

# 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

Issued by Dr Richard Adams

## Contents

Background to the Audit .....	3
Audit Assessment .....	3
Assessment Scope .....	3
Procedures Performed.....	3
Limitations.....	4
Attendance.....	4
Observations.....	4
Comments and recommendations.....	8
 <b>Appendix A – Overall process .....</b>	<b>9</b>
 <b>Appendix B - Information Sources .....</b>	<b>10</b>

## BACKGROUND TO THE AUDIT

The Western Australian Electoral Commission (**WAEC**) (**the Auditee**) plans to introduce technology assisted voting within the 2017 WA State General Election (**SGE**). A requirement for this solution is for an independent third party audit (**the Audit**) to provide confidence that the output of the IVR Voting System (**iVote**) is an accurate reflection of legitimate votes cast using that system and that the information contained within the iVote system remains secure at all times.

Another component of the Audit is for me (**the Independent Auditor**) to provide recommendations to the Electoral Commissioner to reduce or eliminate any risks that could affect the security, accuracy or secrecy of voting.

### Solution Overview

The WAEC has come to an agreement with the New South Wales Electoral Commission (**NSWEC**) to base the iVote system on the NSWEC's iVote system, with customisations. As such, a significant portion of the development, testing and troubleshooting work has already been performed by the NSWEC. The WA iVote system solution is summarised in Appendix A.

At a high level, voters will be able to remotely complete online votes by accessing the Core Voting System and casting their votes. Once cast, there is the ability for an individual to contact the WAEC and have their votes removed or changed prior to close of the polls. After polls have closed, the entries in the two databases are compared and audited for integrity.

## AUDIT ASSESSMENT

I have reviewed the processes and systems used for iVote.

A key consideration has been whether the work undertaken by the auditors for the NSWEC on their system needed to be repeated. On reviewing the documentation produced by PwC I decided that there was no need to re-visit the key elements of the system covered by their reports but to note the exceptions and comments in their final report.

I have focussed on the differences between the system used by NSWEC and that developed for WAEC based on the two documents; WA Electoral Commission iVote Core Voting System Statement of Work and WAEC iVote Registration System changes. My review of these documents leads me to conclude that there are no fundamental changes likely to effect the operation or security of the underlying system produced for WAEC.

Having reviewed all the documentation provided by the WAEC and having observed the L&A Testing as well as the Decryption/Ballot Paper Print/Reconciliation I am of the opinion that the output of the Core Voting System (**iVote**) is an accurate reflection of legitimate votes cast using that system and that the information contained within the iVote system remains secure at all times. During the course of my work I have made several findings together with recommendations for consideration by the Electoral Commissioner that are included at the end of this report.

## ASSESSMENT SCOPE

The following services were considered out of scope for this report and were reviewed by other parties:

- Cryptography
- System architecture.

## PROCEDURES PERFORMED

My assessment is based on observation and the information provided by the Auditee that consisted of the following:

- Documentation review
- Process walkthrough
- Discussions with relevant parties

## LIMITATIONS

- I have not attended the NSWEC facilities or observed any walk-throughs from that location.
- I have not observed security incident management testing
- I have not attended the disaster recovery site

## ATTENDANCE

I have attended the following events

Date	Comment
15 November 2016	System overview and run-through
12-15 December 2016	Preliminary Meetings
1 February 2017	Observe DR cut-over test
16 February 2017	iVote CVS and Verification Lockdown. Creation of iVote Electoral Board. iVote Logic & Accuracy Tests.
17 February 2017	Unlock CVS. Prep and make configuration changes, Logic & Accuracy Tests
24 February 2017	Unlock for IVR race condition fix.
12 March 2017	Decryption Ceremony
13 March 2017	Observe CVS server unlock process

## OBSERVATIONS

### 1. General

- The Defined Impact and Likelihood criteria have not yet been established to assess risks at the WAEC. In addition, the WAEC Risk Register does not accurately describe the identified risks. These issues are outstanding from earlier work undertaken on the Risk Register that was put on hold while preparations were made for the State election of March 2017.

