

Australian Electoral Commission

AUDIT OF AEC'S ELECTRONIC VOTING MACHINE FOR BLIND AND VISION IMPAIRED VOTERS.

BMM Australia Pty Ltd

23 August 2007

The content of this document is strictly confidential. It has been prepared by BMM Australia Pty Ltd (BMM) exclusively for the perusal of Australian Electoral Commission and may not be disclosed to any other party without the prior written approval of Australian Electoral Commission

Executive Summary

BMM Australia Pty Ltd has been engaged to perform an audit of the AEC electronic voting machine (EVM) for blind and vision impaired voters to be used in the Australian 2007 federal election.

BMM asserts its independence from the supplier of the system and from any political party.

BMM has been asked to ensure that the EVM meets the following criteria:

- ❑ Resistant to malicious tampering by users;
- ❑ Resistant to malicious tampering by external parties by electronic means;
- ❑ Free from malicious source code;
- ❑ Presents an accurate representation of votes cast in the printed record without variation; and
- ❑ Erases all record of voter's preferences when so instructed by the polling official.

Our findings are as follows:

1. BMM is satisfied that the system design includes features that provide the level of security required by the AEC;
2. BMM is satisfied that the AEC conducted its testing of the EVM with due diligence;
3. BMM found no evidence of malicious source code in the EVM;
4. There were no errors detected in BMM tests for security, accuracy and compliance of the system; and
5. BMM is satisfied that risks identified in this report have been avoided or minimised to a level that would allow the EVM to comply with AEC requirements regarding security, accuracy and voting functionality.

We certify that the AEC Electronic Voting Machine for blind and vision impaired voters complies with the specified criteria.

Peter Dilley

Senior Project Engineer

Data Network and Computer Security

Table of Contents

1	INTRODUCTION.....	1
2	SCOPE.....	1
3	METHODOLOGY.....	1
4	SECURITY FEATURES.....	1
4.1	The Polling Officials Barcode Card.....	2
4.2	2Dimensional Barcode.....	2
5	PROPER USE OF THE SYSTEM.....	3
6	SOFTWARE EVALUATION.....	3
7	TESTING THE EVM.....	4
8	RISK ANALYSIS.....	5
8.1	Security Risks.....	5
8.2	Accuracy Risks.....	7
9	CONCLUSIONS.....	8

1 INTRODUCTION

The Australian Electoral Commission (AEC) is required to trial electronic voting for blind and vision impaired voters at the 2007 Federal election. The system to be used for the trial is provided by the Software Improvements Pty Ltd and is based on eVACS®, the electronic voting and counting system developed by Software Improvements Pty Ltd.

It is an AEC requirement that the software solution is audited and certified by an independent auditor to verify that the system meets AEC specified criteria.

2 SCOPE

The audit of the EVM must ensure that the system:

- ❑ Is resistant to malicious tampering by users;
- ❑ Is resistant to malicious tampering by external parties by electronic means;
- ❑ Is free from malicious source code;
- ❑ presents an accurate representation of votes cast in the printed record without variation; and
- ❑ erases all record of voter's preferences when so instructed by the polling official.

3 METHODOLOGY

The methodology employed by BMM includes the steps outlined below:

- a. Review of system requirements, design documentation and design features;
- b. Risk assessment including identification of areas of risk that could affect security, accuracy or secrecy of the voting machines and associated components;
- c. Review of documentation, AEC test strategy, test cases and test results;
- d. Inspection of source code;
- e. Identification of additional tests of critical functionality and end-to-end testing;
- f. Evaluate operating procedures that are required to minimise risks; and
- g. Form a view as to the compliance of the system with respect to the AEC requirements.

4 SECURITY FEATURES

It is not possible for a computer system to prevent tampering. While physical security can minimise the opportunity for tampering, it cannot be infallibly prevented. Therefore, it is important for the computer system and independent auditors to be able to detect and report on tampering or attempts at tampering with its electronic data.

The AEC BVI EVM system election setup computer and voting EVMs are not connected to a network whether by direct connection, modem or wireless. The EVMs and election setup computers are stand-alone systems. It is therefore not at risk of a network attack or viruses from the internet. The Central Processing Unit is also enclosed in a case. In addition, a polling official's barcode card is required to access the system. These features provide physical security.

Secrecy of the votes is assured by the use of a 2Dimensional barcode and is supplemented by the existing AEC procedures for handling the votes.

4.1 The Polling Officials Barcode Card

The Polling Officials barcode is used to facilitate interfacing at four key areas of the EVM.

