference, E-Vote-ID 2016* (October 2016).

Robert Krimmer, Melanie Volkamer, Nadja Braun Binder, Ardita Driza Maurer, David Duenas-Cid, Norbert Kersting, Oksana Kulyk, Leontine Loeber, Olivier Pereira, Peter Roenne, Carsten Schurmann, Priit Vinkel (Eds.), *E-Vote-ID 2017 Second International Joint Conference on Electronic Voting,* (October 2017).

Government of Norway, *Expert Study Mission Report The Carter Center Internet Voting Pilot: Norway's 2013 Parliamentary Elections* (March 2014).

NSW Auditor-General, *Report to Parliament: Detecting and responding to cyber security incident* (March 2018).

NSW Labor, Submission No 11 to Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into the Administration of the 2015 NSW State Election and related matters* (August 2015).

NSW Nationals, Submission No 16 to Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into the Administration of the 2015 NSW State Election and related matters* (August 2015).

Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D (January 2017).

*Parliamentary Electorates and Elections Act 1912* (NSW).

Sir Eric Pickles, *Securing the ballot: Report of Sir Eric Pickles' review into electoral fraud* (August 2016).

Rodney Smith, 'Internet Voting and Voter Interference: A report prepared for the New South Wales Electoral Commission (March 2013).

Rodney Smith, 'Multiple Voting and Voter Identification: A research report prepared for the New South Wales Electoral Commission' (February 2014).

Shooters and Fisheries Party, Submission No 17 to Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into the Administration of the 2015 NSW State Election and related matters* (August 2015).

Dr Vanessa Teague and Prof Rajeev Goré, Submission No 2 to Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into the Administration of the 2015 NSW State Election and related matters* (July 2015).

Vision Australia, Submission No 60 to Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Inquiry into the 2012 Local Government Elections* (February 2013).

# Appendix 3 ECANZ *'Eleven essential principles for an Australian internet voting service'*

Electoral Council of Australia & New Zealand

# Eleven essential principles for an Australian internet voting service

The following eleven essential principles for an internet voting service were endorsed by the Electoral Council of Australia and New Zealand (ECANZ) on 4 July 2017.

These principles are reflective of existing best electoral practices as they apply to current voting channels.

In developing these principles, the ECANZ examined the United States Election Assistance Commission's 'Voluntary Voting System Guidelines (VVSG 2.0)', and the Council of Europe's intergovernmental standards for e-voting (CM/Rec (2017)5) - drawing on these standards and principles to develop eleven essential principles to guide the design and implementation of an internet voting service in Australia for use by all member Electoral Commissions.

## Enfranchisement

### Accessibility

**– as far as is practical, all eligible people should be able to access the internet voting service**

The internet voting service shall be designed, as far as practicable, to enable eligible voters to vote independently regardless of disabilities, technology or geography. The internet voting service will be an additional and optional service for specific eligible voters to use. It would be offered in conjunction with other pre-existing methods of voting.

### Usability

**– the process of internet voting should be sufficiently easy for eligible people to cast a vote**

The user interface of the internet voting service should be easy to understand, intuitive, and able to be used by all eligible voters on multiple technology platforms. Information provided may be presented differently depending on the differing technologies and channels which the service can be accessed on. For example, the electoral content presented on an electronic ballot paper will be the same as on the physical paper ballot paper (ensuring impartiality and equitably); however changes may be made in accordance with relevant legislative provisions while ensuring usability on each technology platform.

### One person, one vote

**– the ability to ensure that each eligible elector receives only their voting entitlement**

The internet voting service should enable each eligible voter to be uniquely identified, ensuring that they are distinguishable from other voters. The service should cater for any legislative requirements around the presentation of identification documents. An eligible voter will only be able to use this channel if they can be uniquely identified this way. The service will check eligibility and only grant access to those that have been authenticated as an eligible voter. The service will have a process to ensure that only one vote per eligible voter is admitted to the count.

## Integrity

### Security

**– prevention of loss, corruption or tampering of votes**

The internet voting service and responsible Electoral Management Body shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data. The authenticity, availability and integrity of the electoral roll and lists of candidates shall be maintained. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the electoral event data.

The audit system should be able to detect voter fraud and provide proof that all counted votes are authentic. The audit system shall be open and comprehensive, and actively report on potential issues and threats. Where incidents that could threaten the integrity of the service occur, those responsible for operating the equipment shall immediately inform the electoral management body. Procedures shall be established to ensure regular installation of updated versions and corrections of all relevant software as the service will need to be continually evolved to meet and protect against potential and actual issues and threats.

The service will encrypt votes if they are to be stored or communicated outside controlled environments. The electoral management body shall handle all cryptographic material securely. Votes shall be kept sealed[1] until after the close of polling.

### Robustness

**– the system and processes are not subject to significant interruption or failure**

Robustness applies to people, process and technology. The internet voting service must be available, reliable and secure to ensure that it can function on its own, irrespective of shortcomings in the hardware or software. The technical solution for the service will be peer-reviewed to help ensure availability, reliability, usability and security. The service shall identify votes that are affected by an irregularity so that

[1] Sealed is an analogy to the seal on a physical ballot box. This is the term used in the European standards

necessary measures are taken and stakeholders are informed. The electoral management body administering the service will ultimately be responsible for compliance with the above even in the case of failure.

## Transparency

**– the service and processes be designed to enable scrutiny, to provide stakeholder confidence**

The internet voting service and accompanying processes will be established with a focus on transparency. The service will ensure that the way in which eligible voters are guided through the internet voting process shall not lead them to vote without due diligence or without confirmation. The service should be designed to allow the voter to express his or her true will. A voter will be allowed sufficient time to consider their choices and will be under no obligation to commit their vote without time for reflection on their choices. Upon casting their vote, the service will verify to the voter that his or her intention is accurately represented and that the vote has been submitted. Any alteration to the voter's vote should be detected by the service.

Voters and third parties should be able to observe the count of the votes and check that only eligible voters' votes are included in the results. The service will provide evidence that only eligible voters' votes have been included and this evidence will be auditable.

Clear and unambiguous information about the internet voting service should be available to the public explaining how to use the service and how the service operates.

The service should be open for verification, assurance and scrutiny purposes. Observers, to the extent permitted by law, shall be enabled to observe, comment on and scrutinise the internet voting component of an election, including the compilation of the results.

## Independence

**– accountability for the system and processes shall rest with the Electoral Management Body**

The electoral management body will be accountable for the internet voting service of an electoral event. The electoral management body must be able to put into place assurances that maintain their electoral integrity and independence.

## Impartiality

**– the voters intention should not be affected by the voting service**

An eligible voter's intent should not be affected by the internet voting service. The service will ensure that the way in which voters are guided through the process and the information displayed will not influence their vote.

The service should be structured to ensure that voter's do not miss anything during the voting process. It should provide a means for informal voting by allowing a blank vote to be cast, however advising the voter they would be casting an informal vote and providing them with the option to change their vote if they wish. This provides an equitable approach across channels enabling voters to cast an informal vote via both the service and the paper-based option. Other than a blank ballot paper, all formality rules will be enforced by the service.

### Accuracy

**– the service should accurately capture, store and export the voters intention**

The internet voting service shall provide sound evidence that only votes from eligible voters are included in the final result while de-identifying a completed ballot paper from its voter. The service shall support the voter in marking the ballot paper and accurately store, capture, verify, and export the vote cast. Before an event, the electoral management body administering the service shall satisfy itself that the service is genuine and operates correctly.

The service shall allow and support evaluation regarding the compliance of the service and its related components. This should occur upon introduction, periodically and after significant change to the service has been made.

## Privacy

### Privacy of personal information

**- the system and processes shall maintain the privacy of personal information**

The internet voting service shall process and store, as long as necessary, only the personal data needed for the conduct of the electoral event. The electoral management body administering the service will determine what information is deemed necessary to keep and dispose in accordance with relevant legislative obligations.  Any information retained will be secure and any information not required to be retained will be securely disposed of.

### Secrecy of vote cast

**– the service shall maintain the secrecy of the votes cast**

The internet voting service shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting process – from pre-polling through to counting of the votes. Votes shall remain sealed until the counting process commences. During completion of the ballot paper, the service will protect the secrecy of the voter's choice. The service should not provide a proof of vote preferences that would facilitate coercion or vote buying.

