www.pwc.com.au

Electoral Commission NSW

Post Implementation Review of the iVote Project

FINAL Report

electoral commission NSW

Final Report

July 2015

Contents

1 Executive Summary

1.1 Introduction

PricewaterhouseCoopers ("**PwC**", "**our**", "**us**" or "**we**") has been engaged by the NSW Electoral Commission ("**NSWEC**", "**your**" or "**you**") to undertake a Post-Implementation review of the technology assisted voting application, called the iVote Remote Electronic Voting System ("**iVote**"). This follows an Interim Pre-Implementation review of iVote undertaken by PwC which was finalised on 9th March 2015.

The Interim Pre-Implementation report highlighted significant issues only and did not form an opinion to approve effectiveness of iVote, go-live readiness of iVote or the completeness of its technical of functional requirements in relation to the Parliamentary Electorates and Elections Act.

The scope of the Interim Pre-Implementation review included:

- Undertake a desk top review of certain iVote-related project documents created by NSWEC and third party providers. These documents include iVote system requirements, iVote technical specifications, the iVote test strategy and plan, the iVote business continuity processes and iVote pre-implementation readiness documents;
- Review and assess the project governance of iVote by interviewing NSWEC project members to understand the project operating framework and reviewing key evidence documents, such as project steering committee minutes and project risk management frameworks provided to us by NSWEC, and;
- Review sample of test cases to report on whether the functional requirements of iVote developed by NSWEC, such as behaviours that affect the operations of user activity, have documented expected outcomes. This was achieved by us selecting a random sample of tests cases, along with expected outcomes, and providing them to us to review the outcome against the expected result.

1.2 Objectives and Scope

The objective of our engagement was to undertake a Post-Implementation review of iVote to aid NSWEC in meeting its obligations for independent auditing of technology assisted voting, under the '*Parliamentary Electorates and Elections Act 1912 (the "**Act**"), amendment No. 41, division 12A, 120AD: relating to technology assisted voting*'.

The scope of the Post-Implementation review was to perform the following activities:

i. Follow up the NSWEC actions taken with regards to the issues raised in the PwC iVote Interim Pre-Implementation Report, to track management's completion of the agreed actions from the review, specifically in relation to the:
   - iVote system development standard findings
   - Project governance findings

ii. Assess by review and observation the processes and controls used to secure access to iVote before the commencement of voting.

iii. Undertake a visit to the offices of the third party who are providing a Security Operations Centre (SOC) during voting, to:
   - Observe the SOC and monitoring controls that are in place.
   - Review the incident event log for any adverse incidents and the process for escalating issues to NSWEC.

iv. Assess by review and observation the NSWEC processes for testing the logic and accuracy of the iVote system and note any adverse findings. Logic and accuracy testing is the process by which voting equipment is configured, tested, and certified for accuracy prior to an election.

v. Assess by review and observation the processes and controls used for the voting decryption ceremony once the election has ended.

vi. Review relevant reports created by third parties, such as security intelligence output from relevant third party security monitoring and data centre hosting providers, to understand any adverse findings.

Scope clarification

We understand that NSWEC may wish to make this report publically available on its website. Unless otherwise approved by us in writing, NSWEC may only make the report available on the following conditions:

- the report is published in its entirety and in its final form;
- the report is only published on NSW government websites; and
- no summary of the report is published.

We do not accept any liability or responsibility to any other party to whom this report may be shown or into whose hands it may come.

In the performance of our services, we have not verified the accuracy or completeness of information and materials provided by NSWEC in respect of the analysis we have undertaken. This includes information and comments referenced as "management comments" throughout the report, which were received directly from NSWEC in response to findings that were raised during the Interim Post Implementation Report, carried out by PwC.

This report does not provide any express or implied representation on:

- the accuracy or completeness of any software, or compliance of software with legislation or regulations;
- the go-live readiness of the iVote software;
- the suitability of the iVote software for future elections;
- previous versions of the iVote software, or;
- improvements made to the iVote software following pervious audits or independent reviews.

