

## **Australian Electoral Commission**

### **AUDIT AND CERTIFICATION OF A REMOTE ELECTRONIC VOTING SYSTEM FOR OVERSEAS AUSTRALIAN DEFENCE FORCE PERSONNEL**

**BMM Australia Pty Ltd**

**14 September 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 remote electronic voting system for overseas Australian Defence Force (ADF) personnel to be used in the Australian 2007 federal election.

The software solution for providing the remote electronic voting system for overseas ADF personnel is called eLect.

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

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

- Resistant to malicious tampering by users;
- Resistant to malicious tampering by external parties;
- Free from malicious source code;
- Presents an accurate representation of votes cast in the printed record without gain or loss; and
- Does not allow the association of a voter with the vote cast.

Our findings are as follows:

1. BMM is satisfied that the eLect system implementation includes features that provide the level of security required by the AEC;
2. BMM is satisfied that the eLect system has been tested with due diligence;
3. BMM found no evidence of malicious source code in the eLect system;
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 eLect system to comply with AEC requirements regarding security, accuracy and voting functionality.

We certify that the AEC remote electronic voting system for overseas Australian Defence Force personnel complies with the specified criteria.

Anna Fernando

VP – Technical Services

## Table of Contents

1	INTRODUCTION.....	1
2	SCOPE.....	1
3	METHODOLOGY.....	1
4	SECURITY.....	1
5	SOFTWARE EVALUATION.....	2
6	SOFTWARE CONFIGURATION.....	2
7	TESTING THE ELECT SYSTEM.....	2
8	LOAD TESTING.....	3
9	PROCESS & PROCEDURES.....	4
10	RISK ANALYSIS.....	4
10.1	Security Risks.....	5
10.2	Accuracy Risks.....	6
11	CONCLUSIONS.....	7

## 1 INTRODUCTION

The Australian Electoral Commission (AEC) is required to trial remote electronic voting for overseas Australian Defence Force personnel at the 2007 Federal election. The eLect system to be used for the trial is provided by Registries Limited.

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

## 2 SCOPE

The audit of the eLect system must ensure that the system:

- Resistant to malicious tampering by users;
- Resistant to malicious tampering by external parties;
- Free from malicious source code;
- Presents an accurate representation of votes cast in the printed record without gain or loss; and
- Does not allow the association of a voter with the vote cast.

## 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 solution;
- 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

eLect is installed on servers housed in AEC's secure data centre in Canberra with access only allowed to specified and security cleared AEC personnel, or escorted supplier staff for support reasons. ADF personnel access eLect over the Department of Defence's (DoD) intranet, the Defence Restricted Network (DRN) via the Intra-government Communications Network (ICON). Traffic over ICON is hardware encrypted;

Security of the DRN, ICON and the AEC data centre is outside the scope of this audit.

## 5 SOFTWARE EVALUATION

This refers to the source and executable software provided to the Auditor and the AEC. 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; and
- There is no malicious code that records voter preferences onto the database.

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 eLect software.***

## 6 SOFTWARE CONFIGURATION

The software reviewed by BMM consists of the following:

Software component	Md5
electSenateSwing.jar	446f0337e05db0f98ccabfef43ad2669
VoteEncryptor.class	00d9cab058795711a4aaf3edeadb5f6
egad.jar	7c5ca939979a8ffc131f3c0a40694b80

## 7 TESTING THE ELECT SYSTEM

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

Testing was performed by four different organizations:

- Everyone Counts
- Registries Limited
- Australian Electoral Commission
- Department of Defense

The Testing strategy comprised the following:

- Unit Testing – Everyone Counts
- Integration Testing – Registries Limited
- Business Functionality Testing – Australian Electoral Commission
- Communication, network performance and end user testing – Department of Defense

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 test cases that covered business functionality of the system. Faults were recorded and tracked and tester feedback was recorded in the form of test comments.

Audit testing was directed at end to end testing and independently verifying the operations of various features designed to ensure security and accuracy.

Particular functionality tested included:

- The system can be configured to cater for all required electorates and candidates for the Senate and House of Representatives;
- The configuration can only be modified by authorised persons;
- The system can be opened and closed for pre-election and election day voting;
- Voting is only possible when the system is open for voting;
- Unauthorised users are not able to access the system;
- A voter is able to cast a vote according to his or her preferences;
- A voter can navigate through the screens to cast a formal or informal vote for each house;
- A voter can correct mistakes prior to confirming and casting a vote;
- Voter preferences are accurately, anonymously and securely stored on the server;
- Votes can only be decrypted by authorised persons;
- Voter anonymity is maintained in the decryption process;
- Votes are not compromised in the event of loss of internet connections;
- Printed ballots contain preferences as specified by the voter.
- The system does have some method of logging errors in log files;
- Voters cannot cast more than one vote;
- The system does not allow multiple vote sessions of the same remote voter to result in more than one vote for the voter;

***Finding: BMM is satisfied that the eLect system has been tested with due diligence.***

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

## 8 LOAD TESTING

The system has not been through a load test. It is anticipated that the load on the system will not be high as the trial is limited to four remote sites. The number of voters expected to take part in this trial is not expected to exceed 3000.

