



Report into

Remote Electronic Voting at the 2007 Federal Election for Overseas Australian Defence Force Personnel

Australian Electoral Commission
West Block Offices
Queen Victoria Terrace
PARKES ACT 2600

Department of Defence
Russell Offices
CANBERRA ACT 2600

CONTENTS

GLOSSARY	3
1.0 EXECUTIVE SUMMARY	4
1.1 BACKGROUND	4
1.2 SCOPE.....	4
1.3 LEGISLATION	4
1.4 SYSTEM ACQUISITION, DESIGN, TESTING AND DEPLOYMENT	4
1.5 VOTING PROCESS	5
1.6 CONTRACTOR PROJECT REPORT	5
1.7 TRIAL EVALUATION	5
1.8 CONCLUSION.....	6
2.0 REMOTE ELECTRONIC VOTING REPORT	7
2.1 PURPOSE.....	7
2.2 BACKGROUND	7
2.3 JSCEM REPORT/GOVERNMENT DECISION	7
2.4 SCOPE.....	8
2.5 ICT SYSTEM DEVELOPMENT.....	11
2.6 USER ENGAGEMENT	15
2.7 IMPLEMENTATION.....	16
2.8 COSTS	22
2.9 CONTRACTOR'S PROJECT REVIEW	23
2.10 INDEPENDENT TRIAL EVALUATION	24
2.11 FUTURE OPTIONS.....	27
2.12 CONCLUSION.....	32
APPENDICES	34
1.0 SUPPLEMENTARY DETAILED TECHNICAL REPORT	34
APPENDIX B – LETTER OF AGREEMENT	80
APPENDIX C – SYSTEM AND ASSOCIATED SECURITY ISSUES	83
APPENDIX D – STATEMENT OF REQUIREMENT	88
APPENDIX E – PROJECT SCHEDULE	97
APPENDIX F – 'HOW TO CAST YOUR VOTE' PAMPHLET.....	99
APPENDIX G – APPLICATION TO REGISTER FOR REMOTE ELECTRONIC VOTING FOR THE 2007 FEDERAL ELECTION.....	102
APPENDIX H – STANDARD AEC LETTERS.....	103
APPENDIX I – REMOTE ELECTRONIC VOTING SYSTEM ARCHITECTURE	112
APPENDIX J – LOADING AND CHECKING PROCEDURES FOR DIACRITICAL MARKS	113
APPENDIX K – REMOTE ELECTRONIC VOTER USER QUESTIONNAIRE	114
APPENDIX L – FOCUS GROUPS QUESTIONS.....	116
APPENDIX M – EVALUATION FINDINGS AND RECOMMENDATIONS	117

Glossary

ACT EC	ACT Electoral Commission
ADF	Australian Defence Force
AEC	Australian Electoral Commission
AFP	Australian Federal Police
AFPO	Armed Forces Post Office
AO	Area of Operation
CDF	Chief of Defence Force
CEA	Commonwealth Electoral Act 1918
CIOG	Chief Information Officer's Group, Department of Defence
CIS	Computer Information Support, Department of Defence
Defence	Department of Defence
DMO	Defence Materiel Organisation
DRN	Defence Restricted Network
DRO	Divisional Returning Officer
DSD	Defence Signals Directorate
DSOE	Deployed Standard Operating Environment
EC	Electoral Commissioner
ELMS	Election Management System
EOPC	Electoral Officer PC
ESP	Elections System and Policy
EVS	Electronic Voting Section
FACEO	First Assistant Commissioner – Elections Operations
FMA	Financial Management Accountability Act 1997
GPV	General Postal Voter
HMA	Her Majesty's Australian (Ships)
HQJOC	Headquarters Joint Operations Command
ICON	Intra-government Communications Network
ICT	Information and Communication Technology
ISD	Information Systems Division, Department of Defence
JSCEM	Joint Standing Committee on Electoral Matters
MEAO	Middle East Area of Operations
NATA	National Association of Testing Authorities
NO	AEC's National Office
PAR	Post Activity Report
PE	Personnel Executive, Department of Defence
PIN	Personal identification number
REV	remote electronic voter
RFQ	Request for quotation
RFT	Request for Tender
RMANS	Roll Management System
Secretary	Secretary of Defence
SOE	Standard Operating Environment
SOR	Statement of Requirements
TEC	Tender Evaluation Committee
VEC	Victorian Electoral Commission

1.0 Executive Summary

1.1 Background

- 1.1.1 In its report on the 2004 federal election, the Joint Standing Committee on Electoral Matters (JSCEM) recommended that remote electronic voting be considered for certain classes of voters including Defence personnel serving overseas.
- 1.1.2 In August 2006, the Government responded to the JSCEM report and stated that a trial of remote electronic voting would be undertaken for the 2007 federal election. The trial would be restricted to ADF personnel deployed overseas, and was subject to the satisfactory resolution of systems and associated security issues.
- 1.1.3 Advice provided to the Special Minister of State by the AEC in February 2007 outlined potential system and security issues, and described the risks and mitigation activities to be implemented. The Special Minister of State agreed to the continuation of the trial.
- 1.1.4 A project team was formed in October 2006, consisting of staff from the AEC and Defence. A Project Board was established, jointly chaired by the AEC and the Department of Defence (Defence).

1.2 Scope

- 1.2.1 The scope of the trial was restricted to those overseas ADF personnel who had access to the Defence Restricted Network (DRN) and who would be serving in Afghanistan, Iraq, Timor-Leste and the Solomon Islands at the time of the election.
- 1.2.2 The trial was conducted on the Defence Restricted Network (DRN) and was not available on the world wide web – creating a secure software environment for voting.
- 1.2.3 The trial specifically excluded HMA Ships due to bandwidth and connectivity constraints.

1.3 Legislation

- 1.3.1 The Electoral and Referendum Legislation Amendment Act 2007 became law in March 2007, and enabled this trial for the first general election and first senate election after the commencement of the legislation. Consequently the legislation is relevant to the 2007 election only.
- 1.3.2 The Electoral and Referendum Amendment Regulations (ERAR) 2007 (No. 3) were registered in September 2007, and the commencement date was 1 August 2007.

1.4 System Acquisition, Design, Testing and Deployment

- 1.4.1 Following a restricted tender process conducted by the AEC, Registries Limited (an Australian firm working in conjunction with Everyone Counts) was contracted to develop the remote electronic voting application.

- 1.4.2 The tender evaluation phase included a pilot of the proposed application conducted within the DRN.
- 1.4.3 The AEC and Defence were engaged throughout the application design process. This ensured that the design met all security and policy requirements, complied with Australian federal electoral law and with DRN standards and protocols and constraints.
- 1.4.4 The application was extensively tested on multiple deployed technology platforms in each of the target areas of operations, as well as infrastructure located in Canberra and North Queensland.
- 1.4.5 BMM Australia Pty Ltd, a National Association of Testing Authorities accredited firm audited the system post development. The system was certified as having met all requirements.
- 1.4.6 The AEC and Defence undertook a comprehensive system acceptance process prior to deployment into production. Both agencies confirmed that the information system and support procedures were ready for the 2007 Federal election in October 2007.

1.5 Voting Process

- 1.5.1 In all, 2,012 voters were registered and this was 80% of those eligible to participate in the trial. Of these, 1,511 voters, or 75%, used the remote electronic voting system.
- 1.5.2 Electronically submitted votes were printed following polling day, and dispatched to the relevant Divisions for counting.
- 1.5.3 Those voters that could not or did not wish to vote electronically were provided access to alternative means of voting, including general postal voting and pre poll voting at Australian Diplomatic posts.

1.6 Contractor Project Report

- 1.6.1 The Contractor prepared a project report in conjunction with the AEC and Defence.
- 1.6.2 This report concluded that, while some improvements can be achieved, the trial was a success.

1.7 Trial Evaluation

- 1.7.1 The AEC commissioned an independent evaluation of the trial. This evaluation includes voter feedback which was very positive.
- 1.7.2 The trial demonstrated that remote electronic voting for personnel deployed overseas provided a convenient, reliable and secure method of voting in a federal election with voter feedback indicating a high level of satisfaction with the level of service provided by remote electronic voting.
- 1.7.3 The evaluation included recommendations for any future such trial and concludes that the trial was a success.

1.8 Conclusion

- 1.8.1 This trial conducted the first remote electronic voting for any Australian government, and was an historic event.
- 1.8.2 The trial was a significant achievement given the short timeframe to implement and the complexities of conducting a trial in a military operational environment with long and sometimes unpredictable lines of communication.
- 1.8.3 Considerable management and resources especially from joint task forces (ADF) in the areas of operation and from the AEC with regard to registration and tender evaluation were required for the implementation of the trial.
- 1.8.4 Identification and authentication of eligible voters remains an issue especially regarding the timeliness of receiving personal identification numbers, required by voters to access the remote electronic voting system, via the postal system
- 1.8.5 The Contractor's report and the independent evaluation both found the trial to be a success.
- 1.8.6 This report as well documents the end-to-end success: from a technology view as well as from a participation point of view.
- 1.8.7 This success is a solid foundation for the future, should the Australian government undertake further remote electronic voting.

2.0 Remote Electronic Voting Report

2.1 Purpose

- 2.1.1 This report has been prepared by the AEC and the Department of Defence (Defence) to describe the conduct and outcomes of the recent trial of remote electronic voting.

2.2 Background

- 2.2.1 Prior to the 2007 Federal Election, deployed Australian Defence Force (ADF) personnel voted either by postal vote or by pre poll vote at an Australian Embassy or High Commission. The voter could not arrange either of these methods prior to the announcement of the election.
- 2.2.2 In the case of a postal vote, for example, the postal vote application would have to be made after the announcement of the election and posted to the AEC in Australia.
- 2.2.3 For some areas of operation (AO) there is a 3 week delivery time line for mail. Consequently by the time the AEC received the postal vote application, and then posted the ballot material to the voter, the voter often did not receive their ballot papers prior to polling day or if they did, the AEC did not receive back the completed ballot papers within the statutory time frame to include the ballot papers in the count.

2.3 JSCEM report/Government decision

- 2.3.1 In its report on the 2004 Federal Election, the Joint Standing Committee on Electoral Matters (JSCEM) recommended remote electronic voting for certain classes of voters including ADF personnel¹ serving overseas:
- 2.3.2 Recommendation 43 stated:
- “The Committee recommends that the AEC trial remote electronic voting for overseas Australian Defence Force and Australian Federal Police personnel, and for Australians living in the Antarctic. The AEC should develop a proposal that considers matters such as security and verification of identity, and report back to the Committee.”
- 2.3.3 In its response the Government supported the recommendation in principle. It Stated:
- “The AEC will arrange a trial of remote electronic voting for overseas Australian Defence Force (ADF) personnel, subject to satisfactory resolution by the AEC and the Department of Defence of systems and associated security issues. The results of this trial will enable the AEC to inform the development of the broader proposal on remote electronic voting as recommended

¹ For the purposes of this trial, ‘Defence civilians’ are included. A Defence civilian is defined as a civilian who performs duties in an Area of Operations (AO) in support of ADF operations. This includes a person who, with the authority of an authorised officer, accompanies a part of the Defence Force that is:

- (a) outside Australia; or
- (b) on operations against the enemy; and
- (c) has consented, in writing, to subject themselves to the Defence Force Discipline Act while so accompanying that part of the Defence Force.

by the JSCEM. The AEC will keep the Special Minister of State informed on the progress and outcomes of the trial and the development of the proposal for the JSCEM.”

- 2.3.4 Accordingly the AEC undertook a trial of remote electronic voting for overseas Defence (ADF) personnel.

2.4 Scope

2.4.1 Contracted Services

- 2.4.1.1 Recommendation 43 of the JSCEM report to government provided for the AEC to develop a solution that considers matters such as security and verification of identity to allow for remote electronic voting for overseas ADF personnel.
- 2.4.1.2 This solution was required to meet the specific requirements of the Commonwealth Electoral Act 1918 (CEA).
- 2.4.1.3 The solution was required to be compatible with the Defence Restricted Network (DRN) while the voting application resided on stand-alone servers in the AEC data centre.
- 2.4.1.4 The total number of ADF personnel deployed in these areas of operation was around 2,500. All voters targeted for the trial were also registered as General Postal Voters (GPV) and sent a postal vote as a contingency provision at the time of the election should they not be able to access the DRN for operational reasons.
- 2.4.1.5 The developed software allowed for full preferential voting for the House of Representatives, proportional representation for the senate and catered for a referendum if required.

2.4.2 Security Restrictions

- 2.4.2.1 The trial was subject to the satisfactory resolution of systems and associated security issues. To ensure security of the votes, the following basic design elements were determined:
- a. The server storing the votes was housed in the AEC’s data centre although logically part of the DRN;
 - b. Connectivity between the servers and Defence was via ICON, the Intra-government Communications Network in Canberra;
 - c. Data on ICON was hardware encrypted; and
 - d. Access to voting was only available via the Defence Restricted Network (DRN).

2.4.3 Defence Project Organisation

- 2.4.3.1 The PRINCE2 project management methodology was used by Defence to manage its specific deliverables. An internal Defence Project Board was established including stakeholder representation from key Defence Groups including Personnel Executive, Chief Information Officer Group (CIOG), Defence Materiel Organisation (DMO) and Headquarters Joint Operations Command (HQJOC).

- 2.4.3.2 Defence engaged a Project Director and dedicated Project Manager to manage the project on behalf of the Defence Project Board. Defence also engaged a Technical Project Director and a dedicated Technical Project Manager to manage the technology and integration. A “point of contact” was appointed from each of the major stakeholder groups, responsible for managing their group’s stakeholder input (including resources) for the trial.

2.4.4 AEC Project Organisation

- 2.4.4.1 The AEC used its standard project governance methodology for this project. Key roles in that methodology for this project have been as follows:
- a. Steering Committee Chair –First Assistant Commissioner Electoral Operations;
 - b. Project Sponsor –Assistant Commissioner Elections;
 - c. Project Manager –Director, Electronic Voting; and
 - d. Working Party:
 - A. Project Manager
 - B. Assistant Director, Electronic Voting; and
 - C. Two Project Officers.

2.4.5 Risk and Issue Management

- 2.4.5.1 The Government response to JSCEM’s recommendation 43 stated that the trial of remote electronic voting for overseas Australian Defence Force (ADF) personnel was to be subject to the satisfactory resolution of systems and associated security issues.
- 2.4.5.2 The AEC and Defence jointly identified the risks in this area and subsequent mitigation or resolution for each of those risks during the planning phase in December 2006 and January 2007. In February, the AEC provided these details to the Special Minister of State (SMOS) together with a recommendation that the trial should proceed. The Minister agreed with this recommendation on 22 February 2007.

2.4.6 Legislation

- 2.4.6.1 Legislation needed to be drafted for the Commonwealth Electoral Act and in place to support the recommendations in time for the federal election. Finance had previously submitted a bid for a Bill for introduction in the Spring sittings 2006 which had been given ‘A’ status. The Cabinet Submission covering the Government response provided the policy authority for a Bill to be drafted to make the necessary amendments to the CEA.
- 2.4.6.2 There were two further important elements of the Bill. The first was limiting the trial to the first elections and referendum held after the Bill was given Royal Assent. The second was to provide the Minister with the capacity to decide for any reason not to proceed with the trials.
- 2.4.6.3 Royal Assent was given on 15 March 2007.

2.4.6.4 Upon Royal Assent all of the provisions providing for the electronic voting trials commenced. Schedule 2 of the Amendment Act amended the Commonwealth Electoral Act 1918 (Electoral Act) to insert a new Part XVB into the Electoral Act. Division 1 provided for a trial of electronically assisted voting for sight-impaired people while Division 2 provided for a trial of remote electronic voting for defence personnel serving outside of Australia. Schedule 2 also amended the Referendum (Machinery Provisions) Act 1984 (Referendum Act) to insert a new Part IVA into the Referendum Act.

2.4.7 Regulations

2.4.7.1 Following the passage of the Bill through the House of Representatives, work commenced on preparing drafting instructions for the regulations. Instructions were provided to the Office of Legislative Drafting and Publishing on 22 December 2006.

2.4.7.2 The regulations went through a series of drafts as policy was refined and technical attributes were finalised. Due to the complexity and scope of the proposed regulations, the regulations took some time to finalise. As a consequence of this, the regulations were drafted to commence retrospectively on 1 August 2007. Advice from the Australian Government Solicitor was obtained before these instructions were issued. Having the regulations commence retrospectively ensured that there was no risk attached to any action undertaken by the AEC in relation to registering remote overseas electors.

2.4.7.3 The regulations affected the administrative responsibilities of three other Ministers: the Attorney-General in relation to human rights issues surrounding the electronically assisted voting trial; the Minister for Defence in relation to defence personnel; and the Minister for Justice and Customs in relation to the offence provisions in the regulations. Formal approval was sought from the Minister for Justice and Customs for the offence provisions, while support for the regulations was sought from the Attorney-General and the Minister for Defence.

2.4.7.4 The Governor-General made the regulations on 6 September 2007 and they were registered on the Federal Register of Legislative Instruments on 11 September 2007. The regulations were tabled in the Senate on 13 September 2007.

2.4.7.5 Following the registration of the regulations, on 24 September 2007 the Electoral Commissioner determined the four countries in which the trial would take place for remote electronic voters. The Electoral Commissioner's determination was gazetted on 25 September 2007.

2.4.8 Procurement Process Overview

2.4.8.1 The AEC's project team was formed in September 2006 and as a solution was to be available for deployment by 30 June 2007, an

abbreviated procurement methodology was approved under Section 8.65(g) of the Commonwealth Procurement Guidelines

- 2.4.8.2 The following organisations were selected to participate in the direct sourcing for the reasons indicated:
- a. Hewlett-Packard Australia Pty Ltd – this company provided the Victorian Electoral Commission’s solution.
 - b. Software Improvements Pty Ltd – this company provides the ACT Electoral Commission’s solution; and
 - c. Registries Limited – this company provided online voting for the AEC’s Certified Agreement vote in 2002.

2.4.9 Request for Tender

- 2.4.9.1 Subsequent to the first joint project meeting, the AEC commenced development of a Statement of Requirements (SOR) detailing the services required.
- 2.4.9.2 There were two important areas of the SOR that should be mentioned at this stage.
- a. Systems and associated security issues were specifically included in the SOR together with the methodology already determined to address these issues. Vendors were to confirm that they could meet the risk minimisation or resolution in their responses.
 - b. It was imperative that the acquired system operate within the DRN. To this end, the SOR required tenderers to provide a pilot system to determine compatibility of the offered software with Defence’s various software levels.
- 2.4.9.3 The AEC conducted an industry briefing on 18 January 2007. At this briefing the AEC provided an overview of the requirements and outlined the electoral process.
- 2.4.9.4 On 3 April 2007, the FACEO approved the Tender Evaluation Report, which selected Registries Limited (the Contractor) as the preferred tenderer.
- 2.4.9.5 Contract negotiations commenced soon after this date with an agreement entered into by the parties dated 18 May 2007.

2.5 ICT System development

2.5.1 Development

- 2.5.1.1 Development was an iterative process, with AEC staff reviewing the voting application and providing feedback on required improvements or fixes.
- 2.5.1.2 Once initial development was complete, the application was loaded on to the servers in the AEC’s data centre, and testing continued both via the DRN and the EOPC.

2.5.2 Testing Scope

- 2.5.2.1 Testing on this project consisted of the following functional areas:
- a. Connectivity testing from the AEC data centre across the ICON network into the Defence Restricted Network (DRN) to ensure server connectivity and data encryption passed successfully.
 - b. Canberra based functional testing on Defence PC hardware (two different standard operating environments were used) at a Defence site to ensure the encrypted messages could travel back to the server where the votes were recorded.
 - c. Server failover testing.
 - d. Field satellite based testing on Defence PCs in Australia, Solomon Islands and East Timor (two different standard operating environments were tested). As well staff in Afghanistan and Iraq performed a limited amount of testing.
 - e. AEC functional testing (voting, election setup and post election processing).
- 2.5.2.2 Full Election end to end testing over a 2-3 week period (performed by AEC with machines disconnected from DRN).