The services undertaken by us do not constitute tax advice, legal advice or an audit or review in accordance with Australian Auditing Standards, Standards on Review Engagements or Standards on Assurance Engagements as issued by the Auditing and Assurance Standards Board and accordingly no such assurance is provided.

1.3 Summary of findings

The *Parliamentary Electorates and Elections Act 1912* was amended to make provision for technology assisted voting for persons with impaired vision or with certain other disabilities and for persons unable to vote by reason of location. This is the second instance where NSWEC has utilised the iVote approach during a state general election, the first being 2011.

The Post-Implementation review supplements the Interim Pre-Implementation Review that was carried out by PwC between January and March 2015. The Post-Implementation review has focused on management actions to address issues raised by the Interim Pre-Implementation review and observation and assessment of critical processes, detailed in section 1.2 of this report. NSWEC addressed a number of the issues that were raised by the iVote Interim Pre-Implementation Report relating to the design and build of iVote. However some of the issues that were raised regarding the overall governance of the iVote project were not addressed due in part to the completion of the project itself. NSWEC have noted these for consideration in future projects. .

NSWEC and their third party providers were required to undertake a number of critical tasks in order to prepare the system for live voting, such as ensuring the system was secure and stable during voting, through the use of system monitoring tools and secure access mechanisms; and ensuring a successful close down following voting completion, by taking the voting system off-line.

The critical tasks, detailed in section 1.2 of this report, were executed by NSWEC and third party providers. NSWEC identified that a number of potential security threats were identified by monitoring solutions, reviewed and mitigated to prevent exposure of the voting process or data. The number of votes cast was significantly higher than expected due to increased demand of online voting however the system stability remained within NSWEC expectations and nor were there any unexpected impacts to the voting process for the end user.

For those processes observed the processes undertaken were supported by documentation that was updated accordingly where a process may have deviated from what was expected. Additionally all critical processes required authorisation and were subject to review from third parties and PwC.

A summary of the exceptions raised in the Interim Pre-Implementation Review and subsequent actions taken to address them is detailed in section 2 of this report. A summary of the actions and processes observed as part of the Post-Implementation review are detailed in section 3 of this report.