## 9 PROCESS & PROCEDURES

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

- a. Personnel responsible for setting up the election will be properly trained. The election setup manual and high level checklist must be accurate and up to date.
- b. Access to the election officer's PC (EOPC) will be restricted as per current security procedures;
- c. Configuration setup will be carefully checked by two AEC personnel;
- d. The preview election screens will be printed out and compared with printed ballot papers by AEC staff other than those who loaded the data.
- e. The AEC will prevent personnel from making any changes to the configuration setup of an election while the election is open for voting. This will be achieved by the disconnection of the Electoral Officer PC (EOPC) from the Defence Server by AEC IT until the end of the election period;
- f. The AEC will save all logs to the EOPC when they are created to prevent them from being overwritten;
- g. The AEC will check voter data for voters with the same first name, surname and date of births to ensure that this combination is unique. Second names may be used to differentiate remote voters;
- h. The AEC will backup the private key used for decrypting the votes as a precaution.

## 10 RISK ANALYSIS

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

## 10.1 Security Risks

#	Risk	Treatment
S1	The approved Candidates data 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 system to ensure the correct ballot information is correct and free from error. The security setup will prevent unauthorised access.</i>
S2	The approved Referendum data 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 system to ensure the correct ballot information is correct and free from error. The security setup will prevent unauthorised access.</i>
S3	The applications running on the server are interfered with and now contain malicious code.	<i>Inspection of relevant source code found no evidence of malicious software. The versions of software running on the server have been verified by the auditor. The system hardware is currently 'locked down' in a secure area to prevent any unauthorised access.</i>
S4	An unauthorised person could cast a vote on eLect.	<i>Voters access the eLect system through the Defence intranet system. Extensive testing by the AEC and by the Auditor found no instances of unauthorised voters being able to access the system.</i>
S5	A person authorised to cast a vote could cast more than one vote.	<i>Extensive testing by the AEC and by the Auditor found no instances of voters being able to cast more than one vote.</i>
S6	The recorded votes on the eLect database could be substituted by a modified set of votes.	<i>Votes are encrypted with a public key and are stored encrypted on the database and cannot be decrypted without a quorum of AEC officials being present. The encryption is tamper evident and cannot be altered.</i>
S7	Unauthorised persons could decipher and read the contents of an "electronic ballot".	<i>Ballots must be decrypted with private keys and a quorum of AEC officials. Printed ballots are handled in accordance with procedures for all ballot papers and are subject to existing physical security applied to those ballot papers.</i>
S8	Information captured by eLect could be used to identify which individual cast a particular vote.	<i>The vote data does not associate the voter with the votes. Extensive testing by the AEC and by the Auditor found no instances of voters being able to be associated with their vote.  When the ballots are decoded by AEC personnel, they are then handled according to existing AEC procedures for postal ballots to protect the secrecy of the votes through</i>

		<i>separation of the votes from the voter information. These two sets of data are downloaded and processed separately.</i>
S9	An unauthorised person could enable or disable voting	<i>Administrative functions are only available on the Election Officer's PC in Canberra. It is only accessible by authorised personnel.</i>

## 10.2 Accuracy Risks

#	Risk	Treatment
A1	Preferences recorded electronically on the eLect database could be different to preferences entered by a voter.	<i>Extensive testing by the AEC and by the Auditor found no instances of preferences being recorded or recalled incorrectly.</i>
A2	The eLect system may not allow a voter to enter valid preferences or to correct mistakes.	<i>Extensive testing by the AEC and by the Auditor showed that the software allowed correct entry of preferences and correction of mistakes prior to confirmation and casting a vote.</i>
A3	One or more votes could be lost in the system.	<i>All tests of entry of preferences and recall of preferences additionally showed no loss of votes.</i>
A4	A voter may not be able to tell whether or not their vote has been successfully recorded.	<i>A receipt is generated on successful completion of voting. A vote checking service is available to enable remote voters to check that their vote has been recorded.</i>
A5	When the votes are decoded after the election some votes may be dropped or duplicated.	<i>All tests of decryption of votes showed no compromise of votes.</i>
A6	In the event of loss of internet connection, some electronically stored votes may be lost or corrupted.	<i>Votes are recorded on the database when the remote voters submit the votes. Loss of internet connection will not result in a lost of votes or corruption of votes. In some circumstances, a loss of internet connection will result in a vote not being saved. However, the voter will know that this is the case and be able to re-enter and submit their vote.</i>

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

## 11 CONCLUSIONS

Following the audit activities outlined in this report, the Auditor was able to make an informed appraisal of the eLect system's compliance with AEC requirements.

1. BMM is satisfied that the eLect system implementation includes features that provide the level of security required by the AEC;
2. BMM is satisfied that the eLect system has been tested with due diligence;
3. BMM found no evidence of malicious source code in the eLect system;
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 eLect system to comply with AEC requirements regarding security, accuracy and voting functionality.

As a result of the evaluation BMM believes that properly used, the eLect system complies with the specified AEC requirements.