2.5.3 Testing

- 2.5.3.1 The system was extensively tested on multiple simulated deployed technology platforms in Canberra, as well as field tested as shown below.
- 2.5.3.2 Major field testing was conducted as follows.
- a. North Queensland (Exercise Operation Talisman Sabre), from 4 to 8 June 2007;
 - b. Remote testing from Iraq, Afghanistan, Timor-Leste, Solomon Islands on 25-Jun-07;
 - c. Solomon Islands from 20 to 23 August 2007; and
 - d. Final validation of all DRN terminals in all target AOs on 17 October 2007.
- 2.5.3.3 The AEC and Defence undertook a comprehensive system acceptance process prior to deployment of the production system.
- 2.5.3.4 Both agencies confirmed in September 2007 that the information system and support procedures were ready for the 2007 Federal election, and the final System Acceptance document was sign by the Joint Project Board Chairs in October 2007.

2.5.4 Hardware and Connectivity Testing

- 2.5.4.1 The initial tests were conducted over four days testing from 25 to 30 May 2007 testing communications, performance and 'end-to-end' system functionality. Results from testing were mostly positive but further testing was required.
- 2.5.4.2 Further 'end to end' system testing was conducted in Queensland during Operation Talisman Sabre from 4 to 8 June 2007. Testing concluded that technical problems were present using the remote

electronic voting system and Defence's deployed standard operating environment.

- 2.5.4.3 Defence investigated the source of these problems and designed, developed, tested and had Security accepted a solution to allow the electronic voting software to work across the deployed networks. The alternative solution still utilised the deployed network including satellite technology however did not depend upon the underlying Defence DSOE.
- 2.5.4.4 Validation of the system continued in the areas of operation up until the 2007 federal election. This included system 'end to end' testing conducted in the Solomon Islands in late August 2007 by the Defence CIOG representative.

2.5.5 AEC's ICT Hardware Environment

- 2.5.5.1 The AEC's servers were configured in the Canberra data centre and connectivity was established with Defence via the Intra-government Communications Network (ICON).
- 2.5.5.2 ICON is the communications system providing dedicated point-to-point links for Australian government agencies in Canberra through use of an underground system of fibre optic cables and conduits with fibre termination panels located within user premises.
- 2.5.5.3 The voting application itself uses either encrypted Java applets or SSL (secure socket layer), an encryption protocol for point-to-point connectivity over the Intranet.
- 2.5.5.4 In addition to this software encryption, hardware encryption was implemented by the installation of routers on either end of the ICON connection.
- 2.5.5.5 Two servers were configured: a primary server plus a 'fail-over' server. The secondary server also provided redundancy for all data stored on the primary server.

2.5.6 Defence's ICT Hardware Environment

- 2.5.6.1 Defence ICT hardware requirements used for the trial included:
 - a. Defence ICT Infrastructure enabling connectivity to AEC via the ICON network: Defence installed routers procured by AEC to allow ICON connectivity between AEC and Defence. These routers included hardware encryption;
 - b. A middle tier layer using CITRIX technology which was implemented to overcome inconsistencies identified in testing of the DSOEs. This middle tier layer allowed for the distribution of the AEC's remote electronic voting system whilst still using the Defence's underlying DSOE. Four Citrix servers were implemented to provide this capability plus redundancy;
 - c. Deployed DRN workstations consisting of laptop computers in Afghanistan, Iraq, Timor-Leste and Solomon Islands. Software updates (Citrix client) were applied to these laptops to allow for the use of these laptops in the trial; and

- d. General deployed communication devices including the use of satellite technology.

2.5.7 Certification

- 2.5.7.1 The tender included a requirement that the final system be independently audited to verify that the system is secure and accurate.

2.5.8 Independent audit

- 2.5.8.1 To comply with Commonwealth Procurement Guidelines, the project manager determined that a restricted request for quotation (RFQ) be issued to three independent organisations to undertake an independent audit of the system. These were BMM International and two other NATA certified auditors.
- 2.5.8.2 This RFQ was issued on 8 June 2007 and after an evaluation of the responses, BMM International was selected as the successful contractor.
- 2.5.8.3 BMM subsequently issued the following formal findings and certification on 14 September 2007:

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”.*

2.5.9 Defence security accreditation

- 2.5.9.1 Defence information systems operating within the Defence Restricted Network are required to be accredited and certified prior to operational use within Defence.
- 2.5.9.2 The remote electronic voting system, as trialed via the Defence Restricted Network, was successfully certified and accredited for use in early July 2007, confirming its compliance with the accepted Defence ICT security standards and that the security measures employed minimised the residual risk to Defence’s ICT infrastructure to an acceptable level as required by Defence.

2.6 User Engagement

2.6.1 Defence Promotion

- 2.6.1.1 Given that the trial was to take place in four countries with personnel in Australia also needing information on the trial, Defence put in place a methodology to promote the trial. Promotion of the trial involved:
- 2.6.1.2 Defence Military Signals. Numerous military signals were issued to the Joint Task Forces in each of the AOs. Key signals included:
- A. 'Warning Order – Federal Election, General Postal Voting and Remote Electronic Voting' issued on 8 August 2007; and
 - B. Signal 'Notification of Impending Federal Election – Saturday 24 November 2007) issued on 15 October 2007.
- 2.6.1.3 Defence Intranet Website. Defence established a dedicated intranet site for the remote electronic voting trial. Initially released on 9 August 2007 and updated frequently with information on the trial, the website was the central portal/repository for information on the trial. The website contained information on the electronic voting trial as well as information in relation to general postal voting, AEC enrolment and registration forms. This website also contained the link used by ADF members to access the AEC remote electronic voting system.
- 2.6.1.4 Force Preparation. Prior to deployment, ADF members undergo Force Preparation training. Force Preparation training from May 2007 onwards included briefings on the upcoming remote electronic voting trial, with REV application forms being provided from August 2007.
- 2.6.1.5 Navy, Army and Air Force Service Newspapers. Promotional articles on the trial were included in all service newspapers in the 4 October 2007 edition. Services newspapers were made available to all ADF members in the trial locations and in Australia.
- 2.6.1.6 Defence information circular "*Defgram*": The circular released on 11 September 2007 advised of the upcoming trial.
- 2.6.1.7 AO Visits:
- A. Defence and AEC personnel undertook testing in the Solomon Islands in late August 2007. As part of this visit, the trial was promoted to local personnel and enrolment forms were distributed and completed.
 - B. An AEC project officer visited Timor-Leste in October 2007 specifically to promote the trial to ADF members in that location.
- 2.6.1.8 Regular video-conferencing including staff officer consultation with Joint Task Forces from May 2007.

2.6.2 AEC Promotion

- 2.6.2.1 As promotion of the trial was restricted to ADF personnel, the AEC's Communication Plan was much less complex than that required by Defence.
- 2.6.2.2 The AEC's promotion focused on media, the AEC's website and the user instruction pamphlet.
- 2.6.2.3 Media:
 - a. The AEC NO media team issued a joint media release with the Department of Defence on 18 September announcing the trial of e-voting for deployed Defence personnel. Subsequently, media requested further information. The AEC prepared a fact sheet and provided additional information, as well as links to photographs of the trial.
- 2.6.2.4 Website:
 - a. The AEC also had information on the AEC web site with regard to the trial. The Website covered:
 - A. Background to the electronic voting trial;
 - B. Qualifications to Register for the trial;
 - C. Security;
 - D. The voting process;
 - E. What to do if you could not participate in the trial; and
 - F. Audit and certification executive summary of the electronic voting software.
- 2.6.2.5 Pamphlet:
 - a. A draft 'How to cast your vote' pamphlet' was develop by the Contractor. Defence and the AEC then jointly modified the pamphlet to suit the requirements of this trial.
 - b. The pamphlet was issued to each REV with their PIN.

2.7 Implementation

2.7.1 REV Registration and PIN distribution

- 2.7.1.1 The registration of REVs needed to comply with areas of the new and old legislation as well as the policy decision to issue all REVs with a GPV.
- 2.7.1.2 As the trial was restricted to four AOs, the Electoral Commissioner gazetted these areas. This meant that the AEC divisional office staff who were receiving REV registration forms needed a methodology by which to accept applicants who qualified as REVs and reject others who were not within the gazetted AOs.
- 2.7.1.3 The AEC consulted Defence in designing a process for the AEC divisional staff to allow for validation of registration forms. Defence provided six Armed Forces Post Office (AFPO) numbers that were solely located within the gazetted AOs. These were:

Iraq	AFPO 19 and AFPO 20
Afghanistan	AFPO 13 and AFPO 14
Timor Leste	AFPO 5
Solomon Islands	AFPO 11

2.7.1.4 If an applicant did not quote one of these AFPO addresses then they were assessed as not being eligible to be registered.

2.7.2 Addressing the Legislative Requirements

2.7.2.1 Given the requirements of the legislation, particularly Regulation 62, it was decided that, when the Writs were issued for the election, a review of REVS would occur against their applications to ensure that any REV who was in Australia at the time the Writs were issued would be deregistered as a REV if they ;

- a. had returned to Australia permanently; or
- b. would be in Australia at the time of the election

2.7.2.2 Notwithstanding the above, for the majority of the 2012 registered REVs, the process went quite smoothly. Registration and PIN issue progressed through the following steps:

- a. Within the AEC the enrolment would firstly be checked and if the applicant was enrolled they would then be flagged in the RMANS to receive a GPV as well as a REV.
- b. The REV would then receive an acknowledgement letter informing them of their status.
- c. Each week the electronic voting team produced a PIN mailer for each new applicant. The mailing of PINs commenced on 9 October 2007 and the last mail out was on 2 November 2007
- d. The PIN mailer was a letter with a security panel which, when peeled off, would reveal the voter's PIN. The letter contained instructions to the voter and the 'How to cast your vote' pamphlet' was also included.

2.7.3 GPV contingency

2.7.3.1 A contingency process where the voter could still cast their vote was required in the event that deployed personnel may not be able to access a computer in order to vote for various reasons such as:

- a. if unforeseen issues arose with the software or connectivity during the election timetable;
- b. the amount of time it takes to get mail to the middle east area of operations;
- c. concern that the voter should not suddenly find themselves in a situation where they were relying on being close to a computer to vote;
- d. electronic voting no longer being an option due to the voter's own or unforeseen circumstances.

2.7.3.2 In each of these situations, the voter needed to be in a position where they could cast a paper ballot.

2.7.4 Voting Process

- 2.7.4.1 Once nominations were declared the e-voting team loaded candidates' names, party names and groupings into the REV database and the database was sealed with six passwords. The REV database was now ready for votes to be cast.
- 2.7.4.2 PIN Mailers were progressively sent out in the lead up to and during the election period, but ceased at the commencement of the 3 week voting period.
- 2.7.4.3 Once the voting period had commenced a REV would access the DRN and the REV software from the Defence Intranet site.
- 2.7.4.4 The REV needed to have with them the PIN, their date of birth and their name as enrolled by the AEC.

2.7.5 Login Screen

Welcome to the 2007 Federal Election Voting System. Please enter the following information and click Next to log-on
Your Voter Access Code is your First name, Surname, (as they appear on your letter from the AEC) and Date of Birth.
Enter your DoB in the following format DD/MM/YYYY

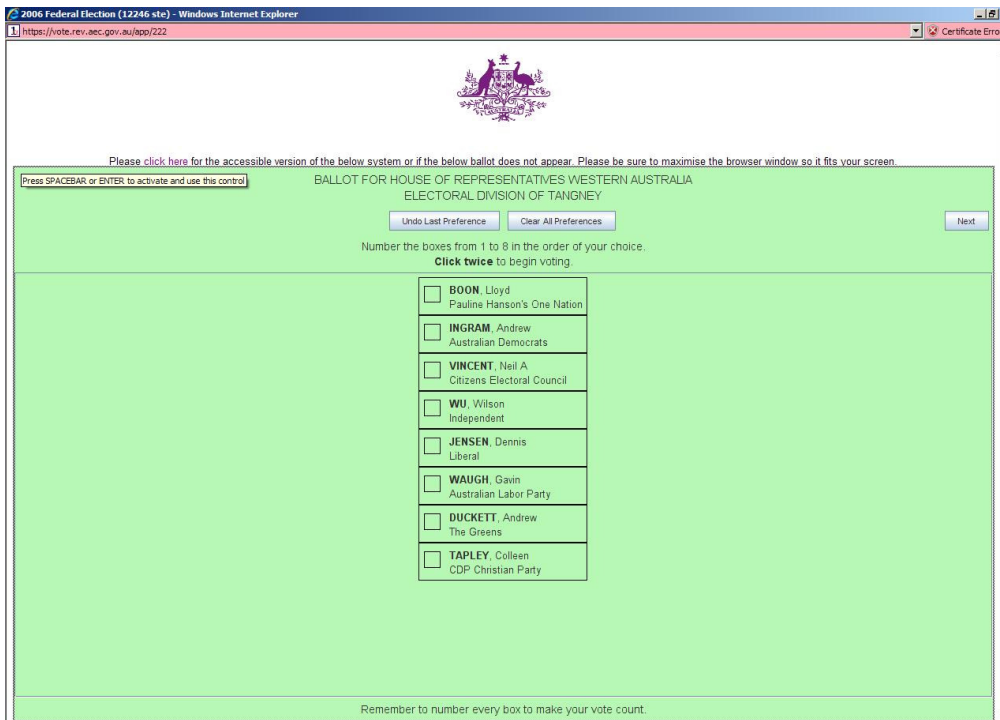
First Name:
Surname:
Date of Birth (as DD/MM/YYYY):
PIN Number:

NEXT

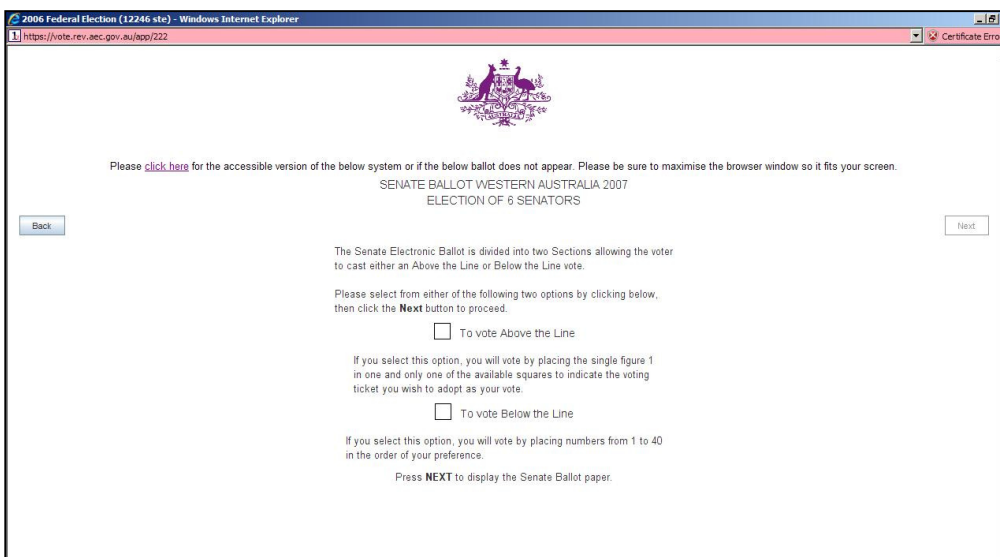
The secure voting software including all appropriate ballots may take approximately 2 minutes to download.
PLEASE DO NOT HIT REFRESH

AEC
Australian Electoral Commission

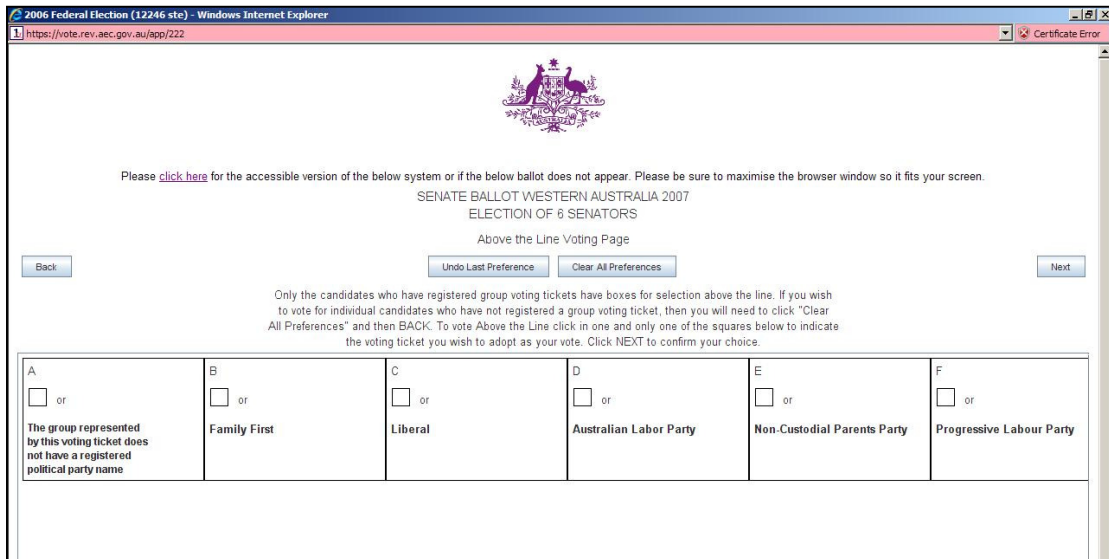
- 2.7.5.1 The REV entered the required detail and then answered a question as to whether they had voted in this election before. If their answer was yes, the system would terminate. If the answer was no they would progress to the following screen in order to cast their vote for the House of Representatives.



- 2.7.5.2 The REV would use the mouse to choose the candidate they preferred most. When the REV clicked on that candidate the number 1 would appear against the candidate. The REV would then choose their next most preferred candidate with the mouse and the number 2 would appear and so on until all candidates had been allocated a preference.
- 2.7.5.3 The REV would be presented with a screen to confirm their preferences cast before progressing to the Senate choice screen shown below.

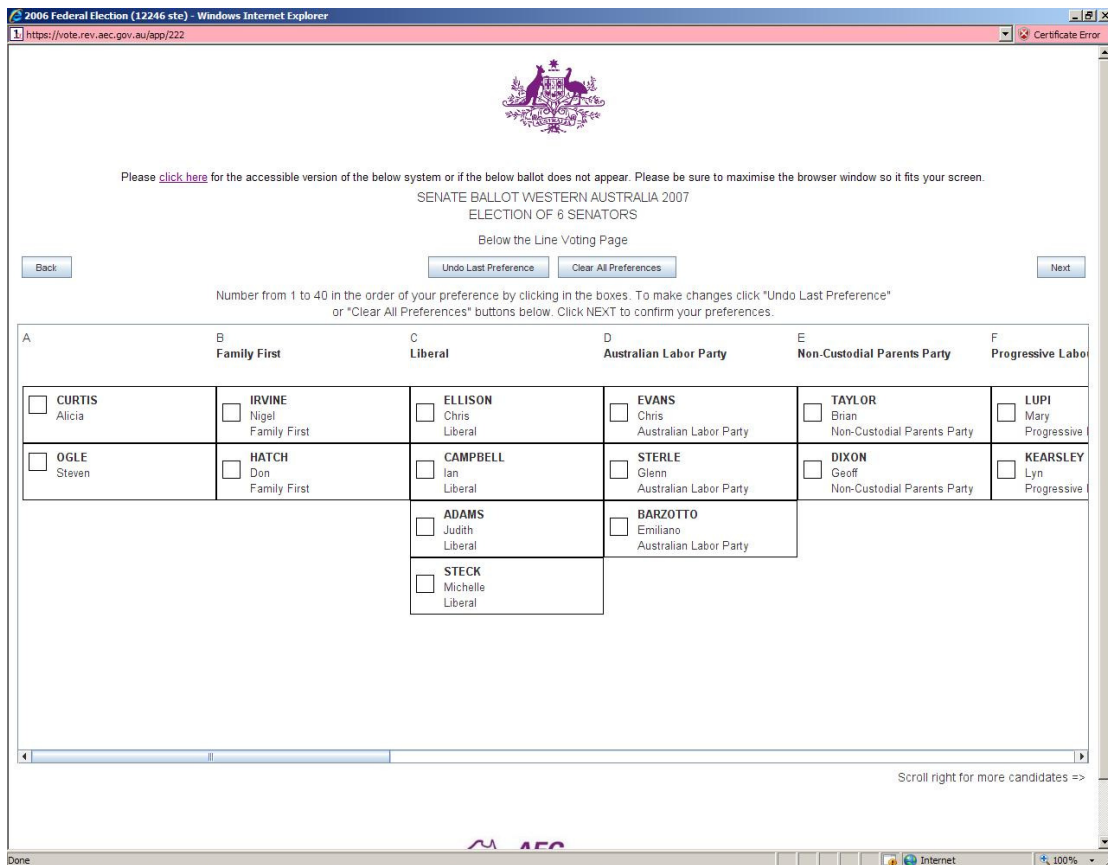


- 2.7.5.4 In this screen the REV is asked to choose whether they want to vote above or below the line. If they chose above the line the following screen would be displayed.