The service will be able to de-identify a voter from their completed ballot paper to preserve the secrecy of the ballot. The order in which votes are cast shall be mixed so as to deny reconstruction of the order of votes submitted.

# Appendix 4 PwC Risk Assessment

www.pwc.com.au

# *NSW Electoral Commission*

## iVote Voting System – Risk Assessment

## Final Report

*NSW Electoral Commission*

*iVote – Risk Assessment*

*February 2018*

pwc

# Contents

1 Executive Summary 4

1.1 Background 4
1.2 Engagement Objective and Scope 5
1.3 Context for this review 6
1.4 NSWEC Risk Appetite 8
1.5 Summary of Findings 9

2 Detailed Risk Mapping and Analysis 14

2.1 System Risk Assessment Framework 14
2.2 iVote Risk Assessment 15

Appendix A - Engagement Approach 41
Limitations and Constraints 41
Appendix B - Stakeholders Consulted 42
Appendix C – Supporting Documentation 45

*PricewaterhouseCoopers prepared this report solely for the use and benefit of NSW Electoral Commission (**NSWEC**) in accordance with and for the purpose set out in our engagement letter with NSWEC dated [10 November 2017] [and section [1.2] of the report]. In doing so, we acted exclusively for NSWEC and considered no-one else's interests.*

*Our engagement did not constitute an audit in accordance with Australian Auditing Standards or a review in accordance with Australian Auditing Standards applicable to review engagements and accordingly no such assurance is provided in this report.*

*We accept no responsibility, duty or liability:*

- *to anyone other than NSWEC in connection with this report*
- *to NSWEC for the consequences of using or relying on it for a purpose other than that referred to above.*

*We make no representation concerning the appropriateness of this report for anyone other than NSWEC. If anyone other than NSWEC chooses to use or rely on it they do so at their own risk.*

*This disclaimer applies:*

- *to the maximum extent permitted by law and, without limitation, to liability arising in negligence or under statute; and*
- *even if we consent to anyone other than NSWEC receiving or using this report.*

# 1 Executive Summary

## 1.1 Background

The iVote Voting System ('iVote' or 'the system') is the New South Wales Electoral Commission's (NSWEC) system for remote electronic voting. The system was initially introduced in 2011 to satisfy the needs of the Blind and Low-Vision (BLV) community. Subsequent to this, the system was again used in the New South Wales State General Election (SGE) in March 2015. It has also been used on nine occasions for NSW State by-elections, and at the March 2017 Western Australian SGE.

iVote allows eligible voters[1] to cast their votes by telephone or by computer with internet access. Under the legislation currently in force[2], eligible users of iVote are voters enrolled in NSW for whom:

a) Vision is so impaired, or the elector is otherwise so physically incapacitated or so illiterate, that he or she is unable to vote without assistance;
b) Disability (within the meaning of the Anti-Discrimination Act 1977 (NSW)) causes them to have difficulty in voting at a polling place or they are unable to vote without assistance;
c) Their real place of living is not within 20 kilometres, by the nearest practicable route, of a polling place; or
d) Will not throughout the hours of polling on polling day be within New South Wales.

While under current legislation iVote will only be in use for NSW State by-elections and for the 2019 NSW SGE, there is the potential that the NSW Parliament may expand the coverage and scope of iVote and it is also possible that, in future, iVote may be used to take absent votes at all pre-polls and selected high volume polling places.

The NSWEC recognises that the operation of iVote carries inherent risks and has, during the systems existence, sought to mitigate those risks. To support ongoing enhancement to iVote, and in time for the 2019 SGE, the NSWEC will undertake an approach (via a Request for Proposal (RFP)) to market with the aim of delivering an enhanced version (or 'Voting System Refresh Project') of iVote. It is anticipated that the outcomes of the new system will address key elements related to:

[1] The recently passed Electoral Bill 2017 is expected to be in force for the 2019 SGE and would mean the eligibility criteria will change and be available for a broader range of eligible electors.
[2] *Parliamentary Electorates and Elections Act 1912* (NSW). Amended in 2010 to enable 'Technology Assisted Voting'.

1. Enhanced system security, voting protocol integrity and updated cyber-security;
2. Increased transparency, auditability and scrutiny;
3. Enhanced functionality and user experience;
4. Enhanced public awareness of iVote with targeted promotion to community and disability groups; and
5. Reduced operational complexity.

In response to a recommendation from the NSW Parliament's Joint Standing Committee on Electoral Matters, the NSWEC has engaged Mr. Roger Wilkins AO to undertake an inquiry into, and author a report concerning iVote. The terms of reference for this inquiry are:

1. Whether the security of iVote is appropriate and sufficient;
2. Whether the transparency and provisions for auditing iVote are appropriate;
3. Whether adequate opportunity for scrutineering of iVote is provided to candidates and political parties; and
4. What improvements to iVote would be appropriate before its use at the 2019 SGE.

## 1.2 *Engagement Objective and Scope*

The objective of this engagement was for PwC to provide support to the inquiry undertaken by Mr Wilkins through the development of this report providing identification, at a high level, of the relevant risks and areas of vulnerability related to the use of iVote including, but not limited to, cybersecurity.

This assessment took into consideration previous risks identified which related to the use of iVote and electronic voting more generally, and examined whether the NSWEC have sufficiently addressed these risks, or are considering the mitigation of these risks through the Voting System Refresh Project. Figure 1 below provides an overview of the scope of this engagement:

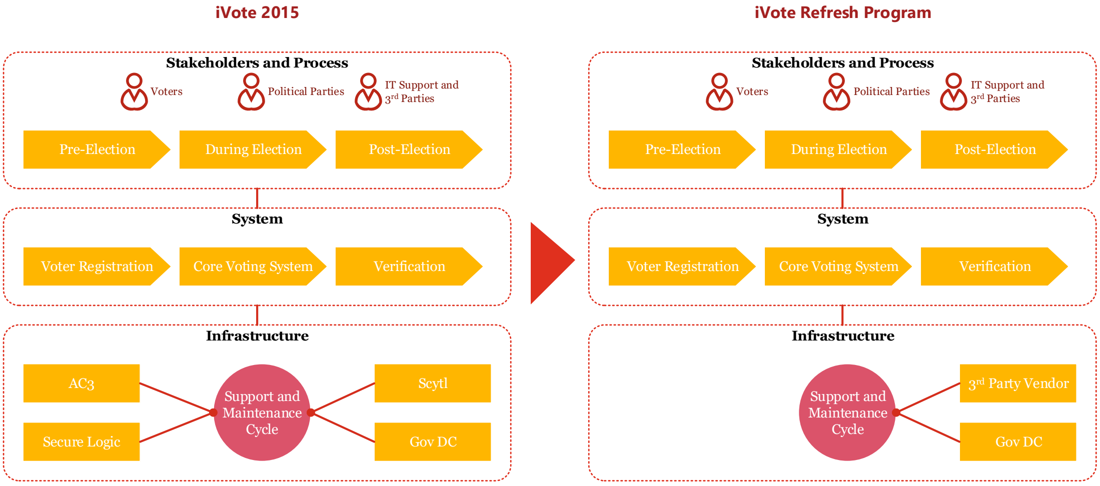


*Figure 1 – Risk assessment scope*

Other areas considered in this risk assessment include:

- Governance frameworks, decision making and service provider/vendor contractual relationships;
- System and process documentation, including deficiencies which may exist in that documentation;
- System infrastructure and configuration, including third party infrastructure; and
- Personnel risks, such as behavioural issues and vulnerabilities of both voters using the system and relevant staff responsible for administering the system and associated processes (both at the NSWEC and by third parties).

The identification of these risks will provide insights into the areas that may require further attention and inform potential remediation activities.

Full details on the PwC approach to address the engagement objective and scope is contained in Appendix A.