2 Interim Pre-Implementation Review Management Actions

This section details the findings that were reported on as part of the iVote Interim Pre-Implementation Review that took place in March and the subsequent actions taken by NSWEC Management to address them.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
2.1	**The process for replication and redundancy is yet to be detailed, documented and tested** NSWEC intends to utilise the NSW Government Data Centre for hosting, replication and redundancy purposes, contracted as a managed service through Secure Logic. However the process is yet to be fully detailed and documented. Furthermore the process to perform a replication test before live voting, to validate the system restore process, has not been scheduled. The NSW Government Data Centre is a Government approved Tier 3 hosting environment located in Silverwater and Unanderra, the hosting solution has support for the full scope of services including provisioning and support of hosting environment, connectivity, security, and professional services on the solution implementation and integration. The requirements and responsibilities need to be documented and confirmation that the facility can meet these requirements needs to be obtained.	NSWEC created comprehensive documentation detailing the replication and redundancy processes in place at the main Government data centre located at Silverwater and the secondary recovery site located at Unanderra. This documentation described the services and responsibilities provided by the data centre in relation to the iVote System, such as: Secure Computing Platform (SCP) • Web Application Firewall (WAF) for web servers • File Integrity Monitoring • Cloud based DDOS protection • SIP Trunking. A test of replication and redundancy was undertaken across the entire platform before live voting commenced. This test informed NSWEC that in the event of an issue with the primary data centre, the service could be replicated to the secondary site, without interruption to voting. Included in this testing was the successful emulation of a failover from the primary data centre to the recovery location. Documentation of the detailed testing and results was reviewed by PwC as part of this review.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
2.2	**The process for monitoring, assessment and defence of the core voting system has not been detailed and documented** NSWEC intend to use internal and external monitoring solutions to validate the integrity of the system during voting, however the process of monitoring has not been formalised or documented. NSWEC expect to use a specialist security organisation to perform monitoring, however they are yet to define what monitoring solutions will be used, the frequency of monitoring and how incidents will be raised, escalated and addressed. There are also a number of internal NSWEC solutions that will support the system monitoring process; the scope of activity these solutions will monitor is also yet to be defined and the process of tuning these solutions to factor in false positives and low level events has not taken place.	NSWEC implemented a number of internal and external defence, logging and monitoring controls that continuously tracked and reported any threats to the iVote system during live voting. These were: • A Security Operations Centre (SOC) at the specialist third party security provider's facility in North Ryde to receive log feeds from defined iVote infrastructure and application nodes. This was manned 24/7 and regular daily updates were provided to NSWEC. • A Network Operations Centre (NOC) maintained by Secure Logic that monitored the iVote Core Voting System hosting environment. • NSWEC logging and monitoring applications, including Splunk (the primary repository for all log feeds), PIWIK, Monitis and Nimsoft. A document detailing the above controls, monitoring procedures, incident management, escalation procedures and key contacts was created and shared with all parties prior to live voting. A number of incidents were reviewed by PwC to confirm that they were reported to the NSWEC Chief Information Officer (CIO), for resolution and closure.
2.3	**The process to secure the system during voting has not been detailed, documented and tested** During voting the system is locked down so that only authorised individuals may gain access; however the lock down process has not been formally detailed and fully documented. Additionally NSWEC intends to automate the lock down process, but as it is yet to be detailed and fully documented and planned testing has not yet been scheduled.	NSWEC created and documented a system lock down procedure, *'iVote – Lock Down Procedures Manual v1.2'*, prior to live voting. The document outlined the high level requirement to lock down access to the system during live voting, in order to prevent unauthorised access, and the detailed tasks involved for each stage. The high level process consisted of the following steps: • Initiation from the NSWEC CIO • Split passwords for access to the management server • Passwords stored in a tamper proof bag under custody • Oversight and coordination from the NSWEC CIO and CIO of Secure Logic to validate the process. Additionally the process was independently observed as part of this review, see report section3 observation 2.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
2.4	**End to end testing of all critical scenarios must take place before live voting** A testing schedule is in place prior to the system being used in a live election. At the time of the review incremental software releases were still occurring, as such testing of end to end scenarios has not been fully completed. A test plan, process, scripts and team are in place to execute end to end testing once the final version of the code is delivered.	End to end testing was undertaken with each incremental software release, and additional testing took place during the final software release in the week of 9 March. In addition, after code freeze and lockdown but before going live for the election, a final Logic and Accuracy Test (L&A) end to end test took place with the final election build and configuration. L&A testing processes were observed as part of the Post-Implementation Review, see report section 3, finding 4.
2.5	**An Incident Management reporting process has not been detailed or documented** NSWEC have yet to define and document an incident management process in the event of a security issues or other such event that may impact the core voting system during voting.	NSWEC created an Incident Management Policy and Procedure before the commencement of live voting - '*NSW Electoral Commission iVote Project Incident Reporting Procedure*'. This was shared with all third parties who provided iVote services to ensure NSWEC were notified of any potential incidents in line with the agreed SLAs. The document detailed: • Situations that may initiate an incident • Format of the incident report • Escalation • Approvals. This document was supported by an Incident Report Document that required completion and submission to the NSWEC CIO in order to evoke resolution activities.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