2.7.5.5 The REV clicks on the box of the party or group that they wish to vote for.

2.7.5.6 If the REV chooses to vote below the line instead then the following screen is displayed.



2.7.5.7 The REV must now click in all boxes and allocate preferences to all candidates in order to complete a below the line vote.

- 2.7.5.8 In both the House of Representatives and the Senate above and below the line screens the voter would receive a warning if they had not allocated all of their available preferences and asked to go back and complete their ballot.
- 2.7.5.9 At the conclusion of voting the REV was provided with a receipt number that they could use later to check that their vote had been received by the AEC REV database.

2.7.6 User Support

- 2.7.6.1 The complexity of the remote electronic voting solution required a comprehensive and robust support process. The AEC and Defence jointly consulted to develop support arrangements covering both business and technical support.
- 2.7.6.2 A significant hurdle in the development of these procedures included providing support outside normal business hours to coincide with key operational hours in the areas of operation.
- 2.7.6.3 User support was available during the voting period, and was separated into three distinct areas:
- a. Level one support, provided Defence;
 - b. Level two support, provided by the AEC; and
 - c. Level three support, provided by the Contractor.

2.7.7 Summary of user support

- 2.7.7.1 Despite such a comprehensive model being implemented, only three calls were received, and each of these came through the AEC's public call centre. In summary, the issues were:
- a. A voter who thought he was registered, but who had only completed an Overseas Notification form;
 - b. A voter who used his Australian address as his postal address, and who did not receive his redirected PIN in time to vote; and
 - c. A voter who applied to be a REV, but as he did not include an AFPO number, his application was rejected and he was registered as a GPV only.
- 2.7.7.2 One issue was referred directly from the CIOG Project Manager in Defence to the Project Manager in the AEC:
- a. A voter who could not log in. Investigations revealed that his date of birth was recorded incorrectly on the AEC's systems, therefore he needed to use that incorrect date of birth to log in. This voter subsequently advised that he successfully voted.

2.7.8 Technical support

- 2.7.8.1 Technical support was available, once again, on three levels:
- a. Level one support, provided by Defence;
 - b. Level two support, provided by the AEC; and
 - c. Level three support, provided by the Contractor or the AEC's IT staff, as appropriate.

2.7.9 Summary of technical support

2.7.9.1 It is a credit to AEC's IT staff for creating the hardware and communications environment, Defence for managing the access to the voting server from the deployed networks to the AEC electronic voting server, and the Contractor and its application that not one technical support issue was raised during the voting period.

2.8 Costs

2.8.1 AEC costing model

2.8.1.1 The AEC took actual expenditure against salary (for the actual project team), operating expenses and capital for the period from project commencement to 31 January 2008, and included projected costs until the end of the 2007/2008 financial year.

2.8.1.2 These projected costs were for finalisation of the project and shutdown of the hardware after the close of the Court of Disputed Returns.

2.8.2 Defence costing model

2.8.2.1 Defence received no additional funding or resources for the conduct of the trial. Existing resources were reprioritised by Defence to conduct the trial.

2.8.3 AEC Costs

2.8.3.1	Total	\$786,915
	a. Salary	\$245,375
	b. Operating Expenses	\$375,754
	c. Capital	\$165,786

2.8.3.2 Special items (included above)

a.	Total contractor costs	\$479,186
b.	Audit	\$59,801

2.8.4 Defence Costs

2.8.4.1	Total	\$964,000
	a. Salary	\$582,000 ²
	b. Operating Expenses	\$382,000

2.8.5 Cost Per Vote

2.8.5.1 The cost per vote to the AEC was \$521.00.

2.8.5.2 When both Defence and AEC costs are combined the cost per vote is \$1159.00.

-
- Salary costs include direct salary comprising annual salary, allowances and accrued expenses (superannuation and accrued leave). Salary costs for ADF members also include indirect salary.
 - Figure excludes fixed overheads.
 - Unit Costs used in calculations are sourced from Defence Financial Manual (4).
 - Calculations are based upon the estimated days worked by Defence resources for the trial for the period covering project commencement to end of January 2008.

2.9 Contractor's Project Review

2.9.1 Contractor Evaluation

2.9.1.1 As part of their contractual obligations, the Contractor was to provide a final report on the project which critically reviews the implementation.

2.9.2 Request for Tender/Contract Management Process

2.9.2.1 One of the major concerns from all persons who attended the debrief meeting was the very short project delivery timeframe. This was a direct result of the late decision by government [related to the time frame for the 2007 federal election] to conduct the trial, and the fixed delivery date. All parties felt that acquisition needs to be commenced earlier in the cycle to allow all project teams to perform their tasks to the highest standard.

2.9.3 Project Management

2.9.3.1 Successes

2.9.3.2 It was generally agreed that the relationship between the various project teams worked very well and that all were focused on completing the project by the scheduled date of 30 June 2007.

2.9.3.3 The staff assigned by Defence to co-ordinate testing activities worked extremely well with the Contractor during the testing phase with activities co-ordinated by the AEC Project Manager. The direct contact between all parties during the testing phase was critical to resolving matters quickly and completing development and testing on schedule.

2.9.4 Application Design

2.9.4.1 The design scope for the application was restricted to meet the minimum contracted requirements to achieve the tight delivery schedule for the trial. In elections managed for other clients, the 'eLect' software has been fully setup and managed on a day to day basis by the Contractor. The AEC is the first customer that has required their own electoral officers to setup and run the election from the commencement of the election cycle through to completion.

2.9.4.2 An area of concern raised by all parties related to the credentials used for authenticating a voter. It was agreed that anyone who picked up the PIN mailer and had access to the person's date of birth would be able to vote on that person's behalf. There is no evidence that this occurred during the trial.

2.9.4.3 It is recommended that in any future electronic voting exercises, alternative authentication models and processes be investigated and if possible, adopted.

2.10 Independent Trial Evaluation

2.10.1 Planning and process

- 2.10.1.1 In its 2007-08 Budget Statements, the AEC reported on its plan to evaluate the trial of voting using REV as required by JSCEM.
- 2.10.1.2 The overall objective of the evaluation was to determine the effectiveness of the trial in providing a secure, reliable, and convenient method of voting at federal elections for overseas ADF personnel.
- 2.10.1.3 The aims of the evaluation of the trial were to:
- a. determine the effectiveness and efficiency of the REV trial in providing a secure and reliable method of voting at Federal elections, by examining
 - b. the level of take-up for the use of REV,
 - c. the communication strategy to inform eligible electors in the ADF about the trial,
 - d. the use of postal voting by registrants,
 - e. user acceptance of REV,
 - f. exercise of discretion by REV voters, and
 - g. the cost per vote of the trial;
 - h. evaluate whether the use of REV complied with legislative and other standards by examining compliance of procedures and processes implemented in the trial with relevant sections of the Commonwealth Electoral Act 1918 and associated regulations;
 - i. assess whether the use of remote electronic voting led to any increase in electoral offences, or any increase in the risk of electoral offences or fraud by examining
 - j. procedures to manage risks of electoral offences; and
 - k. allegations of electoral fraud arising from the REV trial.

2.10.2 Postal Survey of REV registrants

- 2.10.2.1 Those who had registered to cast a REV vote were sent a survey questionnaire, asked to fill it in on a voluntary basis, and return it to the AEC by post.
- 2.10.2.2 A total of 2012 ADF personnel registered to cast a REV vote, of whom 1511 cast a vote using REV. In the period up to the cut off on 29 January 2008, 372 survey instruments were filled in and arrived at the National Office, AEC. The resulting number of participants in the survey is shown in the following table. This table also identifies the 95% confidence interval for estimates arising from analysis of the survey.

Location	Registrants		Voters	
	Sample Size	Population	Sample Size	Population
Afghanistan	112	669	107	599
Iraq	70	638	62	501
Solomon Is	45	107	44	98
Timor-Leste	144	598	100	313
Total	372	2012	313	1511

2.10.3 Summary of the Evaluation

2.10.3.1 This summary collates comments into high level elements listed at paragraph 2.10.1.3 above.

2.10.3.2 Effectiveness and efficiency of the trial in providing a convenient, reliable and secure method of voting at Federal election for overseas ADF personnel.

- a. The trial demonstrated that remote electronic voting for personnel deployed in Defence operations overseas could provide a convenient, reliable and secure method of voting in a Federal Election. 1511 votes were cast using REV.
- b. The number of deployed personnel known to cast a vote at the 2007 Federal election was significantly higher at 1740 when compared with the 2004 Federal election. REV voting played a very important role in achieving this result.
- c. The registration process was resource intensive for Divisional Offices, mainly due to incomplete information initially provided to the AEC by trial participants, and a high number of REV applicants being enrolled at addresses other than those claimed for on their REV application form. Lessons learnt from the trial on these issues should allow more streamlined administrative processes in any future implementation of REV voting.
- d. The timeliness of receiving mail for some of the Defence personnel overseas, a key driver for the trial, remains an issue, albeit more limited, for the mail out of PINs to access remote voting.
- e. Most of those who registered for REV found out about the trial either through Force preparation training, or through information from their commanding officers or through word-of-mouth.
- f. Three-quarters of those who registered cast their vote using REV, but the proportion varied markedly between locations – many of those deployed to Timor-Leste were unable to cast a vote using REV because of “operational reasons”. Postal voting is used as an alternative to casting a REV vote, but the proportion using this option is comparatively small.
- g. Amongst the REV voters, there was a high level of satisfaction with the level of service that REV voting provided. The main issues raised with REV voting concerned the lack of privacy in casting a vote (16 survey respondents), particularly for those deployed to Timor-Leste and Afghanistan, and the speed that voters were able to log on and cast their vote – an issue of particular concern in the

Solomon Islands and Afghanistan. Both of these issues were raised by a small minority of voters in these locations. Despite the concerns about speed from respondents, the average time to cast a vote was 8.6 minutes after logging on.

- h. Those who used REV to vote were able to vote in a way that reflected their intentions, as evidenced by the relatively high number of BTL voters. However, the proportion of BTL voters was lower from those locations with reported poorer DRN speeds. Information on local candidates, how-to-vote from registered parties and independent candidates, and on GVTs would have further assisted REV voters in casting votes that fully reflected their intentions.
- i. The unit cost per vote in the trial was relatively high. Costs for a future implementation are difficult to forecast as they are contingent on the Government's decision on this issue.

2.10.4 Management of Risks of Electoral Offences and Outcomes

- a. The AEC put in a range of controls to minimise the risks of electoral offences associated with the REV system and its associated processes. These were subject to an independent audit with satisfactory outcomes.
- b. Improvements were suggested in a number of areas to more easily manage the risks.
- c. There have been no allegations of electoral fraud and no official complaints arising from the trial.

2.10.5 Defence Observations

2.10.5.1 The key observations from Defence were as follows.

- a. The DRN is capable of supporting electronic voting noting that alternative strategies were put in place to execute REV on the DRN. These alternative strategies specifically addressed accessibility by deployed ADF members to the DRN and complexities of the differing deployed systems.
- b. Considerable ADF coordination, management and resources were required in the implementation of the trial.
- c. Long lead times were required in the distribution of paper-based personal identification number (PINS) to ADF personnel to counteract the long distance and the sometimes unpredictable postal system. Future trials should consider removing the reliance on the postal system for the distribution of PINS.
- d. Regulation 62 resulted in some ADF personnel not being able to participate in the trial despite registering. Those ADF personnel who were in Australia at the time of issuing of the writ were excluded from participating in the trial even if they would be in the AO at the time of the election. ADF personnel frequently move in and out of operations at short notice. Future trials should, where possible allow all ADF personnel who have pre-registered for electronic voting and are in the deployed AO at the time of the election period to participate in electronic voting.

2.11 Future Options

2.11.1 Introduction

2.11.1.1 Set out below are suggested improvements prepared by the project team that may assist in any future trial. These relate to the following issues:

2.11.2 Staffing – AEC

2.11.2.1 This project needs dedicated resources not shared with other tasks. Suggested levels:

- a. EL1 Project Manager (reporting to an EL2 Section Manager)
- b. APS6 Project Officer
- c. APS6 Procurement Officer
- d. Shared resources
- e. EL2 Section Manager
- f. APS5 finance officer

2.11.2.2 The dedicated staff should have the following capabilities between them:

- a. Extensive electoral experience;
- b. High level project management;
- c. High level procurement skills, including complex requests for tender.

2.11.3 Staffing -Defence

2.11.3.1 Defence made available the necessary resources as required. These resources were made available from within Defence's existing resource allocation with the exception of the project manager, who was a professional service provider.

2.11.4 AEC-Defence

2.11.4.1 The Joint Steering Committee worked well, and should be implemented for any future such project.

2.11.4.2 Dedicated AEC and Defence Project Officers should remain in daily contact to ensure appropriate co-ordination between the organisations.

2.11.5 Defence

2.11.5.1 Defence successfully applied their project management methodology throughout the life of the project. All Defence board members were kept informed via monthly status reports.

2.11.6 Procurement

2.11.6.1 In the 2007 trial, CPG provisions for the procurement of a 'first good or service' were used to undertaking direct sourcing with a restricted tender.

- 2.11.6.2 For any future trial, the provisions for a 'first good or service' will no longer apply, and a much longer lead time must be allowed for procurement.
- 2.11.6.3 A best estimate for this activity is 12 months minimum from commencement of creation of the Statement of Requirements to signing a contract.
- 2.11.6.4 Any Tender should be for a minimum of one 'general election' with the option, at the AEC's sole discretion, for an extension of a second general election.
- 2.11.6.5 The Tender should also include the following elements:
 - a. A pilot of the offered system for preliminary testing on the DRN (or any other network selected for the trial) during the evaluation phase;
 - b. A requirement for the Contractor to provide staff in Canberra during the initial stages of design/system development; and
 - c. A requirement in the tender to deal with diacritical marks: the process used in the 2007 federal election should be identified as one possible option.

2.11.7 System Specifications

- 2.11.7.1 The specifications prepared by the Contractor may be able to be used to update the SOR for the next tender. Any new contract should include the requirement for new specifications to be prepared as part of the design.
- 2.11.7.2 The Contractor should provide staff in Canberra during the initial stages of design/system development.

2.11.8 Design

- 2.11.8.1 Some suggestions for a better design are:
 - a. Have ATL and BTL together, with the ability to enter one OR the other;
 - b. Do not set the size of the STE box as a function of the screen, rather make the box the biggest necessary to hold the full ballot paper; and
 - c. A 'zoom' function may be considered so the complete ballot can be shown on the screen initially.

2.11.9 Testing

- 2.11.9.1 The SOR must include a requirement for a comprehensive test plan, including test scripts to test every functionality from beginning to end. The SOR should include a sample of a script so there is no confusion.
- 2.11.9.2 Formal testing should be undertaken by AEC staff (or staff employed for that purpose) initially.
- 2.11.9.3 After fixing any major issues, usability (functionality) testing should be conducted using a mix of persons from the target audience; that

is, ADF personnel should be asked to participate in the usability testing (and any other target group if necessary).

- 2.11.9.4 Usability testing must be done separately to communication testing. Scripts for communication testing are not dependent on services provided by the contractor, so should be developed by AEC (for Data Centre to ICON communications) and DoD (for ICON to user communications.)
- 2.11.9.5 Final testing should be conducted by AEC staff (or staff employed for that purpose).
- 2.11.9.6 Full documentation should be maintained from all tests as input to the audit.
- 2.11.9.7 Formal reviews should be conducted after each testing session.

2.11.10 Audit

- 2.11.10.1 The Audit process worked well, however some suggestions are offered.
- 2.11.10.2 The tender for an auditor should be repeated for this process. This should be open tender, so some 3 months will be required to get the auditor on board. For this reason, this process needs to start earlier in the process than it did in 2007.
- 2.11.10.3 The auditable elements should be included in the SOR (similar to the last one) for the main tender as well, so the Contractor is not caught unaware.
- 2.11.10.4 An initial meeting should be held between the Auditor, the Contractor and AEC.
- 2.11.10.5 Schedule a complete month after the initial meeting for the audit to be conducted, with at least 2 weeks contingency time.
- 2.11.10.6 Full testing should be conducted so there are comprehensive records for the Auditor.

2.11.11 Working with AEC ICT

- 2.11.11.1 AEC ICT staff worked very well with both Defence and the Electronic Voting team to put in place an excellent technical solution. To repeat this success, ICT Infrastructure should appoint a single point of contact for this project.
- 2.11.11.2 The ICON link and hardware should be ordered earlier in the project, to ensure all is ready when testing is to commence.
- 2.11.11.3 It is suggested that the computer hardware be mandated in the Tender to fit with AEC's standards. This will allow earlier acquisition and a redeployment option for the equipment.

2.11.12 Working with Defence

- 2.11.12.1 Once the Project Board was established and a project manager engaged, communication and project governance was excellent.

- 2.11.12.2 For any future such project, the following suggestions are offered:
- a. Defence should again dedicate full time resources to the project, including ICT where possible and project management staff; and
 - b. Consider having AEC officers 'train the trainer' for presentations at force preparation training
 - c. The AEC should offer assistance at force preparation training to ensure the message is consistent;
 - d. If legislation/regulations restrict who can vote, the AEC should formally agree with Defence (HQJOC) a review processes for determining eligibility; and
 - e. If such a review is necessary, ask for a dedicated resource to undertake such review work.

2.11.13 Working with the AEC

- 2.11.13.1 Successful key relationships were established at the working level ensuring that key deliverables were implemented when required.

2.11.14 Legislation and Regulations

- 2.11.14.1 These will need to be reviewed in line with any varied government requirements.

- 2.11.14.2 Regulation 62 resulted in some ADF personnel not being able to participate in the trial despite registering. Those ADF personnel who were in Australia at the time of issuing of the writ were excluded from participating in the trial even if they would be in the AO at the time of the election. ADF personnel frequently move in and out of operations at short notice. Future trials should, where possible allow all ADF personnel who have pre-registered for electronic voting and are in the deployed AO at the time of the election period to participate in electronic voting.

2.11.15 Registration of REVS

- 2.11.15.1 The following suggestions are offered in designing any future form for registration:
- a. Include a note on the form to say that the REV's postal address where they will be at election time must be used;
 - b. Include the REV's name, rank and PMKeyS number; and
 - c. Include space for a 'camp' as well as the mandatory AFPO number.
- 2.11.15.2 It is suggested that DROs be instructed to enter the postal addresses uniformly as follows:
- a. AFPO XX, then any other information.
- 2.11.15.3 This can be in any line of the address but must be in the same line for all registrants, so sorting of REVs by location can occur.
- 2.11.15.4 Where REVs with no AFPO are to be registered, determine a uniform entry process so their location can be determined by a simple data sort.

2.11.16 Identification and Authentication

- 2.11.16.1 Consider the following alternatives for identification and authentication.
- a. Enrolment can be checked online, so perhaps REV's could be allowed to register online, including providing a password/identifier that the REV select
 - b. Consider providing a sealable envelope with the registration form, and ask the REV for a password when they register; The form can be sealed in the envelope so only the DRO will know; or
 - c. Consider distributing PINs (if necessary) via the REV's Internet email account (yahoo, hotmail).
- 2.11.16.2 In any event, a stronger identification and authentication methodology should be the aim for any future remote electronic voting.
- 2.11.16.3 If PINs are to be posted, registered mail should be used again, and an account established at Post so there are not the issues with franking that there were this time.

