Technology Assisted Voting Audit

Post Implementation Report

June 2011

Disclaimer

Our report has been prepared solely for the use of the NSW Electoral Commission. Except as required by law, this report may not be provided to any other person. We do not accept any responsibility to any other person for any consequences arising from any reliance on our report or any part of it, nor do we accept any responsibility to NSW Electoral Commission for any consequences arising from any reliance on our report or any part of it for any other purpose. Liability limited by a scheme approved under Professional Standards Legislation.

The information, statements, statistics and commentary (together the "Information") contained in this report have been prepared by PwC from material provided by NSW Electoral Commission. PwC have not sought any independent confirmation of the reliability, accuracy or completeness of this information.

Accordingly, whilst the statements made in this report are given in good faith, PwC accept no responsibility for any errors in the information provided by NSW Electoral Commission or other parties nor the effect of any such errors on our analysis, suggestions or report.

The procedures that we have performed 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, consequently, no assurance has been expressed.

NSW Electoral Commission

iVote Audit Reports

Review fieldwork performed:	18 January 2011 – 21 May 2011
Pre Implementation report issued:	7 March 2011
Draft Post Implementation report issued:	7 June 2011
Final Post Implementation report issued:	21 June 2011

DISTRIBUTION LIST

NSW Electoral Commissioner	Colin Barry
NSWEC IT Director	Ian Brightwell

Table of Contents

1 Introduction

PricewaterhouseCoopers (PwC) has been engaged by the NSW Electoral Commissioner to undertake an audit of the technology-assisted voting application, iVote, in compliance with the *Parliamentary Electorates and Elections Act 1912*, amendment No. 41, division 12A.

2 Background

NSW Parliament requested that the Electoral Commissioner investigate the feasibility of remote electronic voting for vision-impaired and other disabled persons, with the primary objective being to enable a secret vote for people who are blind or vision impaired. The final version of the feasibility report was tabled in Parliament on 2 September 2010. The feasibility report concluded that a technology assisted voting application was feasible although it would be difficult to implement to meet the NSW State Election in March 2011.

On 24 November 2010 the *Parliamentary Electorates and Elections Act* was amended to give effect to the Electoral Commissioner's feasibility report. The Bill was agreed in principle to provide blind or vision-impaired people of NSW the ability to vote in secret using a computer or telephone at a private location such as their home. A further amendment was made on 7 December 2010 to include persons unable to vote by reason of location.

The Bill requires an independent audit of the technology-assisted voting system, both before and after each general election, to ensure that it properly reflects the votes cast and that it is secure. This will allow tests of the iVote system software to ensure that it is accurate and that the secrecy of votes is protected, with the system resistant to hackers and any other malicious tampering.

The following Audit requirements exist for the iVote Remote Electronic Voting System and are in accordance with the *Parliamentary Electorates and Elections Act 1912*, No 41, Part 5, Division 12A, 120AD: Independent Auditing of Technology Assisted Voting:

(1) The Electoral Commissioner is to engage an independent person (the independent auditor) to conduct audits of the information technology used under the approved procedures.

(2) Audits under this section are to be conducted and the results of those audits are to be provided to the Electoral Commissioner:

  (a) at least 7 days before voting commences in each Assembly general election at which technology assisted voting is to be available, and

  (b) within 60 days after the return of the writs for each Assembly general election at which technology assisted voting was available.

(3) Without limiting the content of the audit, the independent auditor is to determine whether test votes cast in accordance with the approved procedures were accurately reflected in the corresponding test ballot papers produced under those procedures.

(4) The independent auditor may make recommendations to the Electoral Commissioner to reduce or eliminate any risks that could affect the security, accuracy or secrecy of voting in accordance with the approved procedures.

3 Objectives and Scope

The audit objective is to review the iVote Remote Electronic Voting System in accordance with the *Parliamentary Electorates and Elections Act 1912, No 41, Part 5, Division 12A, 120AD: Independent Auditing of Technology Assisted Voting*. In particular, an Electronic Voting Post Implementation review will be conducted within 60 days after the return of writs (13 April 2011). The Technology Assisted Voting Approved Procedures for NSW State General Election 2011, dated 9 March, detail the audit requirements.

Review objective	Areas reviewed
Accuracy and completeness of votes cast via iVote	• Follow-up of risks identified in pre implementation audit report • iVote Testing and completion reports • creation and approval of "Technology Assisted Voting Approved Procedures for NSW State General Election 2011" • Go/no-go decision • iVote system reports • the exclusion process of votes cast via iVote where a postal vote had also been received • iVote election closure and decryption of votes • conversion of Electoral Mark-up Language (EML) file to PDF for printing
Security of the iVote system	• Security testing reports (penetration testing, application code testing and cryptographic testing) • Infrastructure security including monitoring and alerting processes • NSWEC Security test summary report

4 iVote Statistics

The iVote application went live on 14 March 2011 and remained available for voting purposes until the 25 March 2011. During this period 46,864 eligible iVote users voted. This consisted of 44,605 via the internet and 2,259 via Interactive Voice Response (IVR).