3.1	**Improved structure required to support the go-live readiness planning** Accountability for the decision to cutover lies with the Project Director and Project Delivery Manager, in consultation with the Project Sponsor and other Steering Committee Members. Decision makers will require an objective fact driven approach to understanding the readiness of the iVote and the business. The project has outlined a detailed list of activities to be completed in the lead-up to the iVote system go-live decision, including named resources and effort required to complete each activity. However, governance arrangements to support the assessment (including checkpoints, escalations and timings) and criteria to assess the readiness of the iVote system have not been clearly documented.	A go-live readiness checklist was prepared and updated during daily go live meetings to manage critical activities in the lead up to go live. In addition, the project risk register was updated and reviewed. Project Steering Committee members were informed of progress daily and a formal meeting to review the checklist and risk register and approve a go live decision took place on Wednesday 11 March 2015. Evidence was provided to PwC to support these actions.
3.2	**Planning in relation to detailed cutover tasks is required** The iVote Project cutover is scheduled to take place between Thursday 12th and Monday 16th March 2015. The project has outlined a detailed list of activities to be completed as part of the cutover, including specific individuals assigned to deliver. However, governance arrangements during the cutover window, including communication protocols and key checkpoints and objectives have not been detailed and fully documented.	A detailed cut over procedure was added to the iVote software provider's, Scytl, administration manual. A Logic and Accuracy (L&A) test formed part of the cut over procedure. The Project Steering Committee (PSC) was informed of the results of this final L&A test of the locked down and configured system. NSWEC Contingency Plans included: • An identically configured test environment available for any post locked down testing • A procedure for authorised breaking of the seals on the locked down system in order to reconfigure or apply fixes • Go-live with acceptance of issues that do not affect the integrity of the election • Postponement of go-live to give time for fixing any issues.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
3.3	**A formal contingency plan needs to be developed to address a potential 'no-go' decision** A contingency plan should be developed, outlining the activities and effort required, associated risks and issues, and communications to key stakeholders that need to be distributed in the event that a "no-go" decision is made to cutover to the iVote system. The proposed plan should identify the next most suitable date to cutover. Further, pre-approval should be sought from the Steering Committee ahead of the go-live decision, enabling it to be implemented at short notice. In determining the level of effort required by the project team to enact the contingency plan, considerations should be made as to whether the date of the go-live decision for the iVote system is still appropriate or whether this decision needs to occur earlier.	See management actions in finding 3.2, above.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
3.4	**Updates are required to the project schedule in order to accurately support tracking of project status.** Review of the project schedule identified several areas of improvement: • Several tasks/activities are out-of-date in the schedule, compared to actual dates identified through discussions with the project team; • The schedule does not outline all activities required to be performed by the project team (e.g. detailed steps to the cutover, go-live decision dates), or does not outline tasks to a significant level of detail; • Resources are not assigned to activities/tasks; • The schedule does not maintain an integrated view of all vendor activities at a detailed level; and The schedule does not outline the activities planned beyond the 28th March 2015 when further activities for Release 4.0 will be performed.	NSWEC created detailed election operations process documentation, such as close of poll and encryption ceremony procedures. A go-live checklist was also created to track and action outstanding tasks before live voting commenced. Additional activities to review and implement phase 4.0 of the iVote system took place post live voting. A documented plan was put in place to track these activities and close the final release of software.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
3.5	**Improvements to project status reporting to provide relevant visibility to key governance forums and stakeholder groups.** Review of the Program Board status report highlighted that transparency of key messages and progress of delivery is limited by the presentation approach. The status reports do not include a traffic light status on key project areas and does not provide an objective scale for the allocation of RAG (Red, Amber, and Green) performance rating unique to each health component. Further, the report only outlines milestones dates that have changed, been removed or introduced (without identifying the baseline dates) and does not outline the impact of the changes on existing schedule and the achievement of critical milestones. Discussions with the project team highlighted that the weekly project status reports were stopped in September 2014. This may have increased the risk of business stakeholders having reduced visibility of project delivery issues and reduces the ability for stakeholders to address concerns in a timely manner. The format and notes of the weekly project team meeting minutes is insufficient to appropriately inform the stakeholders of the project's health and status.	NSWEC took note of this recommendation for future projects. This will be considered (as in the iVote project) in the context of a small organisation, where project key stakeholders are often on the Project Steering Committee, who although formal meetings may occur only at key points in the project, are meeting on a regular weekly basis to review all activities.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
3.6	**Instances of incomplete or still to be developed project documentation** The iVote project has broad coverage in relation to ongoing governance and control documentation. Review of a sample of project documentation identified several improvement opportunities: • There was a lack of documented risk management, vendor management and change management processes and procedures; • Documentation was not maintained or updated frequently. This may lead to out-of-date information being relied upon; and • Several key control documents did not exist (e.g. Dependency Register, Resource Management Plan, and Vendor Management). The information captured in these core project documents provides transparency over key aspects of delivery. They confirm that defined governance processes exist to steer the project in the appropriate direction to achieve the desired objectives. It is recommended that the project embeds an increased quality management focus to ongoing project documentation and reporting.	NSWEC have included the improvement opportunities in the close down review of the iVote project.