2.11.17 Hardware and Communications

- 2.11.17.1 Commence procurement of hardware earlier, and allow at least four months for delivery. This includes servers, racks and routers.
- 2.11.17.2 Check the lead time for ICON links, and double this when ordering the link.
- 2.11.17.3 Liaise with Defence in relation to configuration of routers early in the process.
- 2.11.17.4 Negotiate a communication configuration with Defence that allows AEC officers in West Block to have access to the server while it is connected to the DRN.
- 2.11.17.5 Look towards establishing some type of remote access for the contractor, if they are not based in Canberra. This might be a dialup line from the server, initiated by AEC staff at the server, only when the DRN is not connected.
- 2.11.17.6 Maintain the requirement for access from West Block to be from a secure room.

2.11.18 Election Data Load

- 2.11.18.1 Although in their project report (see above), the Contractor believes XML data might provide more opportunities, CSV data is available earlier and has all the data we need, excluding diacritical marks (XML will not have this either, as the host systems have single-byte databases).
- 2.11.18.2 The CSV format is more understandable, and easier to edit than an XML file.

- 2.11.18.3 The XML file has a lot of unnecessary data, and is difficult to edit in regards to diacritical marks.
- 2.11.18.4 A requirement should be included in the tender to deal with diacritical marks. The process used in the 2007 federal election could be suggested as one option.
- 2.11.18.5 Ensure a CSV file showing the relationship between states/territories and divisions is provided.
- 2.11.18.6 The checking process worked well, and should be repeated.

2.11.19 Voting period administration

- 2.11.19.1 Negotiate a communication configuration with Defence that allows AEC officers in West Block to have access to the server while it is connected to the DRN.

2.11.20 Post election processing

- 2.11.20.1 Post election processing worked very well, with all votes being decrypted and handled in accordance with established procedures.
- 2.11.20.2 For any future such processing, platinum express post should be used again, but the Division's street address, not the post office box, should be included.
- 2.11.20.3 Consider printing on coloured paper to make management of ballots in the counting centres easier.
- 2.11.20.4 If required, this would need to be stated in the Tender, so that House and Senate papers are printed in separate files.
- 2.11.20.5 It is suggested that faster printers be acquired.
- 2.11.20.6 Formatting of ballots should be better defined so all ballots can be printed without amending formatting 'on the fly'.
- 2.11.20.7 Consider having the output processing program print in PDFs. Again, this could be asked for in the Tender.

2.12 Conclusion

- 2.12.1.1 After considering the Contractor's project review and the independent evaluation, there is ample evidence to clearly state that the trial was a success from point of view of technology and participation.
- 2.12.1.2 The registration and participation rates were excellent, at 80% of eligible personnel registered and 75% of those voting.
- 2.12.1.3 Project governance worked very well, with the Joint Project Board maintaining control over all aspects of the project.
- 2.12.1.4 Coordination between Defence and the AEC was excellent once the project teams were defined, and both the relative project teams and ICT personnel worked untiringly to achieve an outstanding success.

- 2.12.1.5 The project teams have now been disbanded. If this project were to be repeated there would be a need for a longer time frame to allow for a full open tender process to be undertaken.
- 2.12.1.6 The success of this project is a solid foundation for the future, should the Australian government undertake further remote electronic voting.

APPENDICES

Appendix A

1.0 Supplementary Detailed Technical Report

1.1 INTRODUCTION

1.1.1 Purpose

1.1.1.1 The Supplementary Detailed Technical Report is provided to explain in greater technical detail the steps and process of the project.

1.1.2 Project Initiation

- 1.1.2.1 The AEC and Defence met to initiate the project on 6 October 2006, and a Project Board jointly chaired by senior executive officers from the two agencies met for the first time on 18 December 2006.
- 1.1.2.2 The Electoral Commissioner (EC) subsequently met with the Secretary of Defence and the Chief of Defence Force (CDF) on 24 October 2006 to agree in principle to the project's proposed outcomes.
- 1.1.2.3 The Project Board agreed to the scope of the project, and the EC wrote to the CDF in January 2007 to "to confirm the areas agreed for delivering remote electronic voting for overseas ADF Personnel".
- 1.1.2.4 The CDF responded in February, agreeing to the proposed arrangements. Text of the letter of agreement is included at Appendix B, and the project proceeded in line with that agreement.
- 1.1.2.5 After a comprehensive tender evaluation, Registries Limited (the Contractor), an Australian company based in Sydney, was chosen as the successful tenderer. Their major sub-contractor, Everyone Counts Inc., provided the voting software and has offices in Melbourne.

1.1.3 Summary of Contractual Requirements

- 1.1.3.1 Key contractual requirements are listed below.
- a. Software that allowed for full preferential voting for the House of Representatives, proportional representation for the senate and catered for a referendum if necessary.
 - b. The solution needed to be compatible with the ADF secure intranet (DRN) including a connection from an AEC stand-alone server where the voting application would reside, to the DRN via ICON. This connection included hardware encryption.
 - c. The contractor supplied, installed and supported the voting application and provided an interface to allow AEC staff to set up data for the election.

- d. The contractor developed and provided administration user guides to both AEC technical and election management staff.

1.1.4 Relative Responsibilities

- 1.1.4.1 The AEC and Defence had responsibilities for elements as shown below.

1.1.5 AEC Responsibilities

1.1.5.1 Business elements

- A. Coordinate resolution of system and security issues;
- B. Manage the procurement process and the resultant contract;
- C. Coordinate design, development and testing with input from Defence;
- D. Provide registration forms for remote electronic voters (REVs);
- E. Register REVs;
- F. Determine an identification and authentication protocol for REVs
- G. Prepare and dispatch PINs or any other authentication requirements to REVs;
- H. Have the electronic voting system available for REVs during the election period; and
- I. Coordinate a joint report in the post-election period;

1.1.5.2 ICT elements:

- A. Acquire and configure servers on which the voting system was installed;
- B. Acquire the ICON link from the AEC to Defence, including establishment of connectivity;
- C. Provide and configure routers (including hardware encryption) at either end of the link;
- D. Provide test and live data from the Election Management System (ELMS) to populate the House of Representatives and Senate ballots, Referendum question(s) where applicable, and electoral Divisions;
- E. Provide test and live elector data from the Roll Management System (RMANS);
- F. Provide level 2 Help Desk support during the election period;
- G. Assist with the resolution of systems and security issues;
- H. Participation in the tender evaluation; and
- I. advice and other support as necessary.

1.1.6 Defence Responsibilities

1.1.6.1 Business elements

- A. Provide input into the AEC's software system statement of work
- B. Coordinate Defence's participation in the resolution of system and security issues;
- C. Promote participation in the trial, including registration of REVs;
- D. Assist AEC with REV registration
- E. Encourage REVs to vote
- F. Provide access to ADF personnel to enable the casting of electronic votes;
- G. Participate in a joint reporting process in the post-election period

1.1.6.2 ICT elements:

- A. Participation and assistance to AEC in the AEC software procurement process
- B. Acquire and configure Citrix servers and network equipment required for remote electronic voting of Defence sites;
- C. Work with AEC ICT staff to establish ICT connectivity between the organisations;
- D. Manage the software testing process of elements for the Defence environment;
- E. Acquire and configure deployed SOE platforms for testing in Australia;
- F. Test the remote electronic voting system for compatibility and operability with the Defence Restricted Network (DRN);
- G. Establish an remote electronic voting intranet page within the DRN for access AEC's remote electronic voting system;
- H. Provide level 1 Help Desk support during the election period;
- I. Provide guidance on the security aspects with regard to software and hardware;
- J. Provide guidance on the performance of electronic voting software;
- K. Develop a business and technical support model to handle all enquiries from the deployed areas and integrate this support model with the AEC;
- L. Develop an implementation plan with regard to the rollout of electronic voting capable laptops in deployed areas;
- M. Establish an online help guide for deployed technical staff;
- N. Provide Defence ICT reports for the tender process and two major points within the field test cycles in determining probability of successful deployment;
- O. Participation in the tender evaluation; and
- P. advice and other support as necessary.

1.1.7 Security Restrictions

1.1.7.1 As already mentioned, the trial was subject to the satisfactory resolution of systems and associated security issues. To ensure security of the votes, the following basic design elements were determined:

- a. The server storing the votes would be housed in the AEC's data centre although logically part of the DRN;
- b. Connectivity between the servers and Defence would be via ICON, the Intra-government Communications Network in Canberra;
- c. Data on ICON would be hardware encrypted; and
- d. Access to voting would only be available via the Defence Restricted Network (DRN).

1.1.8 Defence Restrictions

1.1.8.1 Defence determined that this trial would be restricted to the major overseas areas of operation (AO):

- a. Afghanistan;
 - b. Iraq;
 - c. Timor-Leste; and
 - d. Solomon Islands.
- 1.1.8.2 Defence also advised that operational tasking may preclude some members from participating in the trial.

1.1.9 Technical Restrictions

- 1.1.9.1 In discussing the process for voting remotely, Defence requested that HMA Ships be specifically excluded from the trial due to bandwidth and connectivity constraints.

1.1.10 Scope Change

- 1.1.10.1 Changes to the project scope were carefully considered by the Project Manager in consultation with the Defence project team to ensure the project remained adequately funded, resources were available and to ensure that the project was delivered on time for the 2007 election.
- 1.1.10.2 Prior to implementation, all scope changes or adjustments had the consent of the project sponsor and involved consultation with all stakeholders.

1.1.11 High Level Deliverables

- 1.1.11.1 Project deliverables were as follows:
- a. Legislation and regulation changes to enable the trial;
 - b. Acquisition of a solution;
 - c. Software development and implementation;
 - d. Hardware development and implementation;
 - e. Public awareness, voter registration and PIN distribution;
 - f. Certification of the system by an independent auditor; and
 - g. Security accreditation.
 - h. Report into the trial of remote electronic voting, including evaluation and analysis

1.1.12 Exclusions

- 1.1.12.1 The project scope did not include the following:
- a. Overseas ADF personnel outside the four selected AOs; and
 - b. Personnel deployed in the selected AOs serving on submarines and surface ships due to bandwidth and connectivity restraints.

1.1.13 Project Constraints

- 1.1.13.1 The following constraints applied to the project:
- a. The necessary legislation and regulations must be in place to allow the trial to proceed; and
 - b. The contractor provided solution and associated software was to be certified and ready for deployment prior to an election being announced.

1.1.14 Evaluation

- 1.1.14.1 Two evaluations were conducted for this project, excluding this joint report.
- a. The Contractor reviewed the project from the point of view of services provided and a summary of this evaluation is contained in the section “Contractor’s Project Review’.
 - b. AEC’s People and Performance Branch commissioned an independent evaluation and a summary of this evaluation is contained in the section “Independent Trial Evaluation”.
- 1.1.14.2 This joint report examines both of these evaluations. A summary of “Future Options” is contained in the section of that name, and the final section, “Conclusion”, summarises this report.

1.2 Project Management

1.2.1 Introduction

- 1.2.1.1 This section covers the following subjects:
- a. Project governance;
 - b. Project planning and resourcing;
 - c. Defence project management;
 - d. AEC project management;
 - e. Project governance controls;
 - f. Risk and issue management; and
 - g. Project schedule.
 - h. Costs

1.2.2 Project Governance

- 1.2.2.1 Given the significant importance and emphasis placed on the trial by senior management from both organisations, it was recognised early that a strong governance arrangement was required.
- 1.2.2.2 As well, the project was complex given that a dedicated commitment was required both from the AEC and Defence, and from elements of the ADF.
- 1.2.2.3 For these reasons, a comprehensive project management regime was required.
- 1.2.2.4 Governance arrangements were established at the outset of the project with the establishment of a Project Board jointly chaired by AEC (First Assistant Commissioner Electoral Operations) and Defence (Director General Executive – Personnel).
- 1.2.2.5 The terms of reference for the joint AEC/Defence Project Board were:
- a. Provide overall direction of the project;
 - b. Ensure the deliverables of the respective organisations;
 - c. Arbitrate on issues that were unable to be resolved at the working level; and

- d. Provide ministerial briefings on the progress of the project.
- 1.2.2.6 The EC, the Secretary, and the CDF agreed on an exchange of letters to define working arrangements for the project. The project board agreed on these arrangements, the EC wrote to the CDF on 7 February 2007. The CDF formally agreed with the proposals communicated by the EC. The text of the EC's letter is at Appendix B.

1.2.3 Project Planning and Resourcing

- 1.2.3.1 AEC and Defence utilised their own project management methodologies in the management of their assigned deliverables.
- 1.2.3.2 As outlined in the letter of agreement at Appendix B, each agency was to provide its own resources. The AEC was funded to implement the relevant JSCEM recommendations.
- 1.2.3.3 Full details of costs are included in the Costs section below.

1.2.4 Defence Project Organisation

- 1.2.4.1 The PRINCE2 project management methodology was used by Defence to manage its specific deliverables. An internal Defence Project Board was established including stakeholder representation from key Defence Groups including Personnel Executive, Chief Information Officer Group (CIOG), Defence Materiel Organisation (DMO) and Headquarters Joint Operations Command (HQJOC).
- 1.2.4.2 The key stakeholders for Defence were as follows:
 - a. Personnel Executive (PE) were appointed as the responsible authority within Defence for the remote electronic voting trial. This included responsibility for direct liaison between Defence and the AEC and coordination of the whole-of-Defence involvement in the trial. PE involvement was headed by Director General Personnel – Executive, a Project Director and a dedicated Project Manager.
 - b. The CIOG were the technical authority for Defence and were responsible for the information communication technology (ICT) project management and associated deliverables. This included solution infrastructure design, ICT support model design, providing ICT advice and assistance to the AEC, test management and ensuring that the necessary approved changes were made to the Defence ICT infrastructure. CIOG involvement was headed by Assistant Secretary Application Development, Project Director and a dedicated Project Manager.
 - c. The DMO were responsible for assisting and advising CIOG in the initial design of the remote electronic voting system. DMO involvement was headed by Director General Command and Support System.
 - d. HQJOC were responsible for assisting and advising AEC regarding the distribution of electoral matter to, from and within the respective areas of operation. HQJOC also (a) coordinated ADF advice and assistance to AEC on the registration process,

(b) provided coordinated assistance to CIOG in the setup of necessary equipment and testing of the system in the areas of operation (c) coordinated trial awareness and promotion in the areas of operation; and (d) post trial evaluation. HQJOC involvement was headed by Director General Support, Director Personnel and Staff Officer 1 Personnel Plans.

- e. Army who assisted CIOG in making available the necessary resources during some of the system testing.
- f. Other stakeholders included Defence Signals Directorate (DSD) providing technical assistance and support regarding Australian government ICT security standards.

1.2.4.3 Defence engaged a Project Director and dedicated Project Manager to manage the project on behalf of the Defence Project Board. A “point of contact” was appointed from each of the major stakeholder groups, responsible for managing their group’s stakeholder input (including resources) for the trial.

1.2.4.4 Defence’s detailed project planning is contained within its ‘Project Initiation Document’ outlining the project description, project organisation, business case, project plan, project quality plan, communication plan, product breakdown structure and schedule. The Project Initiation Document was endorsed by the Defence Project Board on 12 December 2006.

1.2.5 AEC Project Organisation

1.2.5.1 The AEC used its standard project governance methodology for this project. Key roles in that methodology for this project have been as follows:

- a. Steering Committee Chair –First Assistant Commissioner Electoral Operations;
- b. Project Sponsor –Assistant Commissioner Elections;
- c. Project Manager –Director, Electronic Voting; and
- d. Working Party:
 - A. Project Manager
 - B. Assistant Director, Electronic Voting; and
 - C. Two Project Officers.

1.2.5.2 The AEC’s project management plan was approved in January 2007.

1.2.6 Project Governance Controls

1.2.6.1 The following key controls were established at the outset of the project to provide assurance to the joint AEC/Defence Project Board on the progress of the project:

- A. Regular meetings between Defence and AEC Project Teams;
- B. Monthly Defence highlight status reports reporting issues to the to key stakeholders within Defence and AEC;
- C. Regular AEC/Defence Project Board meetings;

- D. Regular contract management meetings including status reports between the AEC and the Contractor;
- E. Regular status reports to the Defence Senior Leadership Group;
- F. Regular status reports to the AEC Executive; and
- G. Regular Ministerial Submissions to Special Minister of State and Minister of Defence.

1.2.7 Risk and Issue Management

- 1.2.7.1 The Government response to JSCEM's recommendation 43 stated that the trial of remote electronic voting for overseas Australian Defence Force (ADF) personnel was to be subject to the satisfactory resolution of systems and associated security issues.
- 1.2.7.2 The AEC and Defence jointly identified the risks in this area and subsequent mitigation or resolution for each of those risks during the planning phase in December 2006 and January 2007. In February, the AEC provided these details to the Special Minister of State (SMOS) together with a recommendation that the trial should proceed.
- 1.2.7.3 The Minister agreed with this recommendation on 22 February 2007. The details of risks provided to the Minister are included at Appendix C.
- 1.2.7.4 The AEC and Defence managed risk in accordance with their organisation's project management methodologies.

1.2.8 Defence's risk management:

- 1.2.8.1 Defence used the Australian Standard 4360 for risk management with key risks regularly reported to the Project Board in the Defence monthly highlight status reports.
- 1.2.8.2 In the event of a risk or issue being forecast to exceeding the agreed tolerance as set out of the Defence Project Board, the Defence Project Manager immediately advised the Defence Project Board Executive.
- 1.2.8.3 Issues that resulted in the potential slippage of key milestones by Defence and/or AEC were immediately confirmed between AEC and Defence and if the slippage could not be rectified, the issue was escalated to the Joint AEC/Defence Project Board.

1.2.9 AEC's risk management

- 1.2.9.1 In relation to the identification of risk during design, development and testing, the tender required that the successful tenderer provide a risk management plan as part of their project plan.
- 1.2.9.2 The Contractor established the following procedures as part of the risk management plan:
 - a. A Risk Inventory and Assessment Register was maintained by the Contractor;

- b. Apart from the initially identified risks, additional risks could be included in the Register via completion of a Risk Inventory Assessment Worksheet;
- c. A Risk Mitigation Plan was prepared for the project, and all risks in the Register were covered in this plan; and
- d. All outstanding risks were raised at each contract management meeting.

1.2.10 Schedule

1.2.10.1 A joint summary of the key activities/events is listed below. A detailed schedule is contained at Appendix E.

Dates	Activity/Milestone
26 Oct 06	Project Start
12 Jan 07	Statement of Requirements finalised and Tender Released
2 Feb 07 to 2 Apr 07	Tender Evaluation
15 Mar 07	Assent for amendments to Legislation
Early April 07	Tender Evaluation Report
18 May	Contract Signed for REV software
May/Jun 07	System Software Development
25 May to 25 Jun 07	System testing on Defence infrastructure
1 August 07	Effective date Legislation Regulations
6 Sep 07	Legislative Regulations approved
9 Aug 07 to 1 Nov 07	Registration for trial
4 July 07 to 31 August 07	Independent audit
14 September 07	System certified by auditor
8 Oct to 5 Nov 07	Personal Identification Numbers (PINS) issued to trial participants
14 Oct 07	Federal election announced
9 Oct 07	Final System Signoff
5 to 24 Nov 07	Electronic Voting period for 2007 Federal Election
Dec 07 to Feb 08	Evaluation of trial
Jan/Feb 08	Report into Trial of Remote Electronic Voting
End May 08	Project Close

1.3 Costs

1.3.1 AEC costing model

- 1.3.1.1 The AEC took actual expenditure against salary (for the dedicated project team), operating expenses and capital for the period from project commencement to 31 January 2008, and included projected costs until the end of the 2007/2008 financial year.
- 1.3.1.2 These projected costs were for finalisation of the project and shutdown of the hardware after the close of the Court of Disputed Returns.

1.3.2 Defence costing model

1.3.2.1 Defence received no additional funding or resources for the conduct of the trial. Existing resources were reprioritised by Defence to conduct the trial.