## 1.3 *Context for this review*

In addressing the engagement objective and scope, PwC first sought to understand and establish the context in which risks to the system should be identified and assessed. The following points reflect our research based on information provided by engagement stakeholders:

*Table 1. Contextual observations*

| Area | Observations |
|---|---|
| **Australian electoral system and processes** | • Level of trust by the voting public in the Australian electoral process, Australian electoral institutions, and their associated systems or processes is high.<br>• The Australian electoral system has a requirement for mandatory enrolment and voting.<br>• All forms of remote voting come with the risk of some form of voter interference, e.g. coercion, however, overall level of voter interference in Australia is considered low.<br>• Other methods of voting (e.g. postal voting) also have inherent risks with respect to voter interference. |
| **Broader regulatory support** | • It is noted that while legislation drives eligibility criteria for voters to use iVote, without an adequate policy basis or provision of resources to enforce eligibility, there is avenue for usage of iVote by voters who do not meet the legislative criteria. |
| **Electronic voting and iVote participation** | • Trust and integrity in the system is essential as a failure in an election event could cause suspension of, or the need to re-run, that election.<br>• iVote is part of a suite of voting channels used at elections.<br>• iVote captured 46,864 electors in 2011 and 283,699 (6.22% of votes) at the 2015 SGE.<br>• Overall increase in votes cast via iVote equals 505% increase[3] between 2011 and 2015 SGEs.[4]<br>• The level of adoption of electronic voting elsewhere globally is already larger than Australia i.e. Canada, Estonia, Norway, etc. |
| **Previous iVote reviews and risks identified** | • After each NSW SGE a review is undertaken into the conduct of the election process by the Joint Standing Committee on Electoral Matter [5] (JSCEM).<br>• A number of previous reviews and reports reflecting the performance of iVote after each election event have been performed. The undertaking of these reviews reflect a culture of ongoing improvement and lessons learned. The focus of these previous reviews has been on areas of risk such as:<br>○ Voter impersonation |

[3] NSW Electoral Commission Report on the Conduct of the 2015 State General Election, p.17.
[4] May increase as postal voting may be problematic in 5 to 10 years.
[5] A selected cross party committee.

| Area | Observations |
|---|---|
| | ○ Incorrect casting of votes<br>○ Incorrect counting of votes<br>○ Technology and cyber security<br>○ Lack of accessibility of audit mechanisms for political stakeholders<br>○ External influence over process and system integrity |
| **Emerging threat landscape** | • Any expansion of voter eligibility will come with expanded awareness of the system. This in turn may lead to a 'tipping point' in which there will be a potential increase in the exploration by outside parties as to whether there are flaws/issues in the system. As a result of this increased profile, iVote may be exposed to higher numbers of attempted attacks and manipulation. This may include:<br>○ An increase in profile also increases the potential for an increase in malicious activity (e.g. Denial of Service (DoS) attacks, wherein malicious external parties will look to overload servers with massive waves of phony traffic).<br>○ Increase in external parties looking to make and spread false claims related to secure use of electronic voting.<br>• Marketplaces for voter registration data have sprouted on the Dark Web over the last year.<br>• Evidence of Nation State and other malicious actors involvement in electronic voting events internationally. |

## 1.4 *NSWEC Risk Appetite*

The NSW Electoral Commission's (NSWEC) risk appetite statement[6] outlines the amount of risk it is prepared to accept to achieve its strategic and operational objectives (including election, funding and regulation activities). The NSWEC faces a range of risks in its role as the pre-eminent provider of electoral events, services and regulation in New South Wales.

Overall, the NSWEC has a **low** risk appetite. This means that it looks to avoid risks and uncertainty and has a preference for options that have a low degree of inherent risk. However, the NSWEC accepts there is a certain level of inherent risk in its activities and acknowledges that accepting a certain level of risk helps it develop, innovate and better serve

[6] NSWEC Risk Appetite Statement n.d.

its stakeholders and clients. iVote is an example of the NSWEC's approach to innovation in service delivery.

The NSWEC takes a deliberate and measured approach to change to ensure that all risks are properly identified and appropriate mitigation strategies and governance processes are established so as not to compromise the delivery of its core services and activities.

Across certain risk areas, the NSWEC has communicated to PwC its degree of risk appetite or specific tolerance levels related to iVote. These relative tolerances outline how management views the potential impact upon the successful undertaking of election events utilising iVote. These tolerances are reviewed on an ongoing basis relative to environmental scanning and post-election event assessments. In undertaking the iVote risk assessment, PwC has incorporated the stated tolerance to certain risks to inform an understanding of treatment approaches and therefore, the residual risk for the NSWEC.

## 1.5 *Summary of Findings*

In undertaking this risk assessment, it appears that iVote performs the necessary election event functionality as required.  As stated previously, all channels to enable remote voting come with inherent risk, for example, the loss, damage or otherwise tampering of paper ballots. It is clear that no system of remote voting is failsafe and iVote is no different in that regard.

The risk profile of iVote is limited by the extent to which it is promoted as a voting channel. To date, there have been limited categories of eligible voters legally allowed to use iVote, allowing the system to benefit from **'security through obscurity'**, and therefore, the level of risk management of iVote at present is appropriate based on current scale and scope of its use.

iVote as a voting channel has not yet reached the 'tipping point' of visibility that makes it a desirable target for malicious actors. However, in a scenario of increased usage of iVote as a voting channel, the risk profile will consequently increase, necessitating a correspondent increase in risk treatment activities. Therefore, the opportunity to elevate a holistic protective security framework to the iVote environment is worth considering to further support and enable the objectives of the Voting System Refresh Project.

In undertaking our risk assessment, PwC looked to identify and assess potential risks associated with iVote within nine relevant Risk Categories (refer to s2.2 for more detail):

1. Solution Governance
2. Solution Design and Documentation
3. Process Design and Management
4. Data Governance
5. Information Security
6. Personnel Security
7. Physical Security
8. Network and Infrastructure
9. Outsourced Technology Services

This risk analysis took into consideration not only the likelihood and consequence of these potential risks, but also whether or not treatments and mitigations currently exist (or were to be factored in, as part of solution incorporating the Voting System Refresh Project), as well as the NSWEC level of tolerance to these risks.

PwC acknowledges that the RFP for the Voting System Refresh Project incorporates requirements related to the Electoral Council of Australia and New Zealand (ECANZ) *Endorsed 11 essential principles for an internet voting service*[7]. These principles are reflective of existing best electoral practices and based on three major aspects: Enfranchisement of voters, Integrity of the voting process and Privacy of the voters. PwC has taken into consideration the future adoption of process/system functionality aligned to these principles in undertaking our assessment.

PwC's analysis against the potential risks outlined in section 2.2 of this Report has identified some categories/areas which demonstrated a lack of appropriate controls or treatments expected. A number of these risks maintain a residual risk rating of 'High' and are listed below. For ease of action/accountability within NSWEC, these have been outlined below against the key themes of system, process and people related risks:

**System Risks -** iVote will continue to experience risk related to the design of functionality and the interaction of the system with eligible voters. Maintaining voter trust and public confidence will be put in question if NSWEC does not put in place an appropriate controls framework to provide comfort over the integrity of the system and the data held.

- **System Accreditation (Risk ID #11[8])** – iVote is not subjected to a formalised system accreditation process (i.e. Information Security Registered Assessors Program or 'IRAP') which may lead to unknown or unmitigated security risks

[7] As agreed in 2017.

[8] Risk ID# as per the risk table in s2.2.

remaining undetected. However, underlying service providers are ISO270001 certified.

- **Software Development Life-Cycle (Risk ID #12)** – There are no formal NSWEC guiding principles related to the Software Development Life-cycle (SDLC). Ineffective controls applied throughout the SDLC may adversely impact the quality and reliability of delivered software.
- **Software Testing (Risk ID #15) –** In conjunction with the risk above, inconsistent/non-ongoing testing of software and infrastructure (provided either in-house or outsourced) could lead to the introduction of exploitable weakness or unacceptable software being delivered.
- **Vulnerability Testing (Risk ID #42)** – While vulnerability testing of iVote occurs in the lead up to election events, the lack of an ongoing and defined testing program can lead to undiscovered vulnerabilities that could be exploited and compromise system data and functionality.
- **Network Architecture (Risk ID #45)** – The design and implementation of network architecture for iVote needs to balance requirements for protection against denial-of-service attacks with a need to maintain voter anonymity and the secrecy of a votes as cast. There is no defined cybersecurity strategy and plan available to inform how these requirements are addressed.

**Process Risks** - The processes that support iVote also need to be examined on an ongoing basis. The capture of procedures and processes related to iVote are at varying levels of maturity, but for those process that exist, it is their consistent and enforced adherence which lacks evidence.