iVote Pre-Imp Ref	*Findings*	*Action Taken by NSWEC Management*
3.7	**Risk management processes should ensure high risks are identified and reviewed at appropriate governance forums.** It is important that the iVote project team and the Steering Committee have a clear view of the risk profile of the project leading into the cutover. This is required to enable the Electoral Commission to make timely and informed decisions with regard to the project direction and support implementation of effective mitigation strategies. Risk management should remain front of mind for all stakeholders in the lead-up to go-live. Existing and emerging risks should be regularly discussed and reviewed in all key governance forums to ensure mitigating activities are established and are appropriately addressing the risk/issue.	NSWEC performed a risk refresh after the Interim Pre-Implementation Report was issued and prior to go-live.
3.8	**Go-live readiness requires increased formal engagement with business stakeholders** The Steering Committee did not have scheduled meetings between September 2014 and February 2015, having decided instead to meet on as-needs basis. While the project did not operate a formal Steering Committee during this time, the Sponsor and other Steering Committee Members were updated about project status through informal discussions or other Electoral Commission meetings (including the Program Board meetings and Executive Management meetings).	The Steering Committee met formally after the Interim Pre-Implementation Report was issued and prior to go live.

3 Post Implementation Review Findings

This section details the critical tasks that were observed and processes that were reviewed to satisfy the Post-Implementation review scope.

Ref	Observation activity	Finding
1	***Attendance at the Encryption Ceremony*** On 13th March 2015 PwC attended the NSWEC iVote Encryption Ceremony, prior to live voting, in order to witness the encryption process undertaken to encrypt the voting keys required to initiate and close the election. Encrypted keys were created by the election board to initiate and close the election; and to ensure that in the event of an issue or if a voting had to be restarted, this could only be done by a quorum of the election board using their individual encrypted voting keys. Each board member is required to create an encrypted electoral board key using a smart card supported by a strong password that they are responsible for. When the election has ended and the votes are to be decrypted, a quorum of the Electoral Board must do this by each presenting their smart card and password to initiate the process. Detailed documentation was provided to PwC by NSWEC that detailed the process to create the encrypted election keys. PwC understand from NSWEC that Instructions were also provided to Board members with regard to storage and security of their electoral keys.	**No findings noted**

Ref	Observation activity	Finding

2	***Review of the lock down process documentation and observation of the process***
	
	Prior to live voting NSWEC were required to secure iVote to prevent unauthorised access to the system, as this could invalidate or impact the integrity of the voting process. 'iVote – Lockdown Process Procedures Manual, NSW Electoral Commission', provided a detailed guide of how the lock down process should be initiated. The following actions took place to lock down the iVote system;
	
	• NSWEC CIO initiated the lockdown process
	• NSWEC iVote management informs third party support organisations about the beginning of the lockdown process
	• Secure Logic and NSWEC CIO complete lockdown checklist, the following components were included;
	  ○ SCP Physical Environment
	  ○ SCP Platform
	  ○ Data Centre Facility
	  ○ Firewall
	  ○ Management Server
	  ○ Security Cameras
	  ○ Password Management
	• NSWEC CIO and NSW Electoral Commissioner set administration password for the management server and NSWEC CIO set a dedicated firewall password.
	• The split server password is stored in a tamper evident bag under NSWEC custody. If in the event access is required NSWEC iVote Management will open the bag. The dedicated firewall password is held by 3 members of the iVote project team including the NSWEC CIO.
	• Secure Logic CIO and CIO complete and validate lockdown checklist
	• Lockdown process signed and completed
	
	The system lock down was initiated on 14/03/2015 and followed the detailed procedure, outlined above.
	