1.3.3 AEC Costs

1.3.3.1	Total	\$786,915
	a. Salary	\$245,375
	b. Operating Expenses	\$375,754
	c. Capital	\$165,786
1.3.3.2	Special items (included above)	
	a. Total contractor costs	\$479,186
	b. Audit	\$59,801

1.3.4 Defence Costs

1.3.4.1	Total	\$964,000
	a. Salary	\$582,000 ³
	b. Operating Expenses	\$382,000

1.3.5 Cost Per Vote

1.3.5.1 The cost per vote to the AEC was \$521.00.

1.3.5.2 When both Defence and AEC costs are combined the cost per vote is \$1159.00.

1.4 Legislative Framework

1.4.1 Legislation

1.4.1.1 The Government's response to JSCEM's report was presented to the Parliament on 31 August 2006. In its response, the Government supported Recommendations 41 and 42, and supported in principle recommendation 43. The Government limited the trial to Australian Defence Force personnel for Recommendation 43.

1.4.1.2 Finance had previously submitted a bid for a Bill for introduction in the Spring sittings 2006 which had been given 'A' status. The Cabinet Submission covering the Government response provided the policy authority for a Bill to be drafted to make the necessary amendments to the CEA.

1.4.1.3 A team was formed in the AEC to work on the Bill. In consultation with the Minister's Office and the Electoral Policy Unit of Finance, Drafting Instructions were prepared. These were provided to the

-
- Salary costs include direct salary comprising annual salary, allowances and accrued expenses (superannuation and accrued leave). Salary costs for ADF members also include indirect salary.
 - Figure excludes fixed overheads.
 - Unit Costs used in calculations are sourced from Defence Financial Manual (4).
 - Calculations are based upon the estimated days worked by Defence resources for the trial for the period covering project commencement to end of January 2008.

Office of Parliamentary Counsel (OPC) on 13 October 2006 under Finance's letterhead. During this period, the Minister wrote to the Prime Minister to seek an upgrade to category 'T' status for the Bill. While it was recognised that it was impossible to introduce the Bill in the first week of the Spring sittings, the higher category would ensure that drafting resources were available at OPC.

- 1.4.1.4 The Bill was prepared over a six week period with numerous meetings with OPC and the provision of many draft Bills. Clarification on policy was sought from the Minister as the need arose. The key decision that was made early on was for the Bill to establish a legal framework which would provide for regulations to be made to supply the necessary details. One reason for this approach was that the technical aspects of the electronic voting equipment were still being determined and the contracting process was still underway.
- 1.4.1.5 There were two further important elements of the Bill. The first was limiting the trial to the first elections and referendum held after the Bill was given Royal Assent. The second was to provide the Minister with the capacity to decide for any reason not to proceed with the trials.
- 1.4.1.6 The Bill that became the Electoral and Referendum Legislation Amendment Act 2007 (Amendment Act) was introduced into the House of Representatives on 30 November 2006. The Bill was referred to the Main Committee for consideration and was passed by the House of Representatives on 6 December 2006.
- 1.4.1.7 The Bill was then introduced into the Senate on 7 December 2006. On that same day the Bill was referred to the Senate Finance and Public Administration Committee for inquiry and report by 20 February 2007. The AEC made a seven-page submission to the Committee's inquiry essentially outlining the provisions of the Bill. The Committee's report was tabled on 26 February 2007, recommending that the Senate pass the Bill. The Senate passed the Bill on 26 February 2007. Royal Assent was given on 15 March 2007.
- 1.4.1.8 Upon Royal Assent all of the provisions providing for the electronic voting trials commenced. Schedule 2 of the Amendment Act amended the Commonwealth Electoral Act 1918 (Electoral Act) to insert a new Part XVB into the Electoral Act. Division 1 provided for a trial of electronically assisted voting for sight-impaired people while Division 2 provided for a trial of remote electronic voting for defence personnel serving outside of Australia. Schedule 2 also amended the Referendum (Machinery Provisions) Act 1984 (Referendum Act) to insert a new Part IVA into the Referendum Act. Division 1 provided for a trial of electronically assisted voting for sight-impaired people while Division 2 provided for a trial of remote electronic voting for defence personnel serving outside of Australia.

- 1.4.1.9 Section 202AB limited the trials to the first general election, and the first Senate election, held after the commencement of section 202AB. Section 73M limits the trials for voting at the first referendum held after the commencement of the section and only if that referendum is held on the same day as the first general election after the commencement of section 202AB.

1.4.2 Regulations

- 1.4.2.1 Following the passage of the Bill through the House of Representatives, work commenced on preparing drafting instructions for the regulations. Instructions were prepared and circulated to Elections Branch and the Electronic Voting Section for comment. Following a series of consultations, instructions were provided to the Office of Legislative Drafting and Publishing on 22 December 2006.
- 1.4.2.2 The regulations went through a series of drafts as policy was refined and technical attributes were finalised. Due to the complexity and scope of the proposed regulations, the regulations took some time to finalise. As a consequence of this, the regulations were drafted to commence retrospectively on 1 August 2007. Advice from the Australian Government Solicitor was obtained before these instructions were issued. Having the regulations commence retrospectively ensured that there was no risk attached to any action undertaken by the AEC in relation to registering remote overseas electors.
- 1.4.2.3 During the drafting phase comments were sought from the Attorney-General's Department and the Defence during the drafting process. The Attorney-General's Department provided advice in relation to the offence provisions contained in the proposed regulations.
- 1.4.2.4 The regulations affected the administrative responsibilities of three other Ministers: the Attorney-General in relation to human rights issues surrounding the electronically assisted voting trial; the Minister for Defence in relation to defence personnel; and the Minister for Justice and Customs in relation to the offence provisions in the regulations. Formal approval was sought from the Minister for Justice and Customs for the offence provisions, while support for the regulations was sought from the Attorney-General and the Minister for Defence.
- 1.4.2.5 The Governor-General made the regulations on 6 September 2007 and they were registered on the Federal Register of Legislative Instruments on 11 September 2007. The regulations were tabled in the Senate on 13 September 2007. In a letter dated 20 September 2007, Senator Watson, as Chairman of the Senate Standing Committee on Regulations and Ordinances, wrote to the Minister raising some concerns with the drafting of some of the e-voting regulations. A brief covering a proposed response to Senator Watson was provided to the Minister in September 2007.

- 1.4.2.6 Following the registration of the regulations, on 24 September 2007 the Electoral Commissioner determined the four countries in which the trial would take place for remote electronic voters. The Electoral Commissioner's determination was gazetted on 25 September 2007. A similar determination for the places, days and hours where electronically assisting voting would be available was gazetted on 2 November 2007.

1.4.3 Interpretations

- 1.4.3.1 Legal advice was sought on a number of matters when drafting the regulations or to clarify the operation of the Act and regulations. Advice was provided by the Australian Government Solicitor in relation to providing a commencement date for the regulations earlier than the registration date. This approach enabled administrative activity to commence before the regulations were made.
- 1.4.3.2 Advice was also provided on the wording of the REV registration form, in particular the declaration to reflect the wording of the Act and to enable defence personnel to register as GPVs if for some reason their application for registration as a REV failed.
- 1.4.3.3 Advice was also provided on whether scrutineers were able to be present at the printing of the REV ballot papers. The advice noted that regulation 68 provided for scrutineers to be present to observe the printing and bundling of REV ballot papers, but not the ability to closely examine the printout of the ballot papers.

1.5 System Acquisition

1.5.1 Procurement Process Overview

- 1.5.1.1 Shortly after government approval was granted for a trial of electronic voting trial for overseas ADF personnel, the AEC procurement process began.
- 1.5.1.2 In considering the procurement methodology, it was noted that the Victorian government, in their tender for electronic voting services, received some 35 responses, thereby requiring a prolonged evaluation period.
- 1.5.1.3 As the AEC's project did not commence until September 2006 and a solution was to be available for deployment by 30 June 2007, an abbreviated procurement methodology was necessary.
- 1.5.1.4 Section 8.65(g) of the Commonwealth Procurement Guidelines provides for an exemption to the mandatory provisions for procurement of first good or services intended for limited trial. In light of this provision the Delegate approved a direct sourcing process to obtain the services to develop and implement an electronic voting application to provide the limited trial of remote electronic voting.
- 1.5.1.5 The following organisations were selected to participate in the direct sourcing for the reasons indicated:

- a. Hewlett-Packard Australia Pty Ltd – this company provided the Victorian Electoral Commission’s solution.
 - b. Software Improvements Pty Ltd – this company provides the ACT Electoral Commission’s solution; and
 - c. Registries Limited – this company provided online voting for the AEC’s Certified Agreement vote in 2002.
- 1.5.1.6 This section discusses the following topics:
- a. Request for Tender;
 - b. Tender evaluation;
 - c. Approvals; and
 - d. Recording.

1.5.2 Request for Tender

- 1.5.2.1 The Statement of Requirements included in the tender is at Appendix D.
- 1.5.2.2 This document was iteratively developed by AEC with input from Defence. Defence advised of the technical requirements to allow the system to work within the DRN, with the AEC focusing on the statutory and operational requirements of conducting a federal election.
- 1.5.2.3 There were two important areas of the SOR that should be mentioned at this stage.
- a. Systems and associated security issues, discussed under Project Governance above, were specifically included in the SOR together with the methodology already determined to address these issues. Vendors were to confirm that they could meet the risk minimisation or resolution in their responses.
 - b. It was imperative that the acquired system operate within the DRN. To this end, the SOR required tenderers to provide a pilot system to determine compatibility of the offered software with Defence’s various software levels. The results of the pilot tests proved invaluable in the tender evaluations.
- 1.5.2.4 Tender documentation with an invitation to respond was issued by email to the above organisations, and all organisations acknowledged receipt of the documentation.
- 1.5.2.5 The AEC conducted an industry briefing on 18 January 2007. At this briefing the AEC provided an overview of the requirements and outlined the electoral process.
- 1.5.2.6 A range of clarification questions were raised by the invited parties and subsequently answered by the AEC.
- 1.5.2.7 Tenders were received by the closing date and time from the three organisations that were invited to submit Tenders.

1.5.3 Tender Evaluation Plan

- 1.5.3.1 The Delegate approved the Tender Evaluation Plan (TEP) on 1 February 2007. Under this Plan, an independent party was

required to act as the probity advisor. Deacons Projects was appointed to this role, and reviewed each of the following documents before approval by the Delegate:

- a. the Tender;
- b. the Tender Evaluation Plan; and
- c. the Tender Evaluation Report.

1.5.4 Tender Evaluation Committee

1.5.4.1 The Tender Evaluation Committee (TEC) consisted of personnel occupying the following positions.

Position	Title	Organisation
Chairperson	Director National Procurement	AEC
Member	Assistant Director Electronic Voting	AEC
Member	Assistant Director IT Applications	AEC
Member	Director Defence Personnel Systems	Defence
Secretariat	Project Officer Electronic Voting	AEC
Technical Advisor	Director Electronic Voting	AEC

1.5.4.2 The Plan also provided for additional specialist advice to be called upon as follows.

- a. AEC's Manager, Budgets provided specialist advice for the financial risk assessment.
- b. Further technical expertise was provided from Defence's CIOG and AEC's ITC Infrastructure Management Section.

1.5.4.3 These appointments are recorded on file. In accordance with the plan, each of these officers completed Conflict of Interest Declarations and Confidentiality Agreements.

1.5.5 Evaluation Process

1.5.5.1 The evaluation was conducted in accordance with the Tender Evaluation Plan. It progressed through six stages of discrete evaluation. At each of these stages offers could be rejected after assessment by the TEC for failure to comply or unsatisfactory technical solutions.

1.5.5.2 Stage 1 Assessment – Conditions for Participation

- a. This provided the initial assessment of tenders to determine compliance with the Conditions for Participation. As this procurement was direct sourcing, there were no conditions for participation.

1.5.5.3 Stage 2 Assessment – Minimum content and format.

- a. Stage 2 was the assessment of tender responses to determine compliance with the minimum content and format requirements as specified in the request documentation. The TEC recorded the agreed results of this stage. All Tenderers proceeded to Stage 3.

1.5.5.4 Stage 3 Assessment – Functional and Performance.

- a. The overall weighting for the Functional and Performance Criteria grouping represented 90% of possible technical score. The TEC's evaluated the tenderers response to all elements of the Functional and Performance evaluation criteria.
- b. The initial assessment identified that the Stage 3 evaluation response element table contained clauses that referenced the Pricing Schedule. The TEC elected not to assess these elements at this stage to ensure a continued separation of the technical and pricing elements at that time.
- c. As a result of the initial assessment, a number of issues were identified for clarification. Clarification questions were put to each respective Tenderer with arrangements made for them to provide the answers at a presentation convened by the AEC.
- d. The TEC chair authorised the expansion of the committee to include technical ICT expertise from Defence and AEC.
- e. Presentations were held on 15 February 2007, and each Tenderer was allowed 45 minutes. While aspects of the submitted tenders were clarified no new information that had not been previously outlined in the original response could be provided during the presentations.
- f. In conjunction with Stage 3 evaluation a Test Pilot was organised. The purpose of the pilot was to test the compatibility of the offered solutions on the Defence network. The tenderers were provided with a script template to enable the scripting of the testing for their solutions.
- g. Network traffic captures were performed on the 20th February 2007, from two workstations in the test environment at Defence's Russell offices. CIOG staff captured all transactions involved in the electronic voting process from both SOE124 and SOE125 workstations. The intention of this test was to see how each of the proposed software packages generally handled a transaction with regard to creating network traffic. While being a limited trial (not end to end) this was sufficient in enabling a high level comparison.
- h. On 28 February 2007 the TEC met to consider the information from the presentations and the responses to the clarification questions and the results of the pilot test. All the initial scoring was reconsidered in light of the presentations and answers to clarification questions. Finally, the Test Pilot results were also taken into account.

- i. One solution offered proved to be incompatible during testing and together with other ratings that identified less technical worth, was not considered for further stages of assessment.

1.5.5.5 Stage 4 Assessment– Capacity and Capability.

- a. This stage assessed whether the Tenderers' had demonstrated capacity and resources to deliver the services for which it is tendering, had demonstrated capacity and level of knowledge to deliver services and an understanding and preparedness for the risks associated with the delivery of the solution.
- b. Financial and Legal risk assessments were also considered as part of this stage. These ratings were included with the overall score rankings. Both the remaining offers advanced to the next stage.

1.5.5.6 Stage 5 Assessments – Price Analysis.

- a. The TEP requires that an analysis of the submitted price and any offered discounts and other pricing mechanisms will be conducted, as required, to determine an equitable basis of price comparison for the requirement. As well, each major element of the pricing schedule was compared and an assessment conducted of the competitiveness of each element to determine whether further price related risks were identified.
- b. At the completion of Stage 4, a Technical Adviser to the TEC conducted the price analysis. In the role as Technical Advisor this person was not involved in the deliberations and assessments undertaken by the TEC. The TEC members considered the price analysis and agreed with the results that the Technical Advisor had provided.

1.5.5.7 Stage 6 - Value for Money.

- a. The TEP states that this Stage consists of the following steps in order to determine the tender that provides the best value for money to the Commonwealth:
 - A. Consideration of overall risk associated with the tenderers' processes, general operations and price;
 - B. Technical worth including the impact of risks identified throughout the evaluation process; and
 - C. Consideration of price.
- b. On completion of the risk assessment the value for money formula was applied to the accrued evaluation scores. Issues to be resolved during contract negotiations were then identified and a recommendation for a preferred service provider made to the delegate.

1.5.6 Approvals

- 1.5.6.1 On 11 January 2007, the FACEO approved the issue of a Request for Tender and provided FMA9 and FMA10 approval for that purpose.

- 1.5.6.2 On 3 April 2007, the FACEO approved the Tender Evaluation Report, which selected Registries Limited (the Contractor) as the preferred tenderer.
- 1.5.6.3 Contract negotiations commenced soon after this date with an agreement entered into by the parties dated 18 May 2007.

1.5.7 Recording

- 1.5.7.1 Copies of all relevant evaluation documents and attachments are part of the Tender Evaluation Report AEC06/63 have been placed on file.

1.6 Design, Development, Testing and Certification

1.6.1 Software Design

- 1.6.1.1 The basis for the design of the system was the statement of requirements contained in the tender, supplemented by information provided by the Contractor in their tender response. This then formed the “SERVICES TO BE PROVIDED” schedule in the Contract.
- 1.6.1.2 The AEC and Defence then met with the Contractor on 17 April 2007 to commence detailed design of the system.
- 1.6.1.3 As a result of that meeting, the Contractor provided an initial draft of the Business Requirements document.
- 1.6.1.4 This document was updated regularly over the life of the project. The final version was provided, complete with last minute changes included in the lead up to the audit, in December 2007.
- 1.6.1.5 A key difference in the AEC’s requirements compared with other elections provided by the Contractor was that the election setup was to be carried out by AEC staff. Previously, the Contractor took the elector and election data and loaded the election on behalf of the customer. To ensure that the AEC maintained responsibility for all aspects of the federal election, this model necessarily changed.
- 1.6.1.6 Set out below are the differences between the two models.

Item	2007 Federal Election	Contractor’s ‘normal’ model
Physical Server location	AEC’s secure data centre	Contractor’s secure data centre
Elector management: <ul style="list-style-type: none"> • PIN creation and issue; and • Load of elector data 	AEC staff	Contractor staff
PIN issue process	By post	By email (generally)
Elector access to voting application	Defence Restricted Network/ICON	Internet
Election data load	AEC staff	Contractor staff
Post election processing	AEC staff	Contractor staff

1.6.1.7 Possible improvements:

- a. The interface used to run the election was designed for use by the Contractor's technical staff. The interface needs to be more user-friendly and usable by non-technical election administration staff.

1.6.2 Data Files

1.6.2.1 The Tender stated that data would be available in delimited format. During the project review with the Contractor, it emerged that XML 'media feed' files may have allowed more flexibility.

1.6.2.2 However as the Contractor had bid on the basis of processing delimited files, this format was supplied by the AEC.

1.6.2.3 The load process required the following data:

- a. Event.csv
 - the file with the election identification number (13745 for the 2007 federal election), election name, date, and elements of the election (House, Senate and Referendum);
- b. Divisions<extract data time>.csv
 - the list of electoral divisions for the election;
- c. Elector.csv
 - the list of registered electronic voters;
- d. Parties<extract data time>.csv
 - the list of political parties participating in the election;
- e. HouseCandidates<extract data time>.csv
 - the list of House of Representatives candidates;
- f. States<extract data time>.csv
 - the list of states, that is, the list of electoral divisions for the Senate;
- g. SenateCandidates<extract data time>.csv
 - the list of Senate candidates; and
- h. Groups<extract data time>.csv
 - the list of group voting tickets for the Senate.

1.6.3 Development

1.6.3.1 Development was an iterative process, with AEC staff reviewing the voting application and providing feedback on required improvements or fixes.

1.6.3.2 This development was initially carried out on the Contractor's secure server, with project staff accessing the draft application via Internet. This process allowed a rapid turn around of changes, as the developers would update the application on the server with the changes available almost immediately.

1.6.3.3 Once initial development was complete, the application was loaded on to the servers in the AEC's data centre, and testing continued both via the DRN and the EOPC.

1.6.4 Testing

1.6.4.1 During contract negotiation, it was agreed that the Contractor would provide a test plan, and the AEC expected that this would include comprehensive scripts.

1.6.4.2 The Contractor was of the view that the AEC would write the scripts to suit its use of the system. The AEC project team's view was that the Contractor should write the test scripts as the Contractor knew the expected response by the application.

1.6.4.3 The Contractor did provide a limited set of scripts, and testing of the voter interface was performed using these as a basis. From these, CIOG adapted and prepared numerous scripts and variations to assist in testing on the different platforms. In addition, an AEC User procedural manual was also commissioned as part of the project.

1.6.4.4 The test scripts only supported the actual voting process as it would be performed by ADF personnel, and did not provide for a 100% check of the system, end to end.

1.6.4.5 This caused some problems during the formal audit, as insufficient evidence was available as to the range of tests undertaken. The AEC project team was, however, able to provide additional documentation so that the audit was completed successfully.

1.6.4.6 The system was extensively tested on multiple simulated deployed technology platforms in Canberra, as well field tested as shown below.

1.6.4.7 Major field testing was conducted as follows.

- a. North Queensland (Exercise Operation Talisman Sabre), from 4 to 8 June 2007;
- b. Remote testing from Iraq, Afghanistan, Timor-Leste, Solomon Islands on 25-Jun-07;
- c. Solomon Islands from 20 to 23 August 2007; and
- d. Final validation of all DRN terminals in all target AOs on 17 October 2007.