- **Voter Distrust (Risk ID #20) –** A low level of public engagement with voters, candidates, and political parties may introduce a perceived lack of transparency and/or controls, leading to mistrust in the iVote system and low adoption rates.
- **Scrutineering (Risk ID #21) -** Inadequate support of electoral scrutineering process in iVote leads to a lack of perceived or actual transparency. While scrutineering of iVote by political parties is supported in current process and practice, the engagement with candidates and political parties does not extend to facilitating their understanding of the process.
- **Legality of Election Results (Risk ID #24) –** Failure in iVote system security or availability may impact on the integrity of election results and lead to election irregularity and reputational damage to NSWEC. Current gaps in this area relate to minimal stakeholder engagement, especially for political parties and scrutineers to ensure against challenges against the election result.
- **Voter Cybersecurity Awareness (Risk ID #25) –** There is a lack of a continual and proactive approach to provide cybersecurity education and awareness related to

iVote for eligible voters. A lack of a program to clearly address voter concerns can contribute to voter uncertainty and influence of external parties, which in turn can lead to an increased level of voter disenfranchisement.

- **End to end Verification (Risk ID #27)** –End to end verification of votes is a key requirement to support external scrutiny of electronic voting. While functionality to provide logging and audit capability exists[9], there is limited evidence of clear planning to enable the education and awareness for political parties or other auditors on how to interpret these logs. This could lead to mistrust in the system and electronic voting process without the ability for individual or universal verification of 'votes as cast'.
- **Audibility (Risk ID #28) -** iVote currently supports logging of activities with cryptographic protections in place for logs as captured, though the end to end verification of votes is less supported and is dependent upon an understanding of the system and technical capability.
- **IT General Controls (Risk ID #35)** – There is limited evidence related to change management, system access controls and the recovery approach for iVote. The backup and recovery process requires most attention to ensure that the NSWEC understands its ability to restore iVote functionality in the event of a disruption.
- **Cyber Threat Monitoring and Incident Management (Risk ID #41)** – Internally to NSWEC, a cybersecurity strategy and plan were yet to be developed and were not available at the time of fieldwork. The lack of a coordinated threat monitoring and incident management process for iVote infrastructure (at system, network, and/or user interface levels) leads to the potential for the introduction of exploitable vulnerabilities.
- **Vendor/Contract Management (Risk ID #46)** – the oversight of the relevant service provider contracts and performance measures is undergoing an internal NSWEC transition. Previous management of these functions have not incorporated the appropriate level of rigour which has led to ineffective service levels, issue resolution and potential for introduced vulnerabilities through 3rd party channels.
- **Service and Performance Management (Risk ID #48) –** A lack of defined (e.g. ITIL) and ineffective existing service management processes can reduce the quality of service from external providers with potentially adverse impacts on performance and availability.
- **Vendor Software Delivery (Risk ID #49) –**Low maturity in management of vendor software delivery may lead to poor control over changes to iVote, resulting in potential for accidental or intentional breach of compliance requirements, system unavailability, reputational damage and mistrust in iVote.

[9] PwC notes that the iVote Voting System Refresh RFP clearly outlines solution requirements related to ‘logging’ to support auditing.

**People Risks** – PwC identified key personnel risk mainly due to the small numbers of dedicated iVote support staff. Behavioural elements associated with security culture, education and awareness as well as security culture should be examined.

- **Capacity and Capability (Risk ID #36)** – A lack of the necessary level of workforce planning has led to a shortage of the skills / capability required for iVote support. There are acknowledged challenges with the current level of skills and capacity of personnel who support iVote (refer Risk #38 below).
- **Trust and Reliability (Risk ID #37) -** NSWEC has established security vetting via the Australian Government Security Vetting Agency (AGSVA) though this has not been used in relation to iVote personnel. As a result personnel supporting iVote and related processes potentially do not have the appropriate security clearances and/or vetting in place.
- **Reliance on Key Personnel (Risk ID #38) –** iVote support is dependent on a small team within NSWEC. A lack of documented system knowledge and process information results in one or more single point(s) of failure in the current support capability.
- **Education and Awareness (Risk ID #39)** – While staff who support iVote are aware of their overarching responsibilities in relation to the electoral process and the handling of sensitive information, broader training and education is lacking related to regulatory frameworks such as the Australian Privacy Principles.

# 2 Detailed Risk Mapping and Analysis

## 2.1 System Risk Assessment Framework

The PwC Risk Assessment Framework is based on 2 key principles:

- It is to consider the 'whole of system' (people, process and technology); and
- Is to be evidence based

The approach undertaken by PwC for the identification and analysis of risks for iVote is in accordance with the steps contained within the ISO 31000:2009, *Risk management – Principles and guidelines*.

Using this framework, PwC leveraged other better practice guidelines to assist in identifying our 'risk coverage' incorporating; risk categories, potential risks and expected controls/treatments to inform our analysis. These guidelines included:

- Attorney-Generals' Department (AGD) Protective Security Policy Framework (PSPF);
- Australian Signals Directorate (ASD) Information Security Manual (ISM); and
- ISACA[10] COBIT5[11] Management Framework for Enterprise IT.

Following the initial development of our risk coverage, PwC engaged with identified stakeholders (refer to Appendix B - Stakeholders Consulted) and undertook a review of provided supporting artefacts as well as examined previous papers and reports related to previous election events use of iVote and electronic voting more broadly (both nationally and internationally).

The capture and analysis of these fieldwork activities enabled PwC to identify relevant risks, assess inherent level of risk, identify treatments in place (and their effectiveness) and assess the residual risk remaining.

[10] Previously referred to as the Information Systems Audit and Control Association.
[11] Control Objectives for Information and Related Technology.

## 2.2 *iVote Risk Assessment*

The result of PwC fieldwork is outlined in Table 4 below. This table reflects the agreed risk categories, areas and descriptions against which the risk assessment was undertaken. The rating scales represented for likelihood, consequence and inherent risk reflect the guidance outlined within the NSWEC Risk Management Framework.

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 determining the residual risk rating, PwC examined the Treatments (i.e. activities or mitigations in place to address the stated risk), their effectiveness and also took into consideration input from NSWEC related to risk tolerances for those risks.

Key terms in this table are defined below:

- **Risk Category** – Categories have been identified and defined in conjunction with NSWEC, with reference to better practice information security and risk frameworks (as outlined in s2.1).
- **ID** – each risk is assigned a unique identifier.
- **Area** – each risk is related to an area within the Risk Category.
- **Description of Potential Risk Event** – this is a descriptor of what the potential risk event is. This is not intended as statement on the current state of iVote or NSWEC, but represents a potential event that could impact on NSWECs objectives with respect to iVote.
- **Likelihood** – an assessment of the chance of the potential risk event occurring.
- **Consequence** – an assessment of the potential impact of the potential risk event on the NSWECs objectives with respect to iVote.
- **Inherent Risk Rating** – an assessment of the risk rating (Low, Moderate, High or Extreme) inherent in the environment and context of iVote, without taking into account risk treatments or other controls.
- **Treatments Identified** – details of risk treatments that have been identified during the course of this assessment that address the potential risk event, and either assist in reducing a likelihood or impact of a potential risk event.

- **Treatment Assessment** – an assessment of the treatment effectiveness (Effective, Partially Effective or Ineffective) in addressing the identified potential risk event.
- **Residual Risk Rating** – an assessment of the risk rating (Low, Moderate, High or Extreme) that remains in the environment, taking into account treatments identified, the assessment of their effectiveness and the stated tolerance of the NSWEC to that risk.