### 2. Lockdown process – 16 February 2017.

There were deviations from the Lockdown Procedures Manual, specifically:

- Neither of the items in Section 7.1.2 (SecureLogic Admin Accounts) were verified and signed off (account names listed as “?????”)
- Neither of the items in Section 7.1.3 (site-to-site VPNs) were verified and signed off.
- The item in Section 7.1.4 (Whitelisting) was not signed off.
- The item in Section 7.1.5 (iVote Local Domain User Accounts) for the NSWEC CIO to reset the ivote\_admin password was not signed off. The service account was also listed to be disabled but was left active – this appears to have been an error in the Procedures as disabling the account would have adversely affected the functioning of the iVote system.
- Neither of the items in Section 7.1.7 (RDP lockdown) were verified and signed off.
- Items 1, 2, 3 & 6 in Section 8 (Lockdown Validation) were not verified or signed off.
- An additional procedure was carried out on the basis that it replaced the requirements of Section 7.1.1. but was not documented beyond a hand-written note and was not signed off.
- Despite disabling accounts in Active Directory it was necessary to manually disable them in a console session. As far as I am aware the reason for this has still not been identified.

The response I later received to the specific comments made above suggests that the relevant lockdown documentation needs amending.

A further concern during this Lockdown Process was a document entitled 'Login Credentials.xlsx' that was located on the desktop of the machine being used for part of the lockdown process. My proxy in NSW was able to verify that it contained no iVote-related credentials but this is a concern in relation to general security awareness and practice. The response I later received on this matter did not suggest that a 'credential' document such as this was against the Company policies and procedures and should not have been on the laptop.

### **3. iVote Logic & Accuracy Tests – 16/17 February 2017**

There were four issues identified relating to iVote process errors:

1. Audio files not playing on the Web
2. Mobile device and browser login failures
3. An error in LC data entry
4. The IVR system closing the call prematurely

These items were addressed as follows:

1. Audio files not playing on the Web – found to be an error in conversion of sound files such that the required MP3 versions of the sound files were not uploaded. MP3 versions created and uploaded.
2. Mobile device and browser login failures – identified as an extra security feature that had been added to a script. The script was edited. This causes no loss of security as the protection it was intended to provide is handled elsewhere.
3. An error in LC data entry – identified as 'user error'.
4. The IVR system closing the call prematurely – suspected of being a timing issue and addressed (although not completely fixed) through a minor script modification that introduces a delay in part of the process. At worst case a receipt is generated for a vote cast but is not issued to the voter.

There were also five discrepancies between the actual ballot box data and the expected results. These all related to the accuracy of the input data, i.e. human input errors. The anomalies could show that the system performed as expected and that errors could be traced using the logging that forms part of the iVote system.

### **4. Unlock process 17 February 2017**

It was necessary to unlock the CVS to make changes in a script to address the inability to access the iVote web page from tablet and smartphone devices. Witnessed and video recorded.

### **5. Unlock process 24 February 2017**

It was necessary to unlock the server associated with the IVR system to make changes to a script to address a 'race condition'. Witnessed and video recorded.

### **6. Decryption Ceremony 12 March 2013**

The process in general ran very smoothly, the only exception to the standard process was the provision of a Receipt Server by WAEC due to the intended server not being included in the latest production patch. This server contained no sensitive information as it simply held a list of receipts so that the electorate could confirm that their vote had been received.

The time allocated for the printing of the iVote ballot box contents and reports exceeded the estimate. The paper-based process had been paused to allow the iVote output to be slotted into the main process while maintaining sequential batch numbers for the iVote output. The effect of having to re-start the paper-based process while iVote was still printing was that the iVote batch numbers were not sequential, thus requiring a report to be generated and cross-referenced to ensure no batches had failed to print.

## **7. Unlock process 13 March 2017**

The account 'ivadmin' that was deactivated during the lockdown process of 16 February 2017 was found to be active during the unlock process.

Item 1.4 of Post-election checklist for Removal of Lockdown is to confirm that all non-essential accounts for the iVote CVS system are still disabled. However, despite the Active Directory view showing the account 'ivadmin' to be disabled, on further checking via another method (command shell) the account was still shown as 'active'.

All other accounts were checked and verified to be in the correct state.

A request was made for an explanation from the relevant service provider but the explanation given was not satisfactory and this issue needs reviewing.

## **8. Logging in the IVR process.**

At present, there is data being recorded in some of the IVR logs to the extent that there is the potential for a voter's preferences to be determined through comparison of their navigation process and the appropriate ballot paper. The individual voter cannot be identified based on the log information. This data is not required for diagnostics and the logging should be reduced to major events such as the completion of preferences. (The data has now been cleansed following the Election).

## **9. Outstanding modifications to the DR system.**

The browser login fix (item 2 in the iVote Logic & Accuracy Tests – 16/17 February 2017) still needs to be applied to the DR system. This will be accomplished through an addition to the DR cut-over process when the DR system is unlocked.