1.6.4.8 CIOG performed in excess of 12 independent cycles of testing with the software and underlying hardware.

1.6.4.9 The AEC and Defence undertook a comprehensive system acceptance process prior to deployment of the production system.

1.6.4.10 Both agencies confirmed in September 2007 that the information system and support procedures were ready for the 2007 Federal election, and the final System Acceptance document was sign by the Joint Project Board Chairs in October 2007.

- 1.6.4.11 Possible improvements: Any future tender must include the requirement for a complete test plan, including comprehensive scripts to test every facet of the process end-to-end.

1.7 Hardware and Communications

1.7.1 AEC-Defence Connectivity

- 1.7.1.1 As already stated, the physical voting servers were located in AEC's secure data centre. When connected via ICON to the DRN, these servers were effectively an extension of the DRN network. Defence security restrictions did not allow the AEC to have connectivity to the servers when they were connected to Defence. A diagram of the system is contained within Appendix I.
- 1.7.1.2 Access was, however, required to the server for the following purposes:
- a. AEC staff required access to conduct testing of the election process, from data load to post election processing; and
 - b. The Contractor required access to load an updated application after changes were applied.
- 1.7.1.3 An Electoral Officer PC (EOPC) was used to load and download data, and could also be used for voting.
- 1.7.1.4 As the EOPC could not be installed at the AEC data centre (it being a data centre only), Defence agreed to a point-to-point connection being established between the data centre and the EOPC at the AEC's National Office with the following conditions:
- a. The EOPC was to be housed in a secure room with access to that room logged; and
 - b. The EOPC could not be connected to the server while the server was connected to the DRN.
- 1.7.1.5 The AEC complied with these conditions and established an EOPC in a secure room in West Block Offices.
- 1.7.1.6 Defence security requirements precluded remote access to the primary server via dial-up or the Internet by the Contractor to make updates to the application.
- 1.7.1.7 For application updates, the Contractor necessarily updated the servers in person at the data centre.
- 1.7.1.8 Possible improvements: negotiate with Defence to allow remote updating of the servers via dialup when not connected to the DRN, and by allowing further use of a dedicated ICON line for application access from West Block Offices.

1.7.2 Hardware and Connectivity Testing

- 1.7.2.1 Software testing is covered above, but the testing in this section relates to hardware and connectivity.

- 1.7.2.2 The system was extensively tested on multiple deployed technology platforms and across all communication routes. Major rounds of testing are described below.
- 1.7.2.3 A limited 'end to end' test in a 'production like' environment was conducted from 25 to 30 May 2007. The exception was that there was no satellite communication technology and parts of the deployed network were not utilised. The round of testing was conducted using:
- a. Voting software hosted on AEC infrastructure;
 - b. Access to the software via an ICON link; and
 - c. Deployable desktops and server (baseline environments as used in the 4 areas of operation).
- 1.7.2.4 The tests were conducted over four days testing communications, performance and 'end-to-end' system functionality. Results from testing were mostly positive but further testing was required.
- 1.7.2.5 Further 'end to end' system testing was conducted in Queensland during Operation Talisman Sabre from 4 to 8 June 2007. Testing concluded that technical problems were present using the remote electronic voting system and Defence's deployed standard operating environment.
- 1.7.2.6 Defence investigated the source of these problems and designed, developed, tested and Security accepted a solution to allow the electronic voting software to work across the deployed networks. The alternative solution still utilised the deployed network including satellite technology however did not depend upon the underlying Defence DSOE.
- 1.7.2.7 Initial testing using the alternative technical solution was successfully undertaken in mid June 2007. Further testing in each of the areas of operation was coordinated remotely from Canberra on 25 June 2007 confirming the technical solution as robust.
- 1.7.2.8 Validation of the system continued in the areas of operation up until the 2007 federal election. This included system 'end to end' testing conducted in the Solomon Islands in late August 2007 by the Defence Technology Project Manager.
- 1.7.2.9 Final validation was successfully conducted for all DRN terminals (laptops) being used for the 2007 federal election.

1.7.3 Certification

- 1.7.3.1 To meet the requirement of Certification tenderers were required to agree to supply the source code and other documents and equipment to an independent auditor.
- 1.7.3.2 In addition, the system was required to be audited to ascertain compliance with the relevant Chapters of the Australian Government Information and Communications Technology Security Manual (ACSI 33).
- 1.7.3.3 The action taken with these three elements is described below.

1.7.4 Independent audit

- 1.7.4.1 In providing Australia's first remote electronic voting at the federal level, the project team was very mindful of the adverse publicity that electronic voting had attracted overseas, both in the USA and Europe.
- 1.7.4.2 The AEC consulted with both the ACT and Victorian Electoral Commissions prior to defining the requirements for the tender. The ACT EC conducted electronic voting in its previous two elections, and the VEC conducted its first electronic voting in November 2006.
- 1.7.4.3 Both systems were independently audited to establish the integrity of the systems, and both Commissions used BMM International as the auditor.
- 1.7.4.4 In relation to the ACT system, for instance, BMM International certified that the code for EVACS [electronic voting and counting system]:
- a. Appeared to neither gain nor lose votes;
 - b. Appeared to faithfully implement the Hare-Clark algorithm for vote counting provided to BMM by the Commission; and
 - c. Was written in a consistent, structured and maintainable style.
- 1.7.4.5 BMM International is accredited by the National Association of Testing Authorities (NATA) as complying with ISO/IEC 17025-2005: General requirements for the competence of testing and calibration laboratories.
- 1.7.4.6 To comply with Commonwealth Procurement Guidelines, the project manager determined that a restricted request for quotation (RFQ) be issued to three organisations to undertake an independent audit of the system BMM International and two other NATA certified auditors.
- 1.7.4.7 This RFQ was issued on 8 June 2007 and after an evaluation of the responses, BMM International was selected as the successful contractor.
- 1.7.4.8 The RFQ included the following scope of the audit:
- RFQ Clause 1.13 AEC requires the following three elements of the voting system to be audited:*
- *That the system adheres to the security features specified by the AEC, as outlined in the RFQ documents and clauses 1.16 below;*
 - *That the system accurately stores, decrypts and prints all votes cast and there is no gain or loss in the voting process as outlined in clause 1.17 below; and*
 - *That the system software is free from "malicious" coding as outlined in clause 1.18 below.*

RFQ Clause 1.14 Vendors must note that the scope of this audit is intentionally limited to the points above and the audit must strictly adhere to this scope.

RFQ Clause 1.15 Security of the DRN, ICON and the AEC data centre is outside the scope of this audit.

RFQ Clause 1.16 The eLect system should be resistant to malicious tampering, with access to the application restricted to staff who are responsible for its maintenance.

RFQ Clause 1.17 To ensure vote accuracy, the Voting System must:

- Enable full details of a federal election to be loaded from data supplied by AEC;*
- Present ballots in the same order and with the same information as received on a paper ballot, as defined by the supplied data;*
- Record the elector's votes in an encrypted format, with the elector's details stored with the encrypted votes;*
- Require the elector's details to be removed from the votes before they are decrypted, so that there is no opportunity for any vote to be associated with any elector;*
- Allow for printing of the decoded votes so as to present the elector's preferences in the same order as selected; and*
- That in all the processes above, all cast votes are accounted for with no gain or loss.*

RFQ Clause 1.18 AEC require an independent review of the system software to ensure that it is free from code that intentionally alters any aspect of votes cast.

- 1.7.4.9 Final changes to the user interface of the system were undertaken on 4 July 2007, and the audit commenced on 5 July 2007.
- 1.7.4.10 While the audit was due to be complete by 31 July 2007, the auditor advised that they required additional information and code from the contractor. A meeting was convened between the auditor and the contractor to determine an expeditious way forward, and the auditor was subsequently able to complete the audit in late August.
- 1.7.4.11 Learning: For future audits, convene a meeting between the auditor and contractor to initialise the audit.
- 1.7.4.12 BMM subsequently issued the following formal findings and certification on 14 September 2007:

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.”

1.7.5 Defence security accreditation

1.7.5.1 Defence information systems operating within the Defence Restricted Network are required to be accredited and certified prior to operational use within Defence.

1.7.5.2 The remote electronic voting system, as trialed via the Defence Restricted Network, was successfully certified and accredited for use in early July 2007, confirming its compliance with the accepted Defence ICT security standards and that the security measures employed minimised the residual risk to Defence’s ICT infrastructure to an acceptable level as required by Defence.

1.7.6 ACSI 33 audit

1.7.6.1 The requirement for compliance with ACSI 33 was raised by the AEC’s ICT Security Advisor during the development of the Statement of Requirements. At that point in time, the design of the end system was unknown, therefore it was reasonable to include this requirement in the tender.

1.7.6.2 Once the design of the system was completed, an ACSI 33 audit was deemed to be unnecessary due to the low level of risk to the AEC. The risk was assessed to be very low due to the following elements of the design:

- a. There was no connectivity to any AEC systems or LAN – connectivity within the AEC was via direct link from the server to the Electoral Officer PC (EOPC);
- b. The server was stored in secure premises at the AEC Data Centre;
- c. Connectivity with Defence was via ICON, an approved government facility with a direct end-to-end connection from the server to Defence;
- d. The connection to Defence was hardware encrypted, with the application also providing software encryption; and
- e. There was very limited 'external' security threat, as any such threat would need to come through the Defence Restricted Network.

1.8 User Engagement

1.8.1 ADF and AEC Promotion

- 1.8.1.1 User Promotion has previously been described in the main report.
- 1.8.1.2 The text of the 'How to Cast your vote' pamphlet is included at Appendix F.

1.9 Implementation

1.9.1 REV Registration and PIN distribution

- 1.9.1.1 The registration of REV's needed to comply with certain areas of the new and old legislation as well as the policy decision to issue all REV's with a GPV. These were:
 - a. **CEA 185 (4A)** – which required that no details of defence members or Australian Federal Police (AFP) could be included in the register of GPVs that might allow someone to ascertain that this voter is a member of the AFP or Defence or that they are serving overseas. While this section was directed at GPVs and not REV's explicitly it was seen that the spirit of the legislation would follow that a REV should be treated in the same manner.
 - b. **CEA 184A (5) and CEA 185 (1A)** – Both of these sections when read together make it difficult for the voter to arrange matters prior to leaving Australia:
 - A. Section 185(1A)** states that a GPV can not be registered until the voter has left Australia, while **CEA 184A(5)** states that the elector may not apply before he or she has left Australia.
 - c. Regulation 62 requires the Divisional Returning Officer (DRO) to de-register any REV who is in Australia at the time the writs for the election are issued or if the voter has returned to Australia permanently.
 - d. Regulation 61(2)(b) allows for a REV to register if they are serving or may serve outside Australia at the time of the election.
- 1.9.1.2 As the trial was restricted to four AOs, the Electoral Commissioner gazetted these areas. This meant that the AEC divisional office staff who were receiving REV registration forms needed a methodology by which to accept applicants who qualified as REV's and reject others who were not within the gazetted AOs.
- 1.9.1.3 AEC's Roll Management Branch formulated a methodology which included the use of templates via the AEC's standard letter system with instructions as to the criteria for accepting or rejecting a REV registration. The suite of standard letters is included at Appendix H.
- 1.9.1.4 The AEC consulted Defence in designing a process for the AEC divisional staff to allow for validation of registration forms. Defence

provided six Armed Forces Post Office (AFPO) numbers that were solely located within the gazetted AOs. These were:

Iraq	AFPO 19 and AFPO 20
Afghanistan	AFPO 13 and AFPO 14
Timor Leste	AFPO 5
Solomon Islands	AFPO 11

- 1.9.1.5 If an applicant did not quote one of these AFPO addresses then they were assessed as not being eligible to be registered.
- 1.9.1.6 Initially this caused confusion as many applicants used their home address as their postal address. This was compounded by some inconsistent information being provided at Force Preparation sessions by Defence prior to deployment.
- 1.9.1.7 As many of these applicants had subsequently been deployed, a list of applicants was provided to HQJOC for advice as to which areas these applicants had been deployed.

1.9.2 Addressing the Legislative Requirements

- 1.9.2.1 Given the requirements of the above legislation, particularly Regulation 62, it was decided that, when the Writs were issued for the election, a review of REVS would occur against their applications to ensure that any REV who:
 - a. was in Australia at the time the Writs were issued;
 - b. had returned to Australia permanently; or
 - c. would be in Australia at the time of the election would be deregistered as a REV.
- 1.9.2.2 Point c above was interpreted as any person who was in Australia during the three week pre-poll voting period as they were able to vote at an Early Voting Centre or at a polling place on election day.
- 1.9.2.3 Point a was more problematical as when the legislation was written, it was envisaged that registrations for REVs would cease and all future applications would be processed as GPVs. The joint AEC/Defence Project Board had the view that the whole purpose of electronic voting was to be able to facilitate a quick turn around of voting, therefore to close registration when overseas voters might start to consider registering was counter productive for the voter and for the trial.
- 1.9.2.4 Consequently it was decided that the cut off day for registration would be at the "Close of Nominations" as this is when the electronic voting application would be populated with candidate names as well as the REV roll and sealed ready for voting to commence. This decision allowed the maximum number of REV registrations without compromising the security of the database during the voting period.

- 1.9.2.5 However, the issue of complying with Regulation 62 remained. This unfortunately meant that a person could be in Australia at the Issue of the Writs and be deployed the next day but did not qualify to be a REV. Under these circumstances this group of people were sent GPVs and a letter stating that they did not qualify to be a REV but would be sent a postal vote instead.
- 1.9.2.6 Defence were requested to confirm the dates on applications and that the member had not returned to Australia.
- 1.9.2.7 Notwithstanding the above, for the majority of the 2012 registered REVs, the process went quite smoothly. Registration and PIN issue progressed through the following steps:
- a. Within the AEC the enrolment would firstly be checked and if the applicant was enrolled they would then be flagged in the RMANS as a GPV and then as a REV.
 - b. The REV would then receive an acknowledgement letter from the Standard Letter System.
 - c. Each week the electronic voting team received a download of data from RMANS of REV applicants and produced a PIN mailer for each new applicant. The mailing of PINs commenced on 9 October 2007 and the last mail out was on 2 November 2007
 - d. The PIN mailer was a letter with a security panel which, when peeled off, would reveal the voter's PIN. The letter contained instructions to the voter and the 'How to cast your vote' pamphlet' was also included.
 - e. The pamphlet contained step-by-step instructions with regard to logging in and voting and also included instructions with regard to on-the-ground support should the voter experience any technical difficulties. The pamphlet also described the vote checking service so that the voter could verify that their vote had been received by the AEC's database. The pamphlet text is included at Appendix F.
- 1.9.2.8 Possible improvements:
- a. PIN issue and registration could be more automated to eliminate the delays incurred in posting information to voters.
 - b. Regulation 62 will need to be addressed should this electronic voting be approved for future elections to alter the active date to the close of nominations.

1.9.3 GPV contingency

- 1.9.3.1 A contingency process where the voter could still cast their vote was required in the event that deployed personnel may not be able to access a computer in order to vote for various reasons such as:
- a. if unforeseen issues arose with the software or connectivity during the election timetable;
 - b. the amount of time it takes to get mail to the middle east area of operations;

- c. concern that the voter should not suddenly find themselves in a situation where they were relying on being close to a computer to vote;
 - d. electronic voting no longer being an option due to the voter's own or unforeseen circumstances.
- 1.9.3.2 In each of these situations, the voter needed to be in a position where they could cast a paper ballot.
- 1.9.3.3 JSCEM's Recommendation 9 stated that all members of Defence and the Australian Federal Police should be able to register as General Postal Voters for the duration of their deployment. The Government agreed to this recommendation, and enabling legislation was passed in early 2007.
- 1.9.3.4 Given the complexities of providing an electronic vote in this first trial, the joint decision was made to issue all personnel who applied to become a REV automatically with a General Postal Vote (GPV). This would mean that the voter could make a choice based on their individual needs or circumstances as to the best method to vote. Administratively, in order to do this within the existing AEC systems, it was decided that the AEC would register all REV voters primarily as General Postal Voters and then to add a subsequent flag to indicate that they were also REV voters.

1.9.4 Data Load

- 1.9.4.1 AEC's IT Applications team supplied election data on the afternoon of 3 November 2007. Full details of all files required for the data load is under Design above.
- 1.9.4.2 Data was loaded on Sunday 4 November.
- 1.9.4.3 After the data load, a full set of ballot papers were printed.
- 1.9.4.4 These ballot papers were then checked against live ballot papers to verify that the data load was successful.
- 1.9.4.5 One problem was identified in the checking process. One House ballot paper had the wrong state. This was traced to data that had not been cleared from the server after testing.
- 1.9.4.6 Contractor support staff removed all data from the server, and the load process commenced again.
- 1.9.4.7 All checking was then completed successfully.
- 1.9.4.8 This issue identified a problem with administration of the EOPC.
- 1.9.4.9 As already mentioned under Design above, the Contractor's normal process is for their staff to manage administration of an election. For this reason, the EOPC interface is not as 'user friendly' as it should be for a non-technical electoral officer.
- 1.9.4.10 Due to the limited time available to design, develop and test this system, the EOPC interface could not be improved. However the ability for the AEC to independently load data and manage the

election processes will need to be a requirement for any future projects of this nature.

1.9.5 Diacritical Marks

- 1.9.5.1 The AEC allows diacritical marks in the spelling of a candidate's name. Therefore when a candidate successfully nominates and the name on the nomination form contains a diacritical mark, these are printed on ballot papers.
- 1.9.5.2 The AEC databases use a single-byte character set, and do not have the ability to capture a diacritical mark. This means that a ballot paper that needs to display a diacritical mark must be manually typeset. For the E-Voting team this also meant that the diacritical mark would not be passed to the E-Voting systems in the data supplied from these AEC databases.
- 1.9.5.3 The E-voting team sought advice with regard to altering the data that was supplied from the AEC systems so that a candidate's name would include any diacritical marks and consequently provide the same information as would appear on a paper ballot as required by CEA 202AH(3)
- 1.9.5.4 Appendix J shows the loading and checking procedures that were approved for the alteration of data prior to upload, as well as the subsequent checking.
- 1.9.5.5 In the development stages of the software diacritical marks were raised, but not fully addressed. This issue will need to be included in the Statement of Requirements for future electronic voting projects.

1.9.6 User Support

- 1.9.6.1 The complexity of the remote electronic voting solution required a comprehensive and robust support process. The AEC and Defence jointly consulted to develop support arrangements covering both business and technical support.
- 1.9.6.2 A significant hurdle in the development of these procedures included providing support outside normal business hours to coincide with key operational hours in the areas of operation.
- 1.9.6.3 User support was available during the voting period, and was separated into three distinct areas:
 - a. Level one support, provided Defence;
 - b. Level two support, provided by the AEC; and
 - c. Level three support, provided by the Contractor.

1.9.7 Level one support (Business)

- 1.9.7.1 Defence provided first level support, adapting the existing ADF Computer Information Support (CIS) support model as the first point of contact for members experiencing problems with remote electronic voting during the voting period.

- 1.9.7.2 Issues relating to AEC business processes involving registration and PINS, that is, user support issues, were to be directed by the local CIS support to the AEC.
- 1.9.7.3 CIS did not receive any request for support during the trial, although this process was bypassed with some support requests being made direct to the AEC (see below).
- 1.9.7.4 A 'Frequently Asked Questions' document was also made available on the Defence remote electronic voting intranet website.

1.9.8 Level two support

- 1.9.8.1 AEC's IT help desk provided level two support, with issues not able to be resolved at that level escalated either to the AEC project manager or the Contractor. This help desk was available for extended hours over the election period.

1.9.9 Level three support

- 1.9.9.1 The Contractor provided services from 8 am to 6 pm Canberra time each day during the voting period, with polling day support extended to 6 pm Perth time, as that was the close of electronic voting.

1.9.10 Technical support

- 1.9.10.1 Technical support was available, once again, on three levels:
 - a. Level one support, provided by Defence;
 - b. Level two support, provided by the AEC; and
 - c. Level three support, provided by the Contractor or the AEC's IT staff, as appropriate.