	PwC was present on 27/03/2015 to observe the unlocking of the system, due to a change that was required to improve the logging of the security monitoring services, in order to improve the performance of the system. The change was raised by NWSEC IT and the supporting third parties; and approved by the NSWEC CIO. The system was re-locked following the change and the process detailed above, was followed throughout.
		No findings noted

Ref	Observation activity	Finding
3	***Assessment and observation of the monitoring processing controls*** A number of monitoring controls were put in place prior to live voting, these were managed by a number of parties, including CSC, Secure Logic and NSWEC; CSC • A dedicated Account Security Manager (ASM) • 24x7 Event Monitoring and Logging of in-scope systems and devices using our Australian based SOC for all in-scope applications and devices • Baseline correlation rules for alerting and notification based on collected logs • Log sources that are collected in Splunk will be monitored after-hours by CSC Security Analysts via direct console access. This will be monitored on a periodic basis and used for further investigation if a SOC event occurs. • The primary function of the SOC is 27/4 WAF monitoring, out of hours monitoring of Splunk and threat intelligence feed. If ancillary devices are unable to be monitored it will not affect the efficacy of the primary monitoring function. • In addition to system monitoring, CSC will provide a feed of global threat intelligence aimed at identifying internet activity that might indicate a potential attack on the iVote system • Access to the NSWEC Splunk dashboards to track events Secure Logic • Server SCP monitoring using specialist solution, Nagios • FIM Monitoring, via the iVote solution provider, Scytl • Web Application Firewall (WAF) logging via Spluk and the specialist security solution, Imperva • Distributed Denial of Service (DDoS) monitoring via the specialist security solution, Imperva • Database monitoring • Network Backbone monitoring using via the specialist solutions, Nagios and PRTG • Secure logic service and appliance logs forward to the Splunk application to enable NSWEC and CSC to monitor activity in real time NSWEC Splunk was implemented as the primary repository of information aggregated from logs created at various levels throughout the iVote system. Various components and data sources were fed in to the Splunk solution to create operational monitoring dashboards for each of the three main iVote components: • Registration System • Core Voting System • Verification Service. Additionally PwC attended the CSC SOC on 24/03/2015 to review the monitoring activity and discuss associated controls and escalation with CSC employees. PwC were also provided with any overview of the Splunk application and dashboards. During observations it was clear that all parties were aware of the response and escalation procedures.	**No findings noted**

Ref	Observation activity	Finding
4	***Review of the Logic and Accuracy testing*** Before the live election NSWEC undertook a test of Logic and Accuracy (L&A) of iVote. Logic and Accuracy testing is the process by which voting systems are configured, tested, and certified for accuracy prior to an election.. NSWEC undertook a simulation of a live election during the L&A testing, using coverage to support every intended voting scenario across all voting parties. The purpose of this test is to verify that the system is properly adding votes to each candidate in the same quantity as the votes were manually entered. The system result is compared to a known set of data and must match. NSWEC created detailed process documentation describing the process and records of the tests undertaken were created to support the L&A testing.	**No findings noted**
5	***Observation of the close of poll processes and Decryption Process*** Following the election end and voting suspension at 18:00hrs on 28/03/2015 PwC were present to observe the close of poll processes. This included; • Suspension of the web and phone voting systems. **Note the iVote web application allows users a grace period of one hour, therefore any user active user at 18:00hrs could continue their vote until 19:00hrs.** • Closing of the ballot boxes • Download the ballot boxes to secure encrypted USB drive • Add the downloaded ballot boxes to the offline voting machine • Vote cleansing A fully documented procedure detailing each step in the process was provided by NSWEC. Additionally, once close of poll processes were complete, NSWEC initiated the decryption process, which involves the process to decrypt votes from the core voting system (CVS) for counting and in order to compare these to the votes held by the verification service. The Verification Service votes were independently hosted by a third party, AC3. A member of the AC3 team was required to download the verification service votes using a NSWEC laptop to access the verification service application. The downloaded votes were then copied on to encrypted USB drives that were stored in tamper evident bags and placed in locked storage. The votes from the CVS were downloaded from the remote ballot box, in order for the following processes to take place; • Cleansing • Decryption • Reporting • Re-Encryption The decrypted votes were then copied on to encrypted USB drives that were stored in tamper evident bags and placed in locked storage. The first-preference results were then uploaded to the Election Management Application	**No findings noted**