At 6pm on 26 March the votes cast in iVote were decrypted by the appointed Electoral Board (requiring at least three members of the five member Electoral Board appointed by the Commissioner to control the keys for the encryption/decryption process). A total of 46,864 votes in both Legislative Assembly (LA) and Legislative Council (LC) were decrypted and a report from the system indicated that no tampering had occurred (cryptographic integrity checks). The ballots were printed and checked prior to despatching to be formally counted.

5 Key Findings

During the course of our review nothing came to our attention that would indicate that votes cast via the iVote system were not recorded, extracted and printed accurately. We reviewed the testing of the iVote system and validated the test results which indicated that votes cast via the web and phone matched those entered, encrypted, stored, decrypted and subsequently printed. The security of the iVote system was independently reviewed by third party security experts and included reviews covering:

- iVote penetration testing (web and IVR)
- ivote source code review
- Cryptography audit of iVote
- iVote infrastructure security design and including processes, people and technology.

The results of the security assessments performed by third party security experts during February 2011 highlighted areas that required action to be taken by NSWEC. In the time prior to 'go live' on 14 March 2011, a number of risks were addressed and security testing re-performed. However some of risks identified by third part security experts and NSWEC remained outstanding during the voting period, 14 to 25 March 2011. The risks were accepted by NSWEC prior to 'go live' on 14 March and were documented in their iVote project risk register. Refer Appendix B for summary of areas reviewed.

The information provided by NSWEC and available at the time of our review suggest that no risk raised in the iVote project risk register eventuated that impacted the integrity of the iVote system and the votes cast. However, five incidents occurred through the voting period for iVote and are detailed in Appendix C. The most significant incident affecting 43 ballots was identified by the NSWEC iVote project team on Sunday 27 March when ballots were detected as having the letter "N" instead of numeric preferences. This required a determination to be made by the Electoral Commissioner on each of the 43 votes cast. This has been documented by the iVote project team in an incident report, "iVote by Web allowing letter 'N' onto ballots Incident Report", dated 5 April 2011.

The iVote Project experienced tight timeframes to implement the solution due to the late passing of amendments to the *Parliamentary Electorates and Elections Act 1912.* The compressed timeframe resulted in incomplete documentation, restricted test case formulation and compressed testing activities.

In the most part, except for the detailed incidents, the level of expertise assembled by NSWEC to manage the electronic voting project for the NSW 2011 State Election compensated for the compressed timeframe. However, this did restrict the quality and timeliness of documentation available for our review. In addition the project team dispersed shortly after the election resulting in limited availability of key project staff to respond to questions.

We performed a pre implementation review which highlighted a number of areas requiring attention prior to 'go live'. In the most part these were successfully addressed and are detailed in Appendix A.

6 Acknowledgement

We wish to acknowledge the assistance and co-operation received from staff and management during the course of this review.

Mark Driessen
Partner

Appendix A – Detailed Observations

The table below includes observations and priority ratings made prior to iVote go live in the pre implementation report issued by PwC on 7 March 2011. An additional column, "Action taken by NSWEC", was prepared by PwC as part of our post implementation review activities.

Key Risk Area	Observation	Priority	Action taken by NSWEC
Testing	The first cycle of security testing has been performed against the practice system and significant security vulnerabilities were highlighted in the preliminary Stratsec report. The issues should be formally responded to by EveryoneCounts and NSWEC. A test completion report prepared by NSWEC should summarise the testing performed and conclude on the testing results. Actions required to mitigate or resolve issues raised during testing should also be included.	High	Analysis was performed by NSWEC of all security issues raised and an assessment performed on the residual risk following any mitigation activities. EveryoneCounts, the iVote software vendor, responded to the issues raised and provided several software patches to address risks. The residual risk was accepted by the Project Steering Committee and is documented in the 'iVote Stratsec Test report – detailing actions taken and mitigation of risks identified during white and black box testing'.
	Prior to a 'go live' decision testing should be completed on the final software and hardware configuration. This should include functional and regression testing. A full end-to-end dress rehearsal, including the security key ceremony and all participants that will have a role in iVote, should also be performed. Ballot information will be loaded prior to 14 March and should also have an audit trail to confirm accuracy.	High	Completed, however several issues raised during the voting period indicated that the level of testing should be expanded for future electronic voting applications.

Key Risk Area	Observation	Priority	Action taken by NSWEC
	The traceability matrix, which links testing with the Test Standard to ensure completeness, needs to be finalised prior to implementation.	High	Partially completed. Time constraints prohibited the completion of this activity. This activity would have helped identify gaps in testing.
	Usability and accessibility test completion reports have been prepared and contain a number of issues to be addressed. These issues require analysis to determine whether they can be remediated prior to 14 March and if further testing is required.	Medium	Action was taken to remediate issues prior to go live.
Risk Management	A risk log has been developed, however there is not a consolidated log across all areas of the project. A consolidated risk log, including infrastructure risks, should be developed that clearly shows the risk, the likelihood and impact and how this is being mitigated or accepted. This log will be a key input into the go/no-go decision process.	High	A consolidated risk position was developed for the go/no-go decision.
Go/no-go checklist	A go/no-go checklist should be developed as soon as possible to ensure that clear criteria are established.	High	Completed. A decision was made to proceed on the basis of advice given by the project team and presented in a go/no-go checklist.