1.9.11 Level one support

- 1.9.11.1 Defence adapted the existing ADF CIS support model for technical support.
- 1.9.11.2 Issues relating to Defence ICT infrastructure precluding the use of the remote electronic voting trial were to be directed to the appropriate stakeholders within Defence. Support arrangements were put in place for Defence ICT infrastructure utilised for trial. This included a customised CIS online web resource that included business and technical information for the CIS ICT delivery.
- 1.9.11.3 Defence technical staff advised that no electronic voting ICT hardware or software specific issues were raised during the trial.

1.9.12 Level two support

- 1.9.12.1 Again, AEC's IT help desk provided level two support, with issues not able to be resolved at that level escalated either to the Contractor, for application issues, or to AEC's IT staff, for hardware/communication issues.

1.9.13 Level three support

- 1.9.13.1 Level three support from AEC's IT staff was available 24 hours a day during the voting period.
- 1.9.13.2 The Contractor provided telephonic support for general system maintenance up to the election period, then provided on site support for the election setup.
- 1.9.13.3 During the voting period, the Contractor provided on call support 24 hours a day, with a 2 hour on site response time. This continued up to 6 pm Perth time on polling day.
- 1.9.13.4 The Contractor also provided on site support for post election processing.

1.9.14 Summary of technical support

- 1.9.14.1 From election setup to post election processing, no issues were raised with Level two support. During the election setup, a single issue required Contractor involvement as follows:
 - a. Test data had not been completely cleared from the EOPC. This was primarily due to incomplete instructions from the Contractor on the operations of the EOPC, as all EOPC functions had, in the past, been undertaken by Contractor staff, whereas the AEC required that AEC staff do these tasks for the federal election.

The Contractor, under AEC supervision, cleared all superfluous data from the EOPC and the election load was then completed without incident.

1.9.15 ADF Operational Management

- 1.9.15.1 HQJOC were tasked with coordinating the whole-of-ADF involvement (as distinct from Defence involvement) for the trial which included the provision of ADF advice and assistance to the AEC. This involvement included:
 - a. Provision of assistance and advice to AEC in relation to:
 - A. The remote electronic voting system design SOR;
 - B. Distribution of electoral matter to, from and within the respective areas of operation; and
 - C. Invalid/incomplete registration forms and deregistration of invalid trial participants.
 - b. Provision of advice and assistance to CIOG in the design and testing of the remote electronic voting system and for coordinating with each of the Joint Task Forces the setup and testing of the DRN terminals for remote electronic voting in each of the areas of operation.
 - c. Promulgating information on the trial to the relevant Joint Task Forces. The execution and administration for the remote electronic voting trial by the Joint Task Force was detailed in the

support order issued by Chief of Joint Operations Command on 19 October 2007.

- 1.9.15.2 A staff officer grade 1 from Headquarter Joint Operations Command based in Canberra was allocated to coordinate the whole-of-ADF involvement for the trial.
- 1.9.15.3 Given the complex operational environment, the Joint Task Force for Middle East Area of Operations established a small team from Headquarters Staff and a 'voting coordinator' from each Task Group to facilitate voting (including general postal voting).
- 1.9.15.4 Existing CIS staff from each Joint Task Force were responsible for the setup and testing of all DRN terminals (laptops) to be used for the election. Their role also included management of ICT support for remote electronic voting during the federal election.

1.10 Contractor's Project Review

1.10.1 Contractor Evaluation

- 1.10.1.1 The Contractor met with AEC and Defence staff for a project debrief on 4 December 2007 to conduct a system post project review, and subsequently provide a report for review.
- 1.10.1.2 The final report was provided to the AEC in February 2008.
- 1.10.1.3 This section discusses major findings contained in the Contractor's report.

1.10.2 Request for Tender/Contract Management Process

- 1.10.2.1 Areas for improvement
- 1.10.2.2 One of the major concerns from all persons who attended the debrief meeting was the very short project delivery timeframe. This was a direct result of the late decision by government [related to the time frame for the 2007 federal election] to conduct the trial, and the fixed delivery date. All parties felt that acquisition needs to be commenced earlier in the cycle to allow all project teams to perform their tasks to the highest standard.
- 1.10.2.3 During discussions with the various AEC IT areas responsible for producing the electoral data files for the project, it became apparent that there were other data formats than those provided that could have been used as input to the voting application. These alternatives may have resulted in more flexibility in the final product, and may have had the potential to save both time and money. It is recommended for any future such projects, that the range of data formats available is offered as alternatives.

1.10.3 Project Structure and Communications

- 1.10.3.1 Successes
- 1.10.3.2 Communication during the Defence field testing phase with conference calls each afternoon involving all stakeholders was excellent and should be adopted for any future projects (face to face if in same locality).

- 1.10.3.3 Areas for improvement
- 1.10.3.4 Any future projects of this nature need several face-to-face meetings with all major stakeholders in the early stages of the project to gather a detailed understanding of the requirements. As well, Contractor staff should be either co-located with the AEC or closely accommodated so as to more effectively work through the issues in a real time environment.
- 1.10.3.5 A mandatory requirement for involvement in these meetings are subject matter experts from each AEC functional area who are well versed in all electoral matters in order to avoid rework in the application design. Defence IT staff also need to be involved upfront to advise on all network communication design matters within their network.

1.10.4 Project Management

- 1.10.4.1 Project Management Scope
- 1.10.4.2 The scope of Project Management (PM) activities on this project was diverse as each jurisdiction had its own Project Manager (Team Lead) all reporting into the AEC Project Manager who in turn reported to the AEC Project Director.
- 1.10.4.3 Successes
- 1.10.4.4 It was generally agreed that the relationship between the various project teams worked very well and that all were focused on completing the project by the scheduled date of 30 June 2007.
- 1.10.4.5 The staff assigned by Defence to co-ordinate testing activities worked extremely well with the Contractor during the testing phase with activities co-ordinated by the AEC Project Manager. The direct contact between all parties during the testing phase was critical to resolving matters quickly and completing development and testing on schedule.
- 1.10.4.6 Areas for improvement
- 1.10.4.7 In the early stages of the project there was some confusion on the Contractor's behalf as to the reporting protocols between the Contractor and the AEC.
- 1.10.4.8 It is suggested that for any future projects that the general Project Management reporting protocols be agreed at the commencement of the project.

1.10.5 Requirement Analysis

- 1.10.5.1 Successes
- 1.10.5.2 Both the Contractor and the AEC worked together to produce the requirements very early in the project life cycle. This significantly contributed to the application being delivered in sufficient time to meet Defences testing schedule.
- 1.10.5.3 Areas for improvement

- 1.10.5.4 As noted, the lack of face-to-face meetings to confirm the requirements, the fact that Contractor staff were not on-site in Canberra to work with AEC staff directly and the lack of prototypes did cause rework and it was agreed by all stakeholders that these elements need to change for any future projects of this nature.
- 1.10.5.5 The Contractor expected CSV data files as that is what was specified in the RFT and the Contractor had included these in the requirements. It was advised during the debrief that other data formats were available. These alternative data formats would have been more acceptable to the Contractor.
- 1.10.5.6 It was agreed that if a range of data formats is available, this should be specified in the RFT so that Tenderer's can bid appropriately.
- 1.10.5.7 In addition, the Contractor must put in place a more effective document management regime, as version control issues with the Requirements document also lead to a level of software rework.

1.10.6 Application Design

- 1.10.6.1 Design Scope
- 1.10.6.2 The design scope for the application was restricted to meet the minimum contracted requirements to achieve the tight delivery schedule for the trial. In elections managed for other clients, the 'eLect' software has been fully setup and managed on a day to day basis by the Contractor. The AEC is the first customer that has required their own electoral officers to setup and run the election from the commencement of the election cycle through to completion.
- 1.10.6.3 The fact that the AEC ran the election from the outset exposed some usability issues on the administrative side of the application. Had more time been available, improvements in the usability aspect of the application could have been incorporated into the software which would make it less prone to procedural errors by users not fully conversant with the software.
- 1.10.6.4 Successes
- 1.10.6.5 The software and procedural documents supplied by the Contractor along with the testing performed by the AEC were sufficient to enable a successful trial to take place.
- 1.10.6.6 Areas for improvement
- 1.10.6.7 The AEC commented that issues of screen resolution and the viewing area need some redesign for any future projects. In some cases, only one candidate can be seen on a screen, but in the more acceptable circumstances, up to 6 candidates can be seen. While the software is required to replicate the paper ballots, the viewing area will always be a matter of concern, however the display must be suitable to show a reasonable number of candidates on a larger number of devices.

- 1.10.6.8 The Contractor is of the opinion that improvement within the 'eLect' software can be made in the areas of data file loading, data storage and the manner in which test data is removed from the system. At present, the 'eLect' software stores the same files in two different locations. This can lead to a mismatch of data which occurred during the full election simulation test with two different division files being used with different electorates due to recent redistributions.
- 1.10.6.9 AEC staff noted that splitting the Senate ballot paper into separate screens (above the line, below the line) may not have had any direct benefit in making the voting experience easier. This will be reviewed as part of the feedback from Defence personnel via the AEC questionnaire distributed to those members in the trial post trial.
- 1.10.6.10 An area of concern raised by all parties related to the credentials used for authenticating a voter. It was agreed that anyone who picked up the PIN mailer and had access to the person's date of birth would be able to vote on that person's behalf. There is no evidence that this occurred during the trial.
- 1.10.6.11 Credentials used for authentication for the trial were:
- a. Name as it appeared on the PIN mailer
 - b. Date of Birth
 - c. PIN number
- 1.10.6.12 It needs to be noted that the authentication model used for this trial was the only available option given the project time line, and the data available to the AEC.
- 1.10.6.13 It is recommended that in any future electronic voting exercises, alternative authentication models and processes be investigated and if possible, adopted.

1.10.7 Software/Hardware and Network Installation

- 1.10.7.1 Installation Scope
- 1.10.7.2 The scope of this area of work was to install software onto two AEC servers (one for failover) to run the application and a single PC (the EOPC) to be used for election officer functions (administration). The Contractor was to work with AEC IT staff to build the servers and the EOPC in accordance with the Contractor's needs and to supply both training and operating system manuals on how to support the environment to AEC IT personnel. AEC IT was then to work with Defence to establish connectivity across the ICON network into the DRN.
- 1.10.7.3 Areas for improvement
- 1.10.7.4 It was also noted that the clock on the server lost time during the testing period. The server did not have any connectivity that would allow time synchronisation. This needs to be considered for any future projects.

- 1.10.7.5 During the voting period, voting statistics were accessed on the server in the Data Centre by project staff. This was necessary as the server could not be connected to the DRN and to any part of the AEC network at the same time. This was a laborious process, and for future such projects, a methodology for accessing such statistics from a project officer's desktop is necessary.

1.11 Software Testing

1.11.1 Testing Scope

- 1.11.1.1 Testing on this project consisted of the following functional areas:
- a. Connectivity testing from the AEC data centre across the ICON network into the Defence Restricted Network (DRN) to ensure server connectivity and data encryption passed successfully.
 - b. Canberra based functional testing on Defence PC hardware (two different standard operating environments were used) at a Defence site to ensure the encrypted messages could travel back to the server where the votes were recorded.
 - c. Server failover testing.
 - d. Field satellite based testing on Defence PCs in Australia, Solomon Islands and East Timor (two different standard operating environments were tested). As well staff in Afghanistan and Iraq performed a limited amount of testing.
 - e. AEC functional testing (voting, election setup and post election processing).
 - f. Full Election end to end testing over a 2-3 week period (performed by AEC with machines disconnected from DRN).

1.11.2 Defence Network/Connectivity and Functional Testing

1.11.2.1 Successes

- a. The AEC and Defence believe the Contractor's response to debug most issues within 24 hours during the remote testing period allowed the testing to be completed successfully and within the scheduled timeframe and contributed significantly to the success of the project.

1.11.2.2 Areas for improvement

- a. Defence would like to have had a longer time frame to understand the JRE (Java runtime environment) that was used to deliver the voting applet. They would also like to see a beta version of the voting applet as early as possible to facilitate better setup of their environment for testing connectivity matters on their various SOEs.

1.11.3 AEC Functional Testing

1.11.3.1 Successes

- a. The AEC acknowledge that the use of the Contractor's test environment for AEC testing was beneficial as it was not possible to test on the DRN and apply changes quickly due to

the absence of a remote update facility. The Administration User Guide allowed the AEC to run the election without intervention from the Contractor as well as process a full election simulation. This assured the AEC that the application would perform well and that all processes were sound.

1.11.3.2 Areas for improvement

- a. Test scripts from the Contractor needed to be much more extensive to assist AEC staff in performing full user acceptance levels of testing. The AEC should include this requirement in any future Tender so that there is no confusion as to who should supply the test scripts.
- b. The Contractor needs to setup the system to allow for multiple instances of an election to be run at the same time.
- c. The EOPC user interface needs to be more end user friendly. The interface needs a facility that removes old election test data in one easy step. This is required as on several occasions during testing, old data was not deleted and this affected the outcome of subsequent test results. This also occurred during the live election data load but due to the AEC's rigid checking process it was detected prior to the election going live and the test data removed.
- d. The AEC noted that only one or two people performed testing during the early stages and that for future projects, this should be done in a more extensive and rigorous manner.

1.11.4 Contracted Documentation

1.11.4.1 Documentation Scope

1.11.4.2 The Contractor was commissioned to complete the following documentation either as a completed document or as drafts that either the AEC or Defence would refine to meet their own standards.

1.11.4.3 User Documents:

- a. User Guide for Voters
- b. Administration User Guide for election management staff
- c. This Project Review Report.

1.11.4.4 Technical Documents:

- a. Project Plan
- b. Test Plan
- c. System Requirements Specification
- d. Test Scripts (not specified in the contract but required by the AEC)
- e. Administration User Guide for technical staff
- f. Trouble Shooting Manual

- g. Server Operating System Manual provided from the vendor of the operating environment
- 1.11.4.5 All the above documents with the exception of the software test scripts were delivered to the AEC for review ahead of contracted schedule and were refined until they met AEC requirements. The AEC also prepared procedural documents and check lists which they used to setup and run the election.
- 1.11.4.6 Successes
- 1.11.4.7 The general feedback from all concerned was that all documents satisfactorily achieved the purpose for which they were commissioned.
- 1.11.4.8 Areas for improvement
- 1.11.4.9 As covered under Software Testing above, the AEC should include the requirement for test scripts in future Tenders so that there is no confusion as to who is responsible for this element. In such specification, the requirements must be that the scripts test the system from end-to-end, so that the results of tests can be effectively used in the audit process.
- 1.11.4.10 Documentation change management was somewhat ineffective for the System Requirements Specification, with changes made by AEC lost in subsequent versions. Indeed, this document was not completed until after the election due to the number of discrepancies between the document and the system. Document change management must be more strictly controlled in future projects.

1.11.5 Software Audit

- 1.11.5.1 Audit Scope
- 1.11.5.2 This is covered under Independent Audit above.
- 1.11.5.3 Successes
- 1.11.5.4 The software and the procedures surrounding the software passed the audit.
- 1.11.5.5 Areas for improvement
- 1.11.5.6 For future such audits, an initiation meeting involving the Auditor, the AEC and the Contractor at the outset of the Audit would lead to a better understanding of the system by the Auditor. This would have given the Auditor a better understanding of the software architecture, the fact that the software is large and complex (well over a million lines of code) and that it supports electoral models from around the world.

1.11.6 Election Setup

- 1.11.6.1 Scope
- 1.11.6.2 The setup of the election took place in separate stages:

- a. The set up of the EOPC with the division file and voter records loaded on a regular basis in advance of the election to produce PIN Mailers.
- b. The loading of all electoral data files to the EOPC and the server and all voter records as well as election parameters such as opening and closing times. This was performed on the day before the pre-polling period started.
- c. Upon setup completion the servers were then disconnected from the AEC network and connected to the DRN.

1.11.6.3 Successes

1.11.6.4 The election Setup went very well and was complete and verified by 4:00pm on 4th November, 2007

1.11.6.5 Areas for improvement

1.11.6.6 During the requirements gathering phase, the AEC pointed out that a test environment needed to be maintained in the lead up to the election, as well as having the facility to register voters. Voters would be registered prior to the election period to allow time for the PIN mailers to reach the overseas locations. Reissue of PINs was also required during this period. At this stage the AEC did not understand the relationship between the EOPC and the server.

1.11.6.7 However the system was designed to allow reissue of PINs only from the server, something that could not be done while a test environment was running. For any future project, the timings of each element of the election setup, and the facility for conducting each element, for example, PIN issue and reissue, must be more comprehensively defined so that the system can be designed to meet those requirements.

1.11.6.8 There was a significant error on the setup of the election that was caused by residual test data. One House of Representatives ballot had the incorrect state. This was resolved by Contractor technical support staff at the time. For the future, the improved interface and process for removal of old data discussed under Software Design will resolve this issue.

1.11.7 Running the Election

1.11.7.1 Scope

1.11.7.2 The Electronic voting system 'eLect' was to be available for the 20 days of the polling period. Post Election processing consisted of down loading the votes from the server; decrypting the votes; running a 'reporter' program that produced all print files, producing a spreadsheet for matching to the postal voting system;; printing, reconciling and packaging ballot papers; and printing reconciliation reports and packaging with the sealed votes ready for express post to the relevant Divisional Office for counting.

1.11.7.3 Successes

- 1.11.7.4 The server and software did not have any outages during the voting period and Contractor support was not required during this time.
- 1.11.7.5 Areas for improvement
- 1.11.7.6 An issue arose when printing NSW Senate below the line ballot papers where the data would not fit on a simplex A4 page. Font sizes were adjusted and the ballots reprinted. For the future, the design of the output format must take into account a larger number of below the line entries.

1.11.8 Election Support

- 1.11.8.1 Support Scope
- 1.11.8.2 Full details of the scope of support services are under User Support and Technical Support in section 2.7.6 and 2.7.8.
- 1.11.8.3 Successes
- 1.11.8.4 There were no support issues raised with the Contractor during the voting period. The on-site support available in Canberra was invaluable, even if not used, as a rapid response would have been required for any software outage.
- 1.11.8.5 Areas for improvement
- 1.11.8.6 An option to reduce the cost of on-site Canberra support would be for the Contractor to be given access to the server remotely. During this trial, this was not possible as Defence would not allow any other connectivity to the server while it was connected to the DRN, and remote access via dial-in was also not allowed.

1.12 Independent Trial Evaluation

1.12.1 Planning and process

- 1.12.1.1 The overall objective of the evaluation was to determine the effectiveness of the trial in providing a secure, reliable, and convenient method of voting at federal elections for overseas ADF personnel.
- 1.12.1.2 The aims of the evaluation of the trial were to:
 - a. determine the effectiveness and efficiency of the REV trial in providing a secure and reliable method of voting at Federal elections, by examining
 - A. the level of take-up for the use of REV,
 - B. the communication strategy to inform eligible electors in the ADF about the trial,
 - C. the use of postal voting by registrants,
 - D. user acceptance of REV,
 - E. exercise of discretion by REV voters, and
 - F. the cost per vote of the trial;
 - b. evaluate whether the use of REV complied with legislative and other standards by examining compliance of procedures and

processes implemented in the trial with relevant sections of the Commonwealth Electoral Act 1918 and associated regulations;

- c. assess whether the use of remote electronic voting led to any increase in electoral offences, or any increase in the risk of electoral offences or fraud by examining
 - A. procedures to manage risks of electoral offences; and
 - B. allegations of electoral fraud arising from the REV trial.

1.12.1.3 An independent consultant was engaged to identify administrative issues arising from the trial, and make recommendations for improvements should the trial continue or be more widely implemented subsequent to that planned for the 2007 Federal Election.

1.12.2 Scope of Evaluation

1.12.2.1 The scope of the evaluation was focused on the conduct of the trial during the 2007 Federal Election. Attention was given to:

- a. the planning for the trial, covering consultations, communications, testing and training for the trial;
- b. processes and procedures, along with associated guidance and instructions, undertaken at the AEC National Office for receiving and printing the electronic votes, and at Divisional Offices for registering electors for the trial and subsequently in receiving the printed votes; and
- c. views on remote electronic voting as a means of providing a secure and convenient method of voting with improved reliability for ADF personnel serving overseas.

1.12.2.2 The scope of this evaluation did not cover the electronic voting supporting IT infrastructure.

1.12.3 Approach to the Evaluation

1.12.3.1 The evaluation was undertaken in three stages:

- a. Stage 1: Scope and Planning;
- b. Stage 2: Data and Information Gathering; and
- c. Stage 3: Analysis of Data and Reporting the Findings.