Ref	Observation activity	Finding
6	***Attendance at the Decryption Verification Ceremony*** To enhance the security of iVote, two copies of the encrypted votes are created. One copy is sent to a Verification Service and another copy is stored on the Core Voting System (CVS). Following the end of voting on the 28/03/2015, NSWEC re-encrypts the votes from the CVS and compares these votes with those held by the verification service, to ensure they match. To ensure all procedures are followed and to validate the process, the re-encryption and comparison process was repeated by independent third parties at 17:00hrs on the 01/04/2015, with PwC and a number of party scrutineers present to observe the process. The encrypted Verification Service votes and the decrypted votes from CVS were stored on secure USBs in tamper proof bags and stored in locked cabinets prior to the Decryption Verification Ceremony. PwC took custody of the tamper proof bag tear away reference strips to ensure chain-of-custody and that they had not been opened prior to the ceremony. The votes held by the verification service are encrypted; therefore the votes held by the CVS have to be re-encrypted using the same keys before the votes can be compared. These encryption routines are undertaken by NSWEC, plus a number of independent third parties are invited to undertake these tasks in parallel. The independent third parties were required to meet the following criteria in order to undertake this tasks; • Knowledge of the systems development and java • Understanding and experience of cryptography and programming Expressions of interest were submitted and, following a review by NSWEC, two parties were selected; • Computer Scientist and PHD candidate • Computer Scientist A procedure document was created to support the process. PwC observed the process and that the independent third parties confirmed the votes from the Verification Service matched the decrypted votes from CVS.	**No findings noted**

4 iVote Incidents

This section provides an overview the logged incidents that took place during voting, the impact and the current status determined by NSWEC.

Incident	*Description and Impact*	*Status (determined by NSWEC)*
Incorrect Legislative Council virtual ballot	The iVote system is configured using an electronic specification file generated within the NSWEC Election Management Application (EMA). This file is in a standard format called Election Mark-up Language (EML) and specifies all the attributes of the election, such as districts, candidates, groups for both LA and LC contests. The EML included an incorrect specification for the LC ballot which resulted in an inability for iVotes to be cast above the line for Groups B and C.	Closed
Registrations database server reconfiguration	Registrations increase on 16 March caused performance issues so DB was reconfigured	Closed
Fixes to Core Voting System	Splunk server was unresponsive due to a rogue job creating over 300,000 directories on the system drive, which was impacting the underlying O/S and the responsiveness of the Splunk server	Closed
Piwik service removal	Piwik was exposed to be susceptible to a 'FREAK' attack on Friday 20th and NSWEC removed the use of Piwik on Saturday 21st March	Closed
Fix time service issue	Time discrepancies were observed between various servers in the core voting environment and would have caused votes to be rejected if not addressed	Closed
Fix CVS IVR Issue	Caller unable to vote by phone – resolution required a restart of the iVote_PROD_Voice IIS service	Closed
Verification Service changes	Fix signature file, which was preventing verification Change application logging level Fix issue extracting votes from the verification service	Closed

Incident	*Description and Impact*	*Status (determined by NSWEC)*
CVS Database Diagnostic Analysis	Lockdown was removed for Scytl to make performance improvements to the CVS database because test downloads of the ballot box were taking many hours more than expected.	Closed
EMA interface for multi vote removals	EMA failure when processing file of electors who had voted using or registered for the iVote system	Closed
PIN hashes re-encrypted in Reg/CM	CVS had created a new symmetric key in error and when this was identified, the encrypted PIN hashes within registrations had to be decrypted and re-encrypted using the new key	Closed
CVS voter activity failure	At close of election it was found that a significant number of voter activity messages were unsent within CVS, which required a manual update to CM	Closed
Issues raised by Vision Australia	Several incidents throughout the election period which negatively impacted on the Blind Low Vision community	Closed

Appendix A Consultations

The individuals holding the following titles were consulted as part of this engagement:

Position / title
NSW Electoral Commissioner
NSWEC Chief Information Officer (CIO)
NSWEC Director Elections
NSWEC iVote Delivery Manager
NSWEC Consultant
NSWEC Test Manager
NSWEC Tester
Third party providers

pwc.com.au

Final