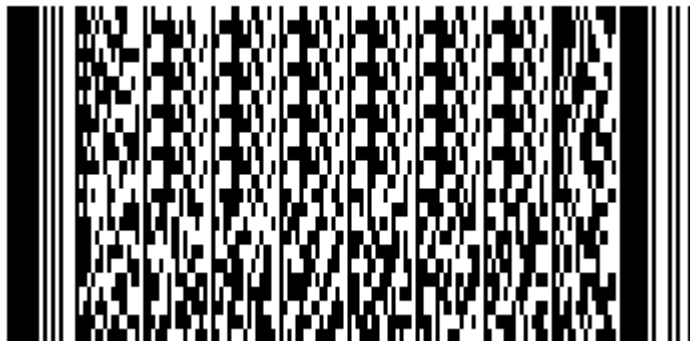
1. On the Welcome screen to bring up the Administration Menu;
2. at the end of a Voting Session to return to the Welcome screen, and remove all vote details from the EVM and printer;
3. at the end of a Practice session to return to the Welcome screen; and
4. on any ballot screen to exit a Voting or Practice Session and return to the Welcome screen.

The Polling Official will most often interface with the EVM for purposes of starting and ending a voting session. The voting session can be broken down into three main parts.

1. Selection by the Polling Official of the relevant State or Territory and Division for the voter;
2. the voter is then able to vote in private until they reach the end-of voting screen and call an Official; and
3. the Polling Official is able to print the votes again if necessary, and then swipe the official barcode to return to the Welcome screen preparing the EVM for the next voter.

4.2 2Dimensional Barcode

For purposes of protecting the secrecy of the voter's preferences, the printed output is encoded in PDF417 format. PDF417 is a 2Dimensional barcode used in a variety of applications, including transport, identification cards, and inventory management.



It is best suited for uses where information needs to move with an item or document. PDF stands for Portable Data File and the PDF417 format was developed by Symbol Technologies. The primary reasons behind the use of a 2Dimensional barcode include the need to store more information than a traditional barcode and represent and having error correction. The PDF417 code can detect and correct erasures, smudges, misprints and other errors, with a configurable amount of redundancy.

Finding: BMM is satisfied that the system design includes features that provide the level of security required by the AEC.

5 PROPER USE OF THE SYSTEM

The security and accuracy of the system will require that the AEC implement the following practices:

- a. Personnel administering any component of the system will be properly trained;
- b. The audit features of the system and procedures will be used to verify the integrity of election data on the created EVM-CD before it is mass duplicated and released for the federal election;
- c. The election setup computer used to create the EVM-CD will be kept physically secure, not connected to a network and protected by passwords;
- d. The DVD ROM media mass-duplication machine and all created EVM-CD discs and polling officials barcode cards will be kept physically secure;
- e. The EVMs will be setup by an authorised technician in the presence of an AEC official and only be allowed to load the EVM-CD software which is provided to the technician by the AEC official;
- f. The physical seals of the EVMs will be checked regularly for evidence of tampering;
- g. Where there is evidence of tampering the EVM will be impounded for investigation and a new EVM machine provided that has been setup using the same safeguards outlined above for new EVMs;
- h. Any person who is issued a polling officials barcode card will keep the card physically secured;
- i. Handling of printed EVM votes will be subject to the same AEC procedures as used for the handling of pre poll votes; and
- j. All media containing the EVM Software and all associated log files will be secured at all times during transportation, usage and that the computers involved with the AEC system will be properly sanitised to ensure that no AEC system software components or logs will remain on the computers for when later used for AEC purposes or released from the AEC for another purpose.

6 SOFTWARE EVALUATION

This refers to the source and executable software provided to The Auditor and the AEC, version 1.5 (AEC D244). The Supplier provided full source code of the system and system design documentation.

Source code inspection focused on the following:

- There is no malicious code that could affect the correct preferences of voters being cast; and
- There is no malicious code that records voter preferences onto the EVM.

It was observed that the source code was maintained in a security-protected source control system and designed, written and documented in a manner that could broadly be described as "industry standard".

Finding: BMM found no evidence of malicious source code in the EVM.

7 TESTING THE EVM

Security of the system depends on its proper use and on correct implementation of the design features mentioned previously. This was demonstrated through extensive testing.

The AEC adopted a testing strategy comprising four stages of testing:

- Shakedown – find as many errors as possible in early releases and resolve misunderstandings about the specification;
- Unit testing – test the operation of the four major modules of the system;
- System testing – test the system as whole; and
- End-to-end testing – simulate a real election to verify the system as a whole and the operational and administrative tasks around it.

The test system was configured with election data that reflected as closely as possible the type of districts, parties, affiliations, candidates and ballot formats expected in a real election.