*Table 4. Risk Mapping and Assessment*

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| **1. Solution Governance** | 1 | Vision and Roadmap | Inadequate vision and strategy may not inform a coherent set of guiding principles to clearly articulate the future direction of the system. | Unlikely | Major | High | • Roadmap and strategic direction are documented as part of the Voting System Refresh Project.<br>• NSWEC- level governance is provided by the Voting System Refresh Project Steering Committee, with plans to transition operational support and management to BAU IT following completion of the Project.<br>• NSWEC is engaged in a national strategy for the development of a national internet voting platform (i.e., through involvement in the development of the ECANZ Essential 11 Principles for Electronic Voting, which have informed the Voting System Refresh Project RFP) | Effective | Medium |
| | 2 | Current Budget | Insufficient budget may not support current system | Moderate | Moderate | High | • Operational budget will be determined at the end of the Voting System Refresh Project | Partially Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | operation and maintenance. | | | | through transition to operational BAU IT support.<br>• Current budget for the support of iVote is project-based, supported from a small operational team in NSWEC. | | |
| | 3 | Future Investment Funding | Insufficient investment and future funding may not support expansion of system functionality in line with defined strategy. | Moderate | Moderate | High | • Scope and vision for iVote platform are documented as part of the Voting System Refresh Project.<br>• Operational budget will be determined at the end of the Voting System Refresh Project through transition to operational BAU IT support. Current budget for the support of iVote is project-based. | Partially Effective | Medium |
| | 4 | Voter Disenfranchisement | Weaknesses or failures in iVote may lead to disenfranchisement of eligible electors and subsequent distrust in technology assisted voting. | Unlikely | Major | High | • Voting System Refresh Project outlines vision for iVote as a voting channel, though there is no clear plan for communication of the vision or a program of public engagement and education.<br>• Communication is not driven from a defined | Partially Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | stakeholder engagement strategy/plan. Most engagement is responsive to identified issues/events only to address voter concerns. | | |
| | 5 | Compliance | Ineffective compliance management may lead to operation of iVote outside of regulatory and legal obligations. | Unlikely | Moderate | Medium | • NSWEC maintain clear policy requirements for iVote Technology Assisted Voting.<br>• Indicative compliance requirements of iVote platform to electronic voting standards and guidelines are captured in the iVote Security Implementation Statement 'Appendix B-Legal, Operational and Technical Standards for e-Voting'.<br>• No detail around how compliance obligations are currently managed and assessed. | Partially Effective | Medium |
| | 6 | Governance Structures | Inadequate control and oversight within governance structures for iVote may inhibit decision making, independence and separation of responsibilities. | Unlikely | Major | High | • The Voting System Refresh Project Business Case identifies the governance and stakeholder groups responsible for the management and operation of iVote. | Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  | 7 | Voter Impersonation | Ineffective controls in voter registration component of iVote may lead to automated or large scale voter impersonation. | Unlikely | Major | High | • The Voting System Refresh Project RFP is based on principles addressing impersonation.<br>• Relative to current paper-based voting, current iVote adds increased security in the registration process through capturing identity information, and postal verification of registration. | Partially Effective | Medium |
|  | 8 | Policy and Procedures | Inadequate, outdated or unenforced iVote policies and procedures may not drive expected organisational behaviours and system outcomes and objectives. | Unlikely | Major | High | • Maintenance of policy and procedure documentation for iVote is within scope of NSWEC Legal and Governance Unit.<br>• Operational budget for support (addressing applicable policy and procedures) will be determined at the end of the Voting System Refresh Project through transition to operational BAU IT support.<br>• Current budget for the support of iVote, including maintenance of procedures, is project-based, supported from a | Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  | small operational team in NSWEC.<br>• Role and responsibility for security, including maintenance of appropriate policy and procedure, have been assigned and are within the scope of Executive Director, Information Services. |  |  |
| **2. Solution Design and Documentation** | 9 | Voting System Refresh Project RFP | Change in RFP approach for Voting System Refresh Project to include "innovative suggestions" from respondents beyond stated requirements may lead to increased complexity in assessing solution responses. | Unlikely | Moderate | Medium | • Voting System Refresh Project has a defined Steering Committee providing oversight and governance.<br>• Voting System Refresh Project RFP documents specify principles, standards and requirements for Voting System software.<br>• Voting System Refresh Project includes a detailed design stage to follow with successful respondent, which should help address inclusion of "innovative solutions". | Partially Effective | Medium |
|  | 10 | Project Requirements and System Documentation | Voting System Refresh Project design may not capture all | Unlikely | Major | High | • Detailed functional and non-functional requirements are included in the Voting | Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | functional or technical requirements through inadequate stakeholder engagement or document standard definition. | | | | System Refresh Project RFP documents, with scope for a detailed design stage to follow with successful respondent.<br>• Governance model and stakeholder analysis and engagement is identified and defined in the Voting System Refresh Project Business Case, to assist business stakeholder engagement in requirements capture.<br>• Details of security requirements and configuration in iVote Security statement (2014) assist in outlining security requirements.<br>• Current Voting System Project RFP documentation identifies detailed security requirements.<br>• Document management policies and control in place in NSWEC. | | |
| | 11 | System Accreditation | Lack of iVote system accreditation may lead to unknown or | Unlikely | Major | High | • iVote underlying infrastructure maintained by external service providers (AC3, | Partially Effective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  |  |  | unmitigated security risks. |  |  |  | SecureLogic, GovDC) is ISO27001 certified.<br>• There has been no external accreditation of internally developed or software vendor systems (Scytl), in the sense of formalised quality standards. iVote applications have been externally reviewed by selected consultants.<br>• Internal responsibilities for iVote security management are defined, across Director, Election Innovations and Executive Director, Information Services<br>• Voting System Refresh Project RFP outlines principles for the refresh of iVote, based on the ECANZ Essential 11 that clearly identify security as a core principle.<br>• Detailed requirements on security are identified in the Voting System Refresh Project RFP, to further inform vendor requirements. |  |  |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  | 12 | Software Development Life-Cycle | Ineffective controls applied throughout the Software Development Life-cycle (SDLC) may adversely impact the quality and reliability of delivered software. | High | Major | High | • No details around a standardised software development approach and framework in place internally to support the design, build, and test of the system.<br>• No ongoing program of independent security assessment is identified.<br>• SDLC controls are outlined in Scytl contract at a high level.<br>• Vulnerability testing is conducted for iVote prior to election events - Logic and Accuracy testing conducted prior to 2015 SGE.<br>• Voting System Refresh Project RFP documents specify requirements for the Voting System, with scope for a detailed design stage to follow with successful respondent. | Partially Effective | High |
|  | 13 | System Scalability | Limited scalability of iVote reduces the capacity of NSWEC to utilise the system across multiple locations and | Rare | Major | High | • Standards/principles for enterprise architecture are included as part Voting System Refresh Project RFP.<br>• The Voting System Refresh Project RFP | Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | concurrent election events. | | | | outlines non-functional requirements for software, to inform future design and build stages of the project, including concurrency of election events. | | |
| | 14 | System Adaptability | Limited adaptability of iVote reduces its capacity to support functionality across expanded categories of eligible voters. | Unlikely | Major | High | • Roadmap and strategic direction are documented as part of the Voting System Refresh Project RFP, considering adaptability of the system.<br>• Standards/principles for enterprise architecture are included as part of Voting System Refresh Project RFP to influence and inform product design around adaptability.<br>• The Voting System Refresh Project RFP outlines non-functional requirements for software, to be used to inform future design and build stages of the project. | Partially Effective | Medium |
| | 15 | Software Testing | Ineffective testing of software and infrastructure may lead to introduction | Moderate | Moderate | High | • High level policy for technical change management exists | Ineffective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | of exploitable weakness or unacceptable software being delivered. | | | | • A standardised software development approach and framework is being developed internally but is not yet in place to support the design, build, and test of the system.<br>• No detailed defined and enforced change and release approach.<br>• Standards/principles for enterprise architecture are included as part of Voting System Refresh Project RFP. | | |
| | 16 | Architecture Standards | Lack of adequate definition in third party architecture may adversely impacts capacity to meet future solution requirements. | Unlikely | Major | High | • Architecture standards outlined in Scytl and AC3 contracts at a high level.<br>• Standards/principles for enterprise architecture are included as part of Voting System Refresh Project RFP. | Partially Effective | Medium |
| | 17 | Usability and Accessibility | Inadequate support for different types of client platforms (i.e. mobile devices) or usage modes (i.e. blind and low vision) may adversely impact eligible | Unlikely | Major | High | • Standards/principles for enterprise architecture are included as part of Voting System Refresh Project RFP.<br>• Voting System Refresh Project RFP references compliance with the ECANZ Essential 11 | Partially Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | voter engagement in the electoral process. | | | | Principles for Electronic voting, which include Usability and Accessibility. | | |
| | 18 | User Interface and Experience | Ineffective design and implementation of user interface and/or experience may introduce a perceived or actual lack of impartiality which adversely impacts voter engagement and/or behaviour. | Unlikely | Major | High | • Previous examples of remediation of design and user interface issues.[12]<br>• The Voting System Refresh Project RFP outlines requirements for software, to be used to inform future design and build stages of the project.<br>• Voting System Refresh Project RFP documents reference compliance with the ECANZ Essential 11 Principles for Electronic voting, which include Usability and Impartiality. | Partially Effective | Medium |
| | 19 | Design Reviews | Lack of periodic design review process may lead to a lag in functionality and shortfall in system usability. | Unlikely | Moderate | Medium | • No details around a standardised software development approach and framework in place internally to support the design, build, and test of the system. | Partially Effective | Medium |

[12] Previous example of 'left-hand' bias in the online screen.