Key Risk Area	Observation	Priority	Action taken by NSWEC
iVote operating procedures	The application architecture document that describes the end to end process from voter registration to vote counting and election closure should be completed. By formalising key documentation it provides different areas of the project with a consistent overview and confirms roles and responsibilities.	High	Partially completed due to time constraints. The core elements were defined. Future electronic voting applications should ensure that documentation is produced in a timely manner.
	All iVote documentation should be centrally managed and should be available to the project team in both hard and soft copy with appropriate version control.	High	Documentation has been stored in a central online folder although many of the documents remain in draft due to time constraints. Some key documentation was finalised post election including the iVote Infrastructure High Level overview document.
Monitoring	At the time of the review, application and system monitoring had not been fully defined. Monitoring of the application had not been fully described by the vendor and testing had not been conducted to ensure required events are logged and escalated appropriately.	High	A detailed design document was prepared prior to go live however was only formally finalised in May. The Intrusion Protection System (IPS) was not implemented as per design due to time constraints on the advice of a third party. Mitigation was achieved through alternative alerting systems.

Key Risk Area	Observation	Priority	Action taken by NSWEC
Service continuity	A business continuity plan had not been developed to fully describe disruption scenarios. It is essential that probable events are planned for and a clear understanding of how the system can be recovered to maintain vote integrity. In the event of e-voting services being disrupted a process to inform registered voters should be developed. In addition the recovery time objective had not been defined to enable testing of the disaster recovery components. A definitive position should be established on what recovery time objective needs to be established to support the voting process and whether the IT infrastructure and associated processes support this objective.	High	Scenarios have been identified and appropriate recovery was detailed in the iVote Infrastructure High Level Overview document. The service continuity was successfully exercised when a communication fault occurred between data centres.
	The recovery time objective had not been defined to enable testing of the disaster recovery components. A definitive position should be established on what recovery time objective needs to be established to support the voting process and whether the IT infrastructure and associated processes support this objective.	High	Not explicitly defined however scenarios identified.

Appendix B – Post Implementation areas reviewed

Review objective	Areas reviewed	Results
Accuracy and completeness of votes cast via iVote	• Follow-up of pre implementation risks • iVote Testing • Go/no-go decision • iVote system reports • the exclusion process of votes cast via iVote where a postal vote had also been received • iVote election closure, decryption and printing of votes • conversion of Electoral Mark-up Language (EML) file to PDF for printing	No exceptions noted
Security of the iVote system	• Security testing reports (penetration testing, application code testing and cryptographic testing) • Infrastructure security including monitoring and alerting processes • NSWEC Security test summary report	A number of risks were identified but accepted by NSWEC and are detailed in the "iVote Test Summary Report". No identified risks were realised from the information provided to us by NSWEC.

Appendix C – Incidents

Incident	Description	Impact
Electors received seven digit iVote numbers	A mistake was made when generating the iVote numbers on 17 March 2011 where the check digit generation step was omitted and a 7 digit number was loaded into iVote (rather than an 8 digit number). Electors were distributed the 7 digit number via email and SMS. The 8 digit iVote number was resent to the affected electors with an explanation.	1,026 people received the 7 digit iVote number. 182 voters cast a vote using their 7 digit iVote number and were asked to re vote with a new 8 digit iVote number. The iVote system didn't prevent the 7 digit number from being used however this was not discovered during testing and relied on 8 digit iVote numbers being set up correctly.
A reminder to vote was sent to people who had already voted in iVote.	On 22 March 2011 electors who had registered for iVote but had not yet cast their vote were sent reminders by email or SMS to vote. However, this correspondence was also sent to electors who had already voted.	842 electors impacted. All 842 electors were notified via SMS and email to assure them that their vote was cast successfully.
Failure of inter-site link between iVote data centres.	At 1:19 am on 21 March 2011 the inter-site link between the ATP and GS data centres failed.	The root cause was identified and all vote traffic for a period of approximately 12 hours was routed through the backup site with no voter impact.

Incident	Description	Impact
Short outage of live iVote system for around 8 minutes.	On 23 March 2011 between 10.24 am and 10.33 am the iVote web system experienced an outage.	No voter impact. After a full investigation no cause could be identified. Details of investigation noted in incident report.
iVote by web allowing the letter "N" onto ballots.	On Sunday 27th March, immediately after polling day, it was observed that an output file of the votes from the iVote system did not appear to agree with the number of votes actually printed. Investigation determined the real issue was that a failure of java script on the iVote web pages had allowed non-numeric characters to be entered as ballot preferences. There were 43 ballot papers affected and 3 of these only had a gap in sequence of preferences that could be handled within normal formality rules. This resulted in the Commissioner determining that 1 of the 4 affected Legislative Assembly ballot papers was informal and that 8 of the 36 affected legislative Council ballot papers were informal.	Following a full briefing from the iVote Project team and the software vendor the Electoral Commissioner made a determination on the affected votes. This has been fully documented. The issue did not occur during testing, including stress testing, but could have been prevented by simple improvements to the system design.