1.12.3.2 Each stage was conducted in close consultation with the AEC Research Section and the Electronic Voting Section.

1.12.3.3 Information for the analysis was collected by the following means:

- a. a postal survey of REV registrants that was sent to each REV registrant in the post election period, whether or not they had cast a vote;
- b. a focus group of, and teleconferences with, DROs and their staff from eight Divisions, including the three Divisions in which 53% of registrants were enrolled (Herbert, Solomon and Brisbane);
- c. statistics recorded of the number of registrants and REV votes from each Division;

- d. interviews with the Electronic Voting Section members, an examination of supporting material developed by the Section and provided by Defence, for example through the REV joint Project Board established between the AEC and Defence (the Board). The Board was established to manage the overall project;
- e. an interview with an Assistant Director, Enrolment;
- f. statistical information about GPVs received from trial locations;
- g. statistical and performance information about the 2004 and 2007 Federal Election relating to number of votes, above/below the line voting, and cost.
- h. desk review and discussion with relevant AEC officials to identify relevant legislative provisions;
- i. costing for the project as assessed by the Electronic Voting Section;
- j. observation of the print-out and dispatch of REV votes on the day following polling day;
- k. information on complaints and allegations regarding the REV trial; and
- l. the Post Activity Report on the Federal Election 2007 and Remote Electronic Voting prepared by Headquarters Joint Operations Command in the Department of Defence.

1.12.4 Postal Survey of REV registrants

- 1.12.4.1 Those who had registered to cast a REV vote were sent a survey questionnaire, asked to fill it in on a voluntary basis, and return it to the AEC by post. A copy of the survey instrument for REV registrants is at Appendix K.
- 1.12.4.2 A total of 2012 ADF personnel registered to cast a REV vote, of whom 1511 cast a vote using REV. In the period up to the cut off on 29 January 2008, 372 survey instruments were filled in and arrived at the National Office, AEC. The resulting number of participants in the survey is shown in the following table. This table also identifies the 95% confidence interval for estimates arising from analysis of the survey.

Location	Registrants		Voters	
	Sample Size	Population	Sample Size	Population
Afghanistan	112	669	107	599
Iraq	70	638	62	501
Solomon Is	45	107	44	98
Timor-Leste	144	598	100	313
Total	372	2012	313	1511

1.12.5 Feedback from DRO and their staff

- 1.12.5.1 A focus group was conducted in Sydney on 18th December with DROs and their staff with responsibilities for Enfield, Parramatta, Chatswood and Wollongong. Teleconferences were held with

DROs and their staff from the following Divisions and on the following dates:

- a. Herbert, Solomon and Brisbane on 13th December 2007;
- b. Lyons on 18th December 2007; and
- c. Adelaide on 20th December 2007.

1.12.5.2 The issues raised with the DROs and their staff at the focus groups and teleconference are at Appendix L.

1.12.6 Findings and Recommendations

1.12.6.1 The full summary of findings and recommendations is at Appendix M.

1.12.6.2 Supporting documentation is contained in the report itself.

1.12.6.3 Below is a summary of the evaluation.

1.12.7 Summary of the Evaluation

1.12.7.1 This summary collates comments into the high level elements listed at paragraph 1.12.1.2 above.

1.12.7.2 Effectiveness and efficiency of the trial in providing a convenient, reliable and secure method of voting at Federal election for overseas ADF personnel.

- a. The trial demonstrated that remote electronic voting for personnel deployed in Defence operations overseas could provide a convenient, reliable and secure method of voting in a Federal Election. 1511 votes were cast using REV.
- b. The number of deployed personnel known to cast a vote at the 2007 Federal election was significantly higher at 1740 when compared with the 2004 Federal election. REV voting played a very important role in achieving this result.
- c. The registration process was resource intensive for Divisional Offices, mainly due to incomplete information initially provided to the AEC by trial participants, and a high number of REV applicants being enrolled at addresses other than those claimed for on their REV application form. Lessons learnt from the trial on these issues should allow more streamlined administrative processes in any future implementation of REV voting.
- d. The timeliness of receiving mail for some of the Defence personnel overseas, a key driver for the trial, remains an issue, albeit more limited, for the mail out of PINs to access remote voting.
- e. Most of those who registered for REV found out about the trial either through Force preparation training, or through information from their commanding officers or through word-of-mouth.
- f. Three-quarters of those who registered cast their vote using REV, but the proportion varied markedly between locations – many of those deployed to Timor-Leste were unable to cast a vote using REV because of “operational reasons”. Postal voting

is used as an alternative to casting a REV vote, but the proportion using this option is comparatively small.

- g. Amongst the REV voters, there was a high level of satisfaction with the level of service that REV voting provided. The main issues raised with REV voting concerned the lack of privacy in casting a vote (16 survey respondents), particularly for those deployed to Timor-Leste and Afghanistan, and the speed that voters were able to log on and cast their vote – an issue of particular concern in the Solomon Islands and Afghanistan. Both of these issues were raised by a small minority of voters in these locations. Despite the concerns about speed from respondents, the average time to cast a vote was 8.6 minutes after logging on.
- h. Those who used REV to vote were able to vote in a way that reflected their intentions, as evidenced by the relatively high number of BTL voters. However, the proportion of BTL voters was lower from those locations with reported poorer DRN speeds. Information on local candidates, how-to-vote from registered parties and independent candidates, and on GVTs would have further assisted REV voters in casting votes that fully reflected their intentions.
- i. The unit cost per vote in the trial was relatively high. Costs for a future implementation are difficult to forecast as they are contingent on the Government's decision on this issue. However, unit costs are expected to decrease, provided the number of electors eligible to vote using REV does not decrease.

1.12.8 Compliance with Legislation

- a. The trial largely complied with relevant legislative sections and regulations relating to REV. Some feedback from REV registrants in Afghanistan and Timor-Leste post trial noted placement of DRN terminals did not provide sufficient privacy. Specific reminders to the commanding officers may assist with this issue in the future.
- b. Some REV registrants may have returned to Australia in sufficient time to cast a vote on polling day, raising the risk of such registrants casting a REV vote while in Australia (but no evidence that this occurred).

1.12.9 Management of Risks of Electoral Offences and Outcomes

- a. The AEC put in a range of controls to minimise the risks of electoral offences associated with the REV system and its associated processes. These were subject to an independent audit with satisfactory outcomes.
- b. Improvements were suggested in a number of areas to more easily manage the risks.
- c. There have been no allegations of electoral fraud and no official complaints arising from the trial.

1.12.10 Defence Observations

1.12.10.1 Key observations from Defence were as follows:

- a. DRN is capable of supporting electronic voting noting that alternative strategies were put in place to execute REV on the DRN. These alternative strategies specifically addressed accessibility by deployed ADF members to the DRN and complexities of the differing deployed systems.
- b. Considerable ADF coordination, management and resources were required in the implementation of the trial.
- c. Long lead times were required in the distribution of paper-based personal identification number (PINS) to ADF personnel to counteract the long distance and the sometimes unpredictable postal system. Future trials should consider removing the reliance on the postal system for the distribution of PINS.
- d. Regulation 62 resulted in some ADF personnel not being able to participate in the trial despite registering. Those ADF personnel who were in Australia at the time of issuing of the writ were excluded from participating in the trial even if they would be in the AO at the time of the election. ADF personnel frequently move in and out of operations at short notice. Future trials should, where possible allow all ADF personnel who have pre-registered for electronic voting and are in the deployed AO at the time of the election period to participate in electronic voting.

Letter of Agreement

1) Introduction

- a) Subsequent to our meeting of 24 October 2006, our respective staff met to clarify the conduct of the above project. Progress has been good, with effective working relationships established with the appropriate Department of Defence staff.
- b) I am writing to confirm the areas agreed for delivering remote electronic voting for overseas ADF Personnel.
- c) The AEC will be responsible for the development of the system to meet the requirements of the Commonwealth Electoral Act 1918 and our electoral processes.

2) Evaluation and Acquisition

- a) The AEC will:
 - i) Prepare the tender;
 - ii) Assess and evaluate responses in conjunction with Defence; and
 - iii) Negotiate and enter into a contract with the successful Tenderer.
- b) The ADF will:
 - i) Participate in the preparation of tender documents;
 - ii) Participate in the evaluation – including testing the offered systems, and
 - iii) Ensure as far as practicable with the test system that it meets with the requirements of operating within the Defence Restricted Network (DRN).

3) Connectivity

- a) Together the AEC and the ADF will establish connectivity between the computer systems using the ICON network.

4) Development and implementation

- a) The AEC will:
 - i) Manage the relationship with the Contractor;
 - ii) Install the system on AEC premises; and
 - iii) Manage modification of the system to meet AEC's requirements for a federal election.
- b) The ADF will:
 - i) Manage testing on the Defence Restricted Network; and
 - ii) Provide advice on encryption protocols so as to facilitate effective security of votes.

5) Voter registration

- a) Defence requires, and the AEC agrees, that only personnel deployed to specific operational areas will participate in the trial. These

areas are Iraq, Afghanistan, the Solomon Islands and East Timor. Ships and submarines will be excluded from this trial for technical reasons.

- b) The AEC will:
 - i) Provide forms for ADF personnel being deployed to areas that will participate in the trial to register as Remote Electronic Voters (REVs); and
 - ii) Provide, subject to tender responses, an authentication mechanism for REVs.
- c) The ADF will:
 - i) Provide appropriate ADF personnel with the registration forms, and facilitate their return to AEC; and
 - ii) Advise AEC when identified personnel are no longer eligible to be a REV, i.e., when they return to Australia or are deployed to an area that is not part of the trial.

6) **Election period**

- a) The AEC will:
 - i) Have the remote electronic voting system available for REVs to vote.
- b) The ADF will:
 - i) As far as practicable and subject to operational requirements, have the DRN available in identified areas for REVs to vote; and
 - ii) As far as practicable and subject to operational requirements, encourage REVs to vote and allow time for that purpose.

7) **Project personnel**

- a) The AEC team will consist of the following personnel:
 - i) Steering Committee Chair – Tim Pickering, First Assistant Commissioner Electoral Operations
 - ii) Project Sponsor – Doug Orr, Assistant Commissioner Elections
 - iii) Project Manager – Keith Millar, Director, Electronic Voting
 - iv) Deputy Project Manager – Judy Birkenhead, Assistant Director, Electronic Voting
 - v) Elections Systems Technical Advisor – Barbara Rab, Assistant Director, Elections Systems and Policy
 - vi) Technical Manager Applications – Amy Lu, Assistant Director IT Applications
 - vii) Technical Manager Infrastructure – Ben Smoker - IT Infrastructure Manager
- b) The ADF team will consist of the following personnel:
 - i) Project Board Executive: CDRE Mark Watson, DGEX-PE (Defence Business Owner)

- ii) Project Board Senior Supplier (Technology/CIOG) Kyrill Brent, Assistant Secretary Application Development
- iii) Project Board Senior Supplier (Policy): CAPT Andrew Whittaker RAN
- iv) Project Board Senior User: GPCAPT Grant MacDonald (HQJOC)
- v) Project Board Executive Assurance: Russell Philbey, Director
- vi) Team Manager (Tech/CIOG): Paul Remy-Maillet
- vii) Team Manager (Policy): Michelle Dean
- viii) Team Manager (User): WGCDR Lindsay Guerin/SQNLDR George Andric
- ix) Project Manager (Defence): Tony Lulic

8) Funding

- a) AEC will be responsible for:
 - i) The software and hardware for the system, including the server, the ICON connection and associated encryption devices;
 - ii) Any payments to the Contractor under the contract; and
 - iii) Staff costs for AEC's responsibilities detailed above.
- b) Defence will be responsible for:
 - i) Staff costs for Defence's responsibilities detailed above.

9) Summary

- a) Should the above arrangements be acceptable, I look forward to your response.

System and Associated Security Issues

The following system and associated security, issues together with mitigation or resolution of those issues, were provided to the Special Minister of State in February 2007.

The numbering from the Ministerial has been maintained.

5. Systems issue: Access

- (a) Issue
 - (i) Which ADF personnel will participate in the trial, and how will they access the voting application?
- (b) Resolution
 - (i) Defence has restricted the trial to Defence members and Defence civilians deployed to specific areas of operations (AOs): Iraq, Afghanistan, East Timor and the Solomon Islands;
 - (ii) As noted above, personnel on submarines and surface ships in these AOs will not participate in the trial; and
 - (iii) Only staff deployed in the AO that have a Defence Restricted Network (DRN) account will be able to vote electronically. After logging on, voters will navigate to the electronic voting application and complete identification and authentication prior to voting.

6. Security issue: the use of applets in the e-voting solution

- (a) Issue
 - (i) It is expected that the systems offered will use applets (a small piece of code) to encrypt votes.
- (b) Risks
 - (i) The DRN may not permit applets to pass through firewalls or travel through network connections; and
 - (ii) The software on target workstations may not be compatible with the applets used.
- (c) Resolution
 - (i) Applets will pass through the firewalls provided that the applets pass DRN sociability, performance and security testing;
 - (ii) Defence staff will test the applets for compatibility within Defence's environment, and will assist in a resolution if required. The assistance provided will not extend to Defence making baseline modifications to Defence's environment to accommodate the applet; and
 - (iii) Whilst best efforts will be made by all concerned, it should be noted that an inability by the vendors to meet Defence's and AEC 'compatibility' requirements may in effect result in the trial not proceeding.

7. Security issue: encryption

- (a) Issue
 - (i) It is expected that the systems offered will use encryption to ensure security of the votes.
- (b) Risks
 - (i) The DRN or Defence policies may not permit encrypted packages to pass through firewalls or travel through network connections; and
 - (ii) The offered encryption may not be compatible with target workstations in terms of encryption/decryption algorithms.
- (c) Resolution
 - (i) The system will be installed and accredited as per Defence requirements. Therefore encryption of the voting will be of an accepted Defence standard;
 - (ii) Defence will assist in identifying and resolving any issues in the area of encryption and decryption; and
 - (iii) The systems offered will be entirely responsible for encryption to ensure security of the vote. There will be no dependency upon the target workstations for encryption.

8. Security issues: Identification and Authentication

- (a) Issue
 - (i) An effective method of identifying a voter, then authenticating their identity is essential to ensure that the correct person exercises their right to vote.
- (b) Risks
 - (i) Although it is explicitly discouraged by Defence policy, some ADF personnel overseas share DRN logons;
 - (ii) Low user confidence in the authentication method will reduce participation in the trial; and
 - (iii) A voter's ability to vote may be usurped if a robust authentication method is not used.
- (c) Resolution
 - (i) The DRN logon process will not be used to authenticate the voter;
 - (ii) ADF personnel will be provided with a password issued by the AEC either prior to their deployment overseas, or via the Defence mail system; and
 - (iii) Potential suppliers will be asked to nominate more secure options, if they exist.

9. Security issue: user concerns re vote security

- (a) Issue
 - (i) ADF personnel may be concerned about the secrecy of their votes, that is, the ability of the system to effectively submit the vote for processing without any connection to the person who cast the vote.

- (b) Risks
 - (i) ADF personnel may not use the system.
- (c) Resolution
 - (i) The communication strategy will address this issue, and provide information to ADF personnel on the capability of the selected software's ability to ensure the secrecy of votes.

10. System issue: host server location

- (a) Issue
 - (i) The server that hosts the voting application may be housed at Defence or the AEC.
- (b) Risks
 - (i) The host organisation must have access to the operating system on the server, and subsequently access to the vote storage area. If this was any organisation other than the AEC, confidence in the integrity of the system may be questioned; and
 - (ii) If the server is hosted at the AEC, security of the connection with Defence may be a risk.
- (c) Resolution
 - (i) Defence agrees that the host server be located on AEC premises; and
 - (ii) To protect the connection with Defence, the server will comply with the following requirements:
 - (1) that the server is 'stand alone', that is, it must not be physically or logically connected to any other part of the AEC ICT network;
 - (2) that the security clearance level for the physical location meets the requirements for a RESTRICTED server installation; and
 - (3) that the security clearance level for staff with access to the server be at the PROTECTED level.

11. System issue: connectivity

- (a) Issue
 - (i) A secure connection must be used between the AEC and Defence.
- (b) Risks
 - (i) Security of the votes transmitted between the organisations may not be guaranteed; and
 - (ii) Security of the Defence network and the AEC voting application server may be compromised.
- (c) Resolution
 - (i) Connectivity between the organizations will be via ICON (Intra-government Communications Network), with hardware encryption on each end of the connection that meets the EAL2 standard (Evaluation Assurance Level 2). This connectivity

meets the requirements of the Defence Security Manual (DSM) which is the primary security reference document for Defence.

12. System issue: bandwidth

- (a) Issue
 - (i) Bandwidth varies significantly in the various areas of operations within the Defence network. In some areas there is a large bandwidth and few personnel, but in others, there is a small bandwidth with a large number of personnel. Also, some connections are not always available due to the complexities of the network; and
 - (ii) Traffic related to the voting application cannot impact on Defence operations, therefore operations traffic will have priority.
- (b) Risks
 - (i) The bandwidth may not be sufficient in some areas to permit voting; and
 - (ii) Period of high volumes of operations traffic may not permit voting at those times.
- (c) Mitigation
 - (i) This issue cannot be finally resolved prior to full system testing, and in some cases, before the actual election. However the risk is mitigated as follows:
 - (1) Defence will model the system using the estimated sizes of transmissions provided by each of the Tenderer, adding an administration load, to determine potential performance;
 - (2) All remote electronic voters will also be registered as general postal voters, so that if bandwidth issues during the election period prevent electronic voting, postal voting will still be possible; and
 - (3) Standard AEC procedures will apply to ensure multiple votes are not counted.

13. System issue: Naval Systems

- (a) Issues
 - (i) Submarines do not have sufficient bandwidth to permit effective online voting;
 - (ii) Surface ships are connected to NAVSYSLAN rather than the DRN, and these two networks would need to be connected for personnel on surface ships to participate in the trial; and
 - (iii) Surface ships are not generally connected permanently, but send and receive data in 'bursts' during the day.
- (b) Risks
 - (i) While the issues with surface ships may be able to be resolved, the work involved may impact the overall project so that a solution may not be available by the target date of 30 June 2007.

- (c) Resolution
 - (i) Personnel on submarines and surface ships will not participate in the trial.

14. System issue: Software Compatibility

- (a) Issue
 - (i) The supplied software must be compatible with Defence's systems so as to allow effective remote electronic voting.
- (b) Risks
 - (i) A system may be acquired that cannot be modified to allow effective remote electronic voting.
- (c) Mitigation
 - (i) Details of Defence's various software levels across the DRN will be provided to potential suppliers for them to comment on compatibility; and
 - (ii) Offered systems will undergo preliminary compatibility testing during tender evaluation.

Statement of Requirement

2 STATEMENT OF REQUIREMENT

2.1 Introduction

2.1.1 The Joint Standing Committee on Electoral Matters, in its report on the 2004 Federal Election, recommended that the Australian Electoral Commission (AEC) trial electronic voting for certain classes of voters.

2.1.2 The Government has supported the recommendation in principle. Two solutions are required: one for blind and vision impaired voters at polling places, and another for remote electronic voting for overseas Australian Defence Force (ADF) personnel.

2.1.3 This Statement of Requirements relates to the solution for overseas ADF personnel.

2.2 Summary of Requirements

2.2.1 AEC requires the provision of a remote electronic voting system for overseas ADF voters.

2.2.2 The requirements detailed in this Tender are for a limited trial only and include:

- a) A system to allow for the specific requirements of the Australian federal electoral system, that is, a voting system that allows for full preferential voting for the House of Representatives, proportional representation for the Senate, and caters for a referendum if necessary; and
- b) The requirement for modification of any offered system to ensure compatibility with the Department of Defence's secure intranet.

2.2.3 The voting application will reside on stand-alone servers in AEC's data centre, and be connected with the Defence Restricted Network (DRN) via the Intra-government Communications Network (ICON). The connection will include hardware encryption.

2.2.4 The system will be accessed by voters through the DRN. Only operationally deployed ADF personnel at a restricted number of overseas locations will participate in the trial. It is expected that the