The AEC executed a large number of test cases for each stage of testing. Test cases included tests of normal operation as well as test of abnormal operation, for example the insertion of invalid base CDs in the election setup phase. Faults were recorded and tracked and tester feedback was recorded in the form of test comments.

Finding: BMM is satisfied that the AEC conducted its testing of the system with due diligence.

Audit testing was directed at independently verifying the operations of various features designed to ensure security and accuracy. Particular functionality tested included:

- The Setup Election Module would not generate EVM-CDs with missing or incomplete data;
- The Setup Election Module would log all access events leaving an audit trail;
- EVMs would not allow multiple vote sessions without the Polling Officials barcode being swiped and the previous voting session closed and a new one opened to the Welcome screen;
- EVMs are setup in a secure manner with the internal hard disk of the EVM computer erased prior to the installation of the voting system files;
- EVMs will only commence voting functions when an authorised Polling Officials' barcode card is swiped and configured to accept votes;
- Votes would not be lost if power is removed from the EVM for a short time due to a dedicated UPS;
- EVMs can recover from power failures;
- EVMs do not store information that could identify individual voters;
- EVMs stores sequence numbers on additional vote preference printouts;
- EVMs display ballot forms correctly and audio messages are not misleading;
- A voter can enter valid preferences or cast an informal vote;
- A voter can correct mistakes prior to confirming and casting a vote;
- The printed ballot can be decoded by using the decoder module whilst being in various states of damage; and
- Printed ballots contain preferences as specified by the voter.

Finding: There were no errors detected in BMM tests for security, accuracy and compliance of the system.

8 RISK ANALYSIS

This table below lists identified risks and documents how the system avoids the risk or how the AEC and the Auditor were able to confirm that the risk is minimised to an acceptable level.

8.1 Security Risks

#	Risk	Treatment
S1	Viruses or malicious code could be installed onto the boot sector or file system of the EVM.	<i>EVM Hardware has been delivered directly into secure storage. EVMs initially boot from an EVM-CD, the internal hard drive is erased and the contents of the EVM-CD are copied to the internal hard drive which is subsequently used to boot the EVM. The EVM-CDs are provided by authorised AEC personnel to technicians who set up the EVM. The EVM is then sealed in a Perspex case and security seals placed on the case to provide additional levels of physical security. Once sealed, the EVM is inaccessible to install further software. The EVM is not connected to any network and access is available only through a limited telephone keypad input device and the Polling Officials barcode scanner input device.</i>
S2	The approved Candidates data upon which the EVM-CD is created from could be substituted by an incorrect or unauthorised version.	<i>The approved candidate data will be supplied directly from AEC core system that also provided information for the development of the ballot paper. The AEC has a procedure in place to manually test the created EVM-CD to ensure the correct ballot information and matching audio is correct and free from error before mass duplication of the EVM-CD and its eventual distribution.</i>
S3	The approved Referendum data upon which the EVM-CD is created from could be substituted by an incorrect or unauthorised version.	<i>The approved referendum data will be supplied directly from AEC core systems. The AEC has a procedure in place to manually test the created EVM-CD to ensure the correct ballot information and matching audio is correct and free from error before mass duplication of the EVM-CD and its eventual distribution.</i>
S4	The approved Audio data upon which the EVM-CD is created from could be substituted by an incorrect or unauthorised version.	<i>An AEC official will observe the recording of the candidate names. The AEC has a procedure in place to manually test the created EVM-CD to ensure the correct ballot information and matching audio is correct and free from error before mass duplication of the EVM-CD and its eventual distribution.</i>
S5	The approved EVM-CD from which the EVM are initially setup from could itself contain malicious code.	<i>Inspection of relevant source code found no evidence of malicious software. The EVM setup CD will be transported according to existing internal AEC procedures and only this CD will be used to install on the EVM machines.</i>