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  | • The Voting System Refresh Project RFP outlines requirements for software, to be used to inform future design and build stages of the project. |  |  |
| **3. Process Design and Management** | 20 | Voter Distrust | Inadequate public engagement with voters, candidates, and political parties may introduce a perceived lack of transparency and/or controls, leading to mistrust in the iVote system and low adoption rates. | Moderate | Moderate | High | • Communication is mainly responsive to identified issues/events, not driven from a defined stakeholder engagement strategy and plan.<br>• No details around cybersecurity strategy and plan were available, for inclusion in a public awareness campaign.<br>• There has been no external accreditation of internal or vendor systems, that is, in the sense of formalised quality standards, to support voter trust in the system. iVote applications have been externally reviewed by selected consultants. | Partially Effective | High |
|  | 21 | Scrutineering | Inadequate support of electoral scrutineering process for iVote | Unlikely | Moderate | High | • Candidates and political parties are invited to observe the vote decryption ceremony. | Partially Effective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | may lead to a lack of perceived or actual transparency. | | | | • Engagement with scrutineering is impacted in that communication related to iVote is mainly responsive to identified issues/events, not driven from a defined stakeholder engagement strategy and plan.<br>• The Voting System Refresh Project RFP outlines requirements for software, to be used to inform future design and build stages of the project. Clear support for external scrutiny is part of these requirements. | | |
| | 22 | Coercion | Use of iVote leads to different forms of potential voter coercion. | Rare | Moderate | Medium | • Current iVote allows a voter to cast multiple votes, with only the final vote being valid and counted, which provides an opportunity for voting without being under coercion.<br>• The Voting System Refresh Project RFP outlines requirements to addresses causes of coercion, to be used to inform future design | Partially Effective | Low |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | and build stages of the project. | | |
| | 23 | Political stakeholder management and education | Inadequate planning and support for candidates/political parties to educate and engage with iVote may result in resistance, disengagement and potential legal challenges. | Unlikely | Moderate | Medium | • NSWEC has undertaken some engagement with political stakeholders in relation to iVote as part of preparatory work for electoral events. | Ineffective | Medium |
| | 24 | Legality of Election Results | Failure in iVote system security or availability may impact on the integrity of election results and lead to election irregularity and reputational damage to NSWEC. | Unlikely | Major | High | • Current system logging, security and availability controls are established and outlined in Voting System Refresh Project RFP.<br>• Public engagement and education in relation to iVote is mainly responsive to identified issues/events, not driven from a defined stakeholder engagement strategy and plan to manage expectations around iVote. | Partially Effective | High |
| | 25 | Voter Cybersecurity Awareness | Ineffective cybersecurity education and awareness in the | Unlikely | Major | High | • Communication is mainly responsive to identified issues/events, not driven from a | Ineffective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | context of iVote may lead to vulnerabilities of voters' devices being exploited during an election event. | | | | defined stakeholder engagement strategy and plan to help address cybersecurity awareness for voters in relation to iVote. | | |
| | 26 | Anonymity | Inadequate controls to protect the anonymity of voters in iVote may lead to reduced integrity of the electoral process. | Unlikely | Major | High | • Controls addressing anonymity are documented in the 2015 Security Implementation Statement.<br>• The Voting System Refresh Project RFP outlines requirements for software, including anonymity, to be used to inform future design and build stages of the project.<br>• Voting System Refresh Project RFP documents reference compliance with the ECANZ Essential 11 Principles for Electronic voting, which includes Secrecy of Vote Cast. | Partially Effective | Medium |
| | 27 | Verification | Inadequate design for individual or universal verification of votes may lead to | Unlikely | Major | High | • Credentials can only be used once thus the legitimate voter will know when their credentials have been | Partially Effective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | mistrust in the iVote system and technology assisted voting more generally. | | | | used because they will not be able to vote. The legitimate voter will be able to re-register and the vote from the stolen credentials will be cancelled.<br>• Voters are able to verify their vote on the verification server, identifying vote tampering or loss.<br>• The Voting System Refresh Project RFP outlines requirements for software, including verification, to be used to inform future design and build stages of the project. | | |
| | 28 | Auditability | Inadequate technical auditability in iVote may result in reduced transparency and a lack of capacity to assure system integrity. | Unlikely | Major | High | • Current iVote system supports logging with cryptographic protections.<br>• The Voting System Refresh Project RFP outlines requirements for software, including specifically the auditability or logging of votes, to be used to inform future design and build stages of the project. | Partially Effective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  | 29 | External Disruption | Increase in "group activism[13]" and distribution of negative propaganda to eligible voters may lead to disruption of technology assisted voting and the relevant election. | Moderate | Moderate | High | • Stakeholder engagement is a key control in mitigating this risk. Public engagement in relation to the iVote platform is mainly responsive to identified issues/events, not driven from a defined stakeholder engagement strategy and plan to inform the electorate. | Ineffective | Medium |
|  | 30 | Regulatory Support for Eligibility Legislation | Inadequate policy basis and enforcement resources for regulation of eligibility may lead to use of iVote by voters who do not meet the legislative criteria. | Moderate | Minor | Medium | • Voters are informed about eligibility criteria and their requirements to comply during the Registration step Also voters are required to positively identify which eligibility criteria entitles them to register. | Ineffective | Medium |
| **4. Data Governance** | 31 | Data Management | Ineffective data management may lead to voter information being used, modified and/or shared inappropriately, adversely impacting on data integrity. | Unlikely | Moderate | Medium | • Data classification and information management policies exist, but are lacking definition of responsibilities. | Ineffective | Medium |

[13] Enabled by social media through micro-targeting

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  | 32 | Data Integrity | System logging in iVote may not provide the ability to confirm or deny 'false claims' related to verification. | Unlikely | Major | High | • Voting System Refresh Project RFP outlines requirements for software in integrity and verification, to be used to inform future design and build stages of the project – key among the principles informing design is verification of votes. | Partially Ineffective | Medium |
|  | 33 | Data Sovereignty | Ineffective design and implementation of controls enforcing data sovereignty[14] may lead to data being located overseas (either in transit or storage) without knowledge or consent. | Rare | Major | Medium | • NSWEC policies identify clear requirements and control for voter data, with responsibilities assigned.<br>• Current design of iVote utilises locally hosted services and infrastructure. | Partially Effective | Medium |
| **5. Information Security** | 34 | Application Controls | Ineffective security controls at the application level may lead to increased risk of data loss or data manipulation, reducing trust in iVote. | Unlikely | Major | High | • The Voting System Refresh Project RFP outlines requirements for security controls in software, to be used to inform future design and build stages of the project. | Partially Effective | Medium |

[14] Data sovereignty refers to where data is stored, and how data stored digitally with a service provider may be stored overseas and subject to the jurisdiction of more than one country