## **10. USB failure**

The reliance on secure USB devices to transfer files between the Bridging Laptop and the Offline Machine has the potential to disrupt some of the iVote processes through corruption of essential files. This has already happened during a test of the decryption process on the DR system.

## **11. External communications**

(a) A letter received by Mr David Kerslake on 16 February 2017 raised the following key security issues:

1. The inclusion of Incapsula to provide proxy services for mitigating DDoS and other external attacks on the iVote systems exposes voter's details and their preferences such that they may be viewed and/or manipulated.
2. The casting of a vote using the iVote system is not verifiable.
3. The source code for the iVote system should be made publically available to ensure security through identification of potential weaknesses achieved through the use of many people reviewing the code.

(b) With regards to **Point 1** there are two aspects to voter's data, their personal details and their vote itself. It is the case that voter details may exist in unencrypted form on Incapsula servers (refer to (e) below) but this data is only transient.

(c) In relation to the second aspect of voter's data transiting through Incapsula systems, the vote itself, the statement was made that "This encryption is only as trustworthy as the server providing the code" and suggests that it would be possible to modify votes cast. This might be the case if the vote information

passing through the Incapsula Servers was only encrypted using their credentials but this is not how iVote is configured.

- (d) In the paper 'A cryptographic overview of the iVote 2015 voting system' (Brightwell et al, 2015) it states that there are two separate 'envelopes' into which the ballot data is placed in encrypted form. Two separate processes are used to encrypt the ballot data and the keys required to unlock this data are not held by Incapsula, therefore they would be unable to look inside the envelopes to view or manipulate the ballot data as it passes through their servers. In addition, the contents of the two envelopes are compared within the iVote system to make sure that their data is the same and that the vote is valid.
- (e) It is my view that the chance of gaining access to the Incapsula systems is very small given their industry standing, reputation and security profile. It is even less likely that someone would be able to gain access to Incapsula systems, identify the data being used in the iVote system and monitor/record voter registration details.
- (f) In my view it is on the outskirts of probability for someone gaining access to Incapsula systems, identifying the data being used by the iVote system and then being able to decrypt one of the ballot envelopes (just to view the data) or decrypt both of the ballot envelopes (to change the data) bearing in mind the limited 'window of opportunity' provided by the iVote session.
- (g) With regards to **Point 2**, in the Halderman/Teague Paper the two authors identified a security vulnerability through the use of a third-party provider of analytics services (Piwik). They specifically identified threats from 'FREAK' and 'Logjam' attacks but both required the compromise of the Piwik servers. These Piwik servers are no longer part of the iVote system so I determine the security vulnerability to have been addressed (failing any new evidence being presented).
- (h) In relation to the specific 'non-verifiable' aspect of Point 2, this is covered in two parts in the Halderman/Teague Paper; simple verification avoidance and using the 'clash' attack.
- (i) The 'verification avoidance' assumes an attacker has control of the iVote system to the extent that they can delay the ballot-submission process such that the voter does not verify their vote which the attacker manipulates and submits. An alternative approach involves directing voters to a fake verification site. Both of these approaches seem to have relied on the obsolete Piwik compromise.
- (j) In relation to the 'clash' attack, this relied upon a compromise approach that again I believe is no longer available.
- (k) For **Point 3**, it is argued that the source code for the iVote system be made available to the public and a reference is made to the findings of a report from the New South Wales Joint Standing Committee on Electoral Matters (REPORT 2/56 – 17 November 2016) (the **JSCEM Report**). However, on reading the Report I think the Committee was addressing the first part of Mr Campbell's comment in 3.36 which suggested not many people took the opportunity to test for flaws, rather than his earlier submission which indicated that there was no guarantee that flaws discovered would be reported and not exploited. I believe the Committee, with no experience in this area, assumed that they had erred on the side of caution by recommending that the source code be made publicly available. I don't agree with that approach.
- (l) My view is that the threats outlined in the correspondence received by Mr David Kerslake on 16 February 2017 are either no longer relevant through the manner described in the Halderman/Teague Paper or have been mitigated to a level where I am comfortable as Auditor.

## 12. Further external communications

- (a) A letter received by Mr David Kerslake on 16 February 2017 identifies a risk that an iVote server is not being protected by the Incapsula proxy service. This seems to have been an issue with leaving access open instead of restricting access just to Incapsula.