S6	An unauthorised person could cast a vote on an EVM.	<i>Voters access EVMs through polling centres via standard AEC procedures for voters at polling centres. Printed ballots are handled using existing pre poll procedures and unauthorised votes are removed prior to the time of scrutiny and not included in the count.</i>
S7	A person authorised to cast a vote could cast more than one vote.	<i>Voters access EVMs through polling centres via standard AEC procedures for voters at polling centres. Printed ballots are handled using existing pre poll procedures and unauthorised votes are removed prior to the time of scrutiny and not included in the count. In addition, the voter needs to have the EVM setup with a new voting session by an AEC official who has the Polling Officials barcode card.</i>
S8	The recorded votes by the EVM could be substituted by a modified set of votes either in the EVM or in their transit to the AEC office.	<i>Encoding functions of the 2Dimensional barcode ensure that the printed ballots reach the AEC decoding location in a private and secure fashion. Once decoded, the votes are handled through standard AEC procedures as for pre poll voting. The EVMs themselves do not store any votes.</i>
S9	The recorded votes by the EVM could be subtly modified to change preferences or the number of votes.	<i>Encoding functions of the 2Dimensional barcode ensure that the printed ballots reach the AEC decoding location in a private and secure fashion. Once decoded, the votes are handled through standard AEC procedures as for pre poll voting. The decoding process will be managed by AEC personnel supervised by scrutineers as per existing processes.</i>
S10	An unauthorised list of candidates, political affiliations or ballot design could be loaded onto an EVM to trick voters into certain voting patterns.	<i>The AEC has a procedure in place to manually test the created EVM-CD to ensure the correct ballot information and matching audio is correct and free from error before mass duplication of the EVM-CD and its eventual distribution. All data comes from AEC core systems.</i>
S11	Unauthorised persons could decipher and read the contents of an "electronic ballot".	<i>Ballots must be decoded using the Decode CD created during the election setup. This CD is to be kept secure by AEC personnel. Printed ballots are stored in ballot boxes with other votes and are subject to existing physical security applied to ballot boxes.</i>
S12	Information captured by the EVM could be used to identify which individual cast a particular vote.	<i>EVMs do not record any information that identifies a voter. When the ballots are decoded by AEC personnel, they are then handled according to already existing AEC procedures for pre poll ballots to protect the secrecy of the votes through separation of the votes from the information stored on the declaration envelope at the counting location.</i>
S13	An unauthorised person could enable or disable voting on an EVM.	<i>Administrative functions are accessed only through use of the Polling Officials barcode card. There are physical redundancy measures in the forms of spares and back ups.</i>

8.2 Accuracy Risks

#	Risk	Treatment
A1	Preferences recorded electronically on the EVM could be different to preferences entered by a voter.	<i>This was extensively tested by the AEC. Additional testing by the Auditor found no instances of preferences being recorded or recalled incorrectly.</i>
A2	The EVM could mislead the voter as to whom preferences are being given.	<i>This was extensively tested by the AEC. Audio messages matched the text messages. Recorded preferences matched the users' screen touches or button presses.</i>
A3	The EVM may not allow a voter to enter valid preferences or to correct mistakes.	<i>This was extensively tested by the AEC. Testing by the Auditor showed that the software allowed correct entry of preferences and correction of mistakes prior to confirmation and casting a vote.</i>
A4	One or more votes could be lost in the EVM computer.	<i>In AEC and Auditor tests no votes were stored inside the EVM computer. All tests of entry of preferences and recall of preferences additionally showed no loss of votes while a voting session was being conducted.</i>
A5	A voter may not be able to tell whether or not their vote has been successfully recorded.	<i>Text and audio messages are given indicating that a vote has been successfully recorded whilst being printed. If in doubt a voter can ask an election official to check the status of his or her vote in the printer. If the printer does not contain the printed vote, the election official can reprint another copy.</i>
A6	When the votes are decoded after the election some votes may be dropped or duplicated.	<i>The AEC processes the decoded votes using the same procedures in place for pre poll voting. Barcodes will enter the count like all other declaration votes. Once decoded, they will be stapled to the ballot paper and added to the rest of the count. This process meets the existing AEC controls to stop duplication or loss of votes during the counting process.</i>
A7	In the event of EVM hardware failure some electronically stored votes may be lost or corrupted.	<i>EVMs do not store votes. Votes are printed in encoded barcode format and processed by the AEC using procedures already in place for handling remote voting. In the event of complete failure, a paper ballot will be issued.</i>

Finding: *BMM is satisfied that risks identified in this report have been avoided or minimised to a level that would allow the EVM to comply with AEC requirements regarding security, accuracy and voting functionality.*

9 CONCLUSIONS

Following the audit activities outlined in this report, the Auditor was able to make an informed appraisal of the -AEC Electronic Voting Machine compliance with AEC requirements.

1. BMM is satisfied that the system design includes features that together can provide the level of security required by the AEC.
2. BMM is satisfied that the AEC conducted its testing of the system with due diligence.
3. BMM found no evidence of malicious source code in the -AEC system.
4. There were no errors detected in BMM tests for security, accuracy and compliance of the system.
5. BMM is satisfied that risks identified in this report have been avoided or minimised to a level that would allow the AEC system to comply with AEC requirements regarding security, accuracy and voting functionality.

As a result of the evaluation BMM believes that properly used, the AEC Electronic Voting Machine complies with the specified AEC requirements.