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  | 35 | IT General Controls (ITGC) | ITGCs related to logical access, change management, and business continuity that are not regularly tested may lead to inappropriate access, change or reduced capability to recover. | Unlikely | Major | High | • Lockdown Procedures Manual articulates control environment for live voting, which limits access to iVote infrastructure during an election event.<br>• iVote infrastructure service provides have resilience and recovery controls.<br>• Disaster recovery for core voting and verification is in one site (GovDC). Registration and core voting production hosting is in one site (Silverwater).<br>• The Voting System Refresh Project RFP outlines requirements for software, including logical access controls and resilience requirements, to be used to inform future design and build stages of the project. | Partially Effective | High |
| **6. Personnel Security** | 36 | Capability and Capacity | Inadequate skills and capability of iVote system support personnel may not be fit for purpose or not | Moderate | Moderate | High | • None. | Ineffective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | available in a timely manner. | | | | | | |
| | 37 | Trust and Reliability | Personnel supporting iVote and related processes do not have the appropriate security clearances and/or vetting in place. | Likely | Moderate | High | • NSWEC follows NSW State Government policies in regards to staff management, with additional requirements for all staff to make a political neutrality statement and to undergo character assessment. (Security statement 2015).<br>• Contract with AC3 stipulated requirement to comply with NSWEC employee conduct conditions with respect to secrecy and security and provisions of legislation. Noted that Secrecy and Security is not an applicable item in contract with Scytl, though they do state that a security questionnaire is completed during recruitment process of their staff. | Ineffective | High |
| | 38 | Key Personnel | Ineffective workforce planning and skill-sharing may result in one | Likely | Moderate | High | • None. | Ineffective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | or more single point(s) of failure in operation and support of the system. | | | | | | |
| | 39 | Education and Awareness | Inadequate education and awareness of personnel may lead to inappropriate handling of sensitive data. | Moderate | Moderate | High | • NSWEC requires their staff to comply with employee conduct conditions with respect to secrecy and security.<br>• iVote training as per Security implementation Statement (2015). | Partially Effective | High |
| **7. Physical Security** | 40 | Physical Environment | Ineffective physical environment controls for iVote infrastructure primary and backup locations may result in inadequate security and unauthorised access. | Unlikely | Moderate | Medium | • Physical infrastructure is maintained by service providers as part of a managed service offering. | Effective | Low |
| **8. Network and Infrastructure** | 41 | Cyber Threat Monitoring and Incident Management | Inadequate threat monitoring and incident management of iVote infrastructure (at system, network, and/or user interface levels) may lead to exploitable vulnerabilities. | Unlikely | Major | High | • NSWEC contracted the operation of a Security Operations Centre (SOC) as part of the SGE 2015.<br>• Internally to NSWEC, a cybersecurity strategy and plan were yet to be developed and were not available at the time of fieldwork. | Partially Effective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | • Role and responsibility for security within the scope of Executive Director, Information Services. | | |
| | 42 | Vulnerability Testing | Ineffective penetration testing may lead to undiscovered exploitable vulnerabilities and compromise of system data. | Unlikely | Major | High | • Vulnerability testing is conducted for iVote prior to election events ('point in time testing only'). Also, logic and accuracy testing conducted prior to 2015 SGE.<br>• Role and responsibility for security within the scope of Executive Director, Information Services.<br>• No details around cybersecurity strategy and plan were available. | Partially Effective | High |
| | 43 | Asset Management | Inadequate asset management approach results in aging and unsupported systems that may lead to outages. | Unlikely | Major | High | • Roadmap and strategic direction related to iVote as an asset is included within the Voting System Refresh Project RFP. | Partially Effective | Medium |
| | 44 | System Integration and Interoperability | Inadequate design and management of integration with other systems may limit capacity for | Unlikely | Moderate | Medium | • Integration testing is addressed in original Testing strategy, and was conducted by Scytl prior to SGE 2015. | Partially Effective | Medium |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
| | | | interoperability and use of data. | | | | | | |
| | 45 | Network Architecture | Ineffectively designed or implemented network architecture may result in system outage or intrusion. | Unlikely | Major | High | • Vulnerability testing is conducted for iVote prior to election events, including testing of network. | Partially Effective | High |
| **9. Outsourced Technology Services** | 46 | Vendor Contract Management | Inadequate vendor/contract management may lead to ineffective service levels, issue resolution and potential for exploitable vulnerabilities through 3rd party channels. | Likely | Moderate | High | • Procurement management for Voting System Refresh Project RFP is being conducted by specialist procurement team, rather than within previous IT team. | Partially Effective | High |
| | 47 | Software Escrow | Inadequate contractual protection may adversely impact NSWEC interests in the contracts with third party software vendors and service providers. | Moderate | Moderate | High | • Contractual agreement that data, software and documentation is sole ownership of NSWEC is in place. | Effective | Medium |
| | 48 | Service and Performance Management | Ineffective service management processes (e.g. ITIL) may lead to | Moderate | Moderate | High | • The Voting System Refresh Project Business Case identifies the governance and | Partially Effective | High |

| Risk Category | ID | Area | Description of Potential Risk Event | Likelihood | Consequence | Inherent Risk Rating | Treatments Identified | Treatment Assessment | Residual Risk Rating |
|---|---|---|---|---|---|---|---|---|---|
|  |  |  | reduced quality of service adversely impacting performance and availability. |  |  |  | stakeholder groups responsible for the management and operation of iVote.<br>• NSWEC-level governance is provided by the Voting System Refresh Project Steering Committee, with plans to transition operational support and management to BAU IT following completion of the Project. |  |  |
|  | 49 | Vendor software delivery | Low maturity in management of vendor software delivery leads to poor control over software change management, and may result in potential for accidental or intentional breach of compliance requirements, system unavailability, reputational damage and mistrust in iVote. | Likely | Moderate | High | • Vendor's software updates are executed only prior elections (when NSWEC requires and ready to test). | Ineffective | High |

# Appendix A - Engagement Approach

The approach to complete this engagement was undertaken through three key phases of activity which were conducted over a five week period between the 27th November and 22nd December 2017:

1. **Phase 1 – Planning:**
    - Identified and met key stakeholders to confirm engagement objectives, timings and deliverables
    - Identified and confirmed high level risk categories
    - Identified key stakeholders to interview and sought supporting documentation for fieldwork review
    - Provided NSWEC a detailed engagement plan outlining key tasks and timings

2. **Phase 2 – Fieldwork:**
    - Undertook scheduled meetings with identified stakeholders
    - Reviewed provided supporting documentation

3. **Phase 3 – Reporting:**
    - Developed a draft report for NSWEC review and feedback
    - Developed a final report incorporating feedback provided

Throughout these phases, PwC engaged on a regular basis with Mr. Wilkins and Mr Gareth Robson (NSWEC) to provide updates related to progress, findings and observations.

## *Limitations and Constraints*

As part of this engagement it was stated that:

- PwC will not provide assurance on the applicability of iVote to meet the stated requirements of the NSWEC.
- PwC will not provide detailed remediation actions, but rather provide identification of risk areas which may require attention.
- PwC will not provide any testing (penetration or technical vulnerability) which examines the ability to exploit iVote.

# Appendix B - Stakeholders Consulted

The following stakeholders were engaged during this review:

*Table 5. Stakeholders consulted*

| Name | Role | Date |
|---|---|---|
| Roger Wilkins AO | Inquiry Report author | 28/11/17<br>Numerous |
| Alastair MacGibbon | Consulting Panel Member and Special Advisor to the Prime Minister on Cyber Security | 13/11/17<br>20/12/17 |
| John Schmidt | NSW Electoral Commissioner | 20/12/17 |
| Antony Green AO | Consulting Panel Member and ABC Election Analyst | 7/12/17<br>20/12/17 |
| Professor Rodney Smith | Consulting Panel Member and University of Sydney Researcher | 12/12/17 |
| Gareth Robson | Legal Officer.<br>NSW Electoral Commission | 21/11/17<br>Numerous |
| Mark Radcliffe | Director, Election Innovation. NSW Electoral Commission | 22/11/17<br>20/12/17 |
| John Cant | Executive Director, Information Services.<br>NSW Electoral Commission | 29/11/17<br>21/12/17 |
| Simon Kwok | Executive Director, Election. NSW Electoral Commission | 29/11/17<br>20/12/17 |
| Sam Campbell | Operation Director.<br>Scytl | 13/12/17 |
| Kieran Deale | Operation Manager.<br>GovDC | 29/1/18 |
| Deepak Singh | Managed Service Manager. SecureLogic. | 29/1/18 |
| Rick Yacob | Relationship Manager.<br>AC3 | 24/1/18 |
| Gerard Azar | Milliways | Requested |

DRAFT

| Name | Role | Date |
|---|---|---|
| Dr Vanessa Teague | Academic researcher.<br>University of Melbourne | 16/01/18 |

# Appendix C – Supporting Documentation

The following supporting documentation was provided and reviewed as part of this review:

*Table 6. Supporting documentation*

| # | Document | Date of the document | Received date |
|---|---|---|---|
| 1 | iVote Initiation Refresh | Nov 2017 | 21/11/2017 |
| 2 | Infrastructure arrangements 2015 | Nov 2017 | 22/11/2017 |
| 3 | iVote Refresh Procurement strategy_V2 | Jun 2017 | 22/11/2017 |
| 4 | Industry engagement outline | Jun 2017 | 22/11/2017 |
| 5 | An overview on iVote system 2015 (article) | Jul 2015 | 22/11/2017 |
| 6 | iVote Strategy for SGE 2015: Key issues, guidelines, application architecture and voting protocol | Mar 2015 | 22/11/2017 |
| 7 | iVote Security_Implementation_statement_Mar2015 | Mar 2014 | 22/11/2017 |
| 8 | iVote Transforms the Electoral System_ Computer Science Corporation | 2014 | 21/11/2017 |
| 9 | Response to Freak vulnerability | Oct 2015 | 22/11/2017 |
| 10 | Response by NSWEC to observations of Bias in iVote results | May 2015 | 22/11/2017 |
| 11 | iVote Incident report_01_Legislative council ballot | Mar 2015 | 22/11/2017 |
| 12 | iVote Audit requirement_ | Sep 2014 | 21/11/2017 |
| 13 | iVote Threat Analysis & Risk Assessment SGE 2015 | Jan 2014 | 21/11/2017 |
| 14 | Doc006 201502 iVote Risk Register_V0.8 | Feb 2015 | 22/11/2017 |
| 15 | 11 Principles for an Australian internet voting service | Jul 2017 | 21/11/2017 |
| 16 | NSWEC Business Case Enhancement for SGE2019 | Feb 2017 | 1/12/2017 |
| 17 | Test Strategy for SGE 2015 | Dec 2014 | 22/11/2017 |
| 18 | Attachment A1: iVote System Overview v2.8 | May 2014 | 22/11/2017 |
| 19 | A2_Detailed System Requirements | May 2014 | 22/11/2017 |
| 20 | Appendix C - Legal, Operational and Technical Standards for e-Voting | 2014 | 22/11/2017 |
| 21 | **RFP:** software interfaces 1.2 | Dec 2017 | 5/11/2017 |
| 22 | **RFP:** Call flows and Phone Interface 1.2 | Dec 2017 | 5/11/2017 |
| 23 | **RFP:** User Interface 1.2 | Dec 2017 | 5/11/2017 |
| 24 | **RFP:** Contests, Ballots and Counting 1.2 | Dec 2017 | 5/11/2017 |
| 25 | **RFP:** iVote System overview 1.2 | Dec 2017 | 5/11/2017 |

| # | Document | Date of the document | Received date |
|---|---|---|---|
| 26 | **RFP:** Voting system RFP requirements 1.2 | Dec 2017 | 5/11/2017 |
| 27 | **RFP**: General Terms and Conditions 1.2 | Dec 2017 | 5/11/2017 |
| 28 | **Scytl:** Core System contract | Dec 2017 | 21/11/2017 |
| 29 | **Scytl:** Core System contract Part II | Dec 2017 | 21/11/2017 |
| 30 | **Scytl:** PIPP | Dec 2017 | 21/11/2017 |
| 31 | **Scytl:** Software specification for Core Voting system | Dec 2014 | 21/11/2017 |
| 32 | **Scytl:** Receipts_UI Specs Mobile | Dec 2014 | 21/11/2017 |
| 33 | **Scytl:** Mobile_receipts_UI Specs 0.1 | Dec 2014 | 21/11/2017 |
| 34 | **Scytl:** Desktop Receipts_UI Specs 0.1 | Dec 2014 | 21/11/2017 |
| 35 | **Scytl:** WebServer_Specification 2.3 | Dec 2014 | 21/11/2017 |
| 36 | **Scytl:** Web Interface_Specification | Dec 2014 | 21/11/2017 |
| 37 | **Scytl:** Web Client Error List 2.5 | Dec 2014 | 21/11/2017 |
| 38 | **Scytl:** WebServer_Specification 2.6 | Dec 2014 | 21/11/2017 |
| 39 | **Scytl:** Web Interface Specifications_v0.7 | Dec 2014 | 21/11/2017 |
| 40 | **Scytl:** Web Client Specification v0.7 | Dec 2014 | 21/11/2017 |
| 41 | **Scytl:** Voting Management Error List 1.3 | Dec 2014 | 21/11/2017 |
| 42 | **Scytl:** Tablet_UI_specifications v4.9 | Dec 2014 | 21/11/2017 |
| 43 | **Scytl:** IVR Error List v1.3 | Dec 2014 | 21/11/2017 |
| 44 | **Scytl:** Desktop_UI_Specifications v0.8 | Dec 2014 | 21/11/2017 |
| 45 | **Scytl:** VoteEncorder v0.3 | Dec 2014 | 21/11/2017 |
| 46 | **Scytl:** Specifications Document v 2.3 | Dec 2014 | 21/11/2017 |
| 47 | **Scytl:** Immutable Logs v 3.1 | Dec 2014 | 21/11/2017 |
| 48 | **Scytl:** Cleansing Decoder v4.3 | Dec 2014 | 21/11/2017 |
| 49 | **Scytl:** Ballot Controller Specification v3.5 | Dec 2014 | 21/11/2017 |
| 50 | PWC Pre-Implementation report 2014 | 2014 | 21/11/2017 |
| 51 | PWC Post-Implementation report 2014 | 2014 | 21/11/2017 |
| 52 | PWC audit 2011 | 2011 | 21/11/2017 |
| 53 | NSW Electoral Commission Report on the Conduct of the 2015 State General Election | 2015 | 10/12/2017 |
| 54 | iVote Incident communication plan_Doc079_v2.7 | Oct 2017 | 14/12/2017 |
| 55 | iVote Security Incident Response Plan v1.3- SBE-Oct-2017_Doc080 | Oct 2017 | 14/12/2017 |
| 56 | **AC3** : Verification service contract | Dec 2014 | 21/11/2017 |
| 57 | **AC3:**Verification Hosting: Infrastructure specifications | Dec 2014 | 21/11/2017 |
| 58 | **AC3:** Change management Process – Emergency ver1.3 | 2016 | 29/01/2018 |
| 59 | **AC3:** Change Management Process - Normal ver 1.3 | 2016 | 29/01/2018 |
| 60 | **AC3:** Change Management Process - Standard ver 1.3 | 2016 | 29/01/2018 |
| 61 | **AC3:** Incident Management Process ver 1.1 | 2016 | 29/01/2018 |

| # | Document | Date of the document | Received date |
|---|---|---|---|
| 62 | **AC3:** Major Incident Management Process ver 1.3 | 2016 | 29/01/2018 |
| 63 | **AC3:** Request Fulfilment Process ver 1.1 | 2016 | 29/01/2018 |
| 64 | **AC3:** Service Desk Triage v1.1 | 2016 | 29/01/2018 |
| 65 | **AC3:** Service Level for IaaS | Feb 2016 | 29/01/2018 |
| 66 | **AC3:** Service Levels for Incidents and Requests | Feb 2016 | 29/01/2018 |
| 67 | **AC3:** ISO 9001 Certificate (QMS41901) 20160413 | Apr 2016 | 29/01/2018 |
| 68 | **AC3**: ISO 27001 Certificate (ITGOV40082) 20160413 | Apr 2016 | 29/01/2018 |
| **69** | NSWEC ICT Technical Change Management Policy | Oct 2017 | 19/02/2018 |
| **70** | CSC-NSWEC SOC Proposal including Order Form | Feb 2015 | 19/02/2018 |
| **71** | NSWEC Code of Conduct Acknowledgement | 2017 | 19/02/2018 |
| **72** | NSWEC Disclosure of Enrolment, Electoral and Election Information Policy | May 2017 | 19/02/2018 |
| **73** | NSWEC Privacy Management Plan | Jun 2017 | 19/02/2018 |
| **74** | NSWEC Appointment as Election Official for Technology Assisted Voting Instrument | Nov 2016 | 15/02/2018 |
| **75** | NSWEC SGE 2015 Candidate Information Seminar presentation | Mar 2015 | 23/02/2018 |
| **76** | NSWEC Scrutineer Guidelines for Technology Assisted Voting | NA | 23/02/2018 |
| 77 | NSWEC NSW State By-elections Bulletin Number 4 2017 | Apr 2017 | 23/02/2018 |

© 2018 PricewaterhouseCoopers. All rights reserved.
PwC refers to the Australian member firm, and may sometimes refer to the PwC network.
Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

Liability limited by a scheme approved under Professional Standards Legislation