- (b) I received notification on 22 February 2017 that this potential vulnerability had been addressed and now all external access to iVote servers is made through Incapsula.


### 13. Splunk dashboard timing issues

Due to time differences between the NSW systems and the local systems many figures shown on the dashboard of the monitoring system did not reflect the current state of the iVote system which limited their usefulness.

## COMMENTS AND RECOMMENDATIONS

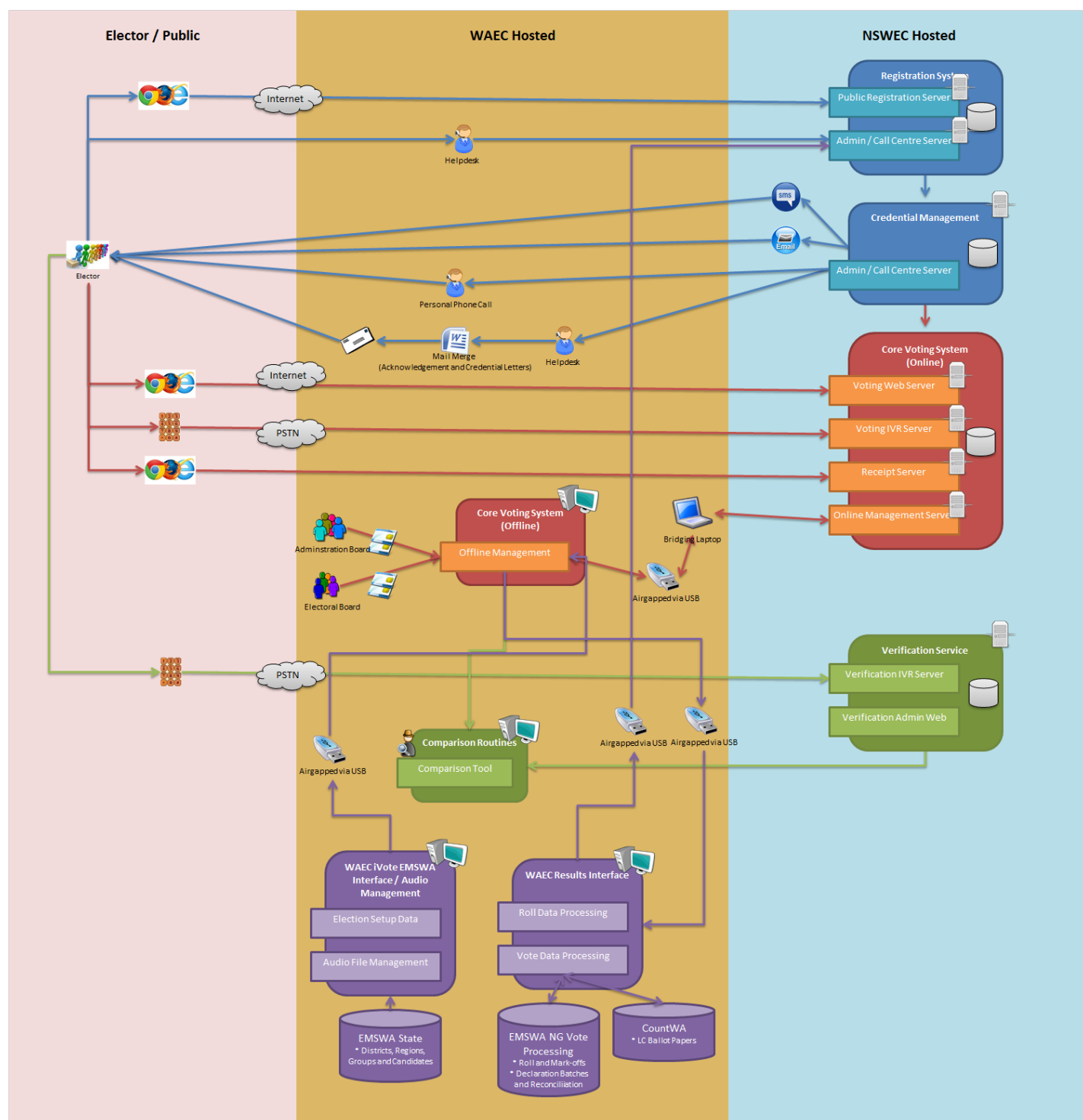
1. Address the outstanding issues with the Risk Register.
2. Ensure that the test plans are prepared prior to production testing.
3. Following my experience with the 16 February Lockdown Process and the Sydney server capable of being accessed outside of Incapsula I have concerns regarding some of the services being provided by third parties, although I don't believe that there has been any real threat to the security of iVote systems for this election.
4. Based on the user entry errors evident in the Logic and Accuracy testing I recommend that this process be reviewed to ensure that all those staff tasked to input data are fully aware of the requirements of their role.
5. Given the failure of the current USB devices and subsequent data corruption I recommend looking at an alternative process or media for transferring data between the Bridging Laptops and Offline Machines.
6. Given the possibility of reverse-engineering voting preferences through a review of certain IVR logs together with the relevant ballot paper I recommend that this process be reviewed and that only the minimum amount of data necessary for diagnostics is recorded.
7. As the IVR system still has some timing issues I recommend a review of the processes and scripts for handling this method of voting to ensure a more robust solution.
8. Given that it would be impractical to delay the paper-based processing for long enough to finish the iVote batch printing in the current hardware configuration I recommend that other options be considered, e.g. having a dedicated print server to run multiple print queues.
9. Identify and address the issue associated with discrepancies between Active Directory reports and the actual status of an account so that you can be confident of the reported status during lockdown procedures.
10. The lockdown documentation should be reviewed to ensure that any changes are necessary to reflect the existing operating environment and that items are not removed for expediency.
11. I recommend that the security policies and procedures of relevant third parties be reviewed as they relate to the protection of WAEC services, particularly in relation to the setting of server access rights.
12. I recommend that a formal document is produced detailing the procedure for the collection and storage of appropriate logs and reports to confirm the status of the iVote systems during an election.
13. I recommend that a check of systems and devices used during an election are examined to confirm that they have been purged of any confidential data.

I am satisfied that the iVote system used in the WA State Election of March 2017 performed its intended function very well and that the integrity of the system was maintained such that voter information was appropriately protected.

A handwritten signature in black ink, appearing to be 'P. Smith', written on a light-colored background.



## APPENDIX A – OVERALL PROCESS



## APPENDIX B - INFORMATION SOURCES

The following source documentation has been used for this audit.

Document
WAEC iVote Project Risk List (Risk Register)
WA Electoral Commission iVote Core Voting System Statement of Work
137447_2_WAEC iVote Credential Management System changes
137262_2_WAEC iVote Registration System changes
WA iVote Implementation Responsibility Matrix
WAEC Impact Matrix
137262_2_WAEC iVote Registration System changes
137364_2_WAEC_iVote-AuditRequirements_160325
NSWEC iVote Post-Implementation Report FINAL
NSWEC iVote Pre-Imp Draft Report v4.0 FINAL
System Testing Regime, Plans and Results
Disability Cohort Groups for Stakeholder Management & Consultation
Procedures for Technology Assisted Voting
iVote Offline Machine Setup.DOCX
iVote Incident Communications Management Plan – SGE 2017
141220_1_WAEC iVote DR Plan v1.1.DOCX
Incapsula Full-Review.pdf
Geneva mounts e-voting charm offensive - SWI swissinfo.ch_files
14_Scytl EMC_Inquiry_No.6.pdf
iVote NSW hearing.txt
Security Incident Response Plan.docx
SGE2015 Elector Feedback.docx
Administration of the 2015 NSW Election and Related Matters.pdf
Lockdown of iVote CVS and VS for WAEC_minutes.docx
2017-02-10_iVote Registration system lockdown.pdf
Teague iVote analysis 1504.05646
2017-02-16_iVote lockdown_iVote Verification Server checklist_signed.pdf
2017-02-16_iVote lockdown_iVote CVS checklist_signed.pdf
iVote Registration System Lockdown Procedure Checklist
SecureLogic Lockdown Procedures Manual
2017-02-16_iVote lockdown_iVote Verification Server checklist_signed.pdf
Lockdown of iVote CVS and VS for WAEC_minutes.docx
iVote2015official.pdf (Scytl protocol description)
Noted corruption of XML file stopping Cleansing in L+A DR test.docx
WAEC iVote Disaster Recovery (DR) Plan – WA State General election March 2017
iVote Roll Mark-Off – Predictive Mode
Decryption and vote Processing steps - signed
iVote Batch numbers – initialled
CountWA First Preference Reconciliation Summary – initialled
iVote LC First Preference – SG1701 - checked
Legislative Council iVote First Preference Reconciliation summary – initialled
LA First Preference votes checklist - checked
Legislative Assembly iVote First Preference Reconciliation Summary - initialled
Post-election Checklist for Removal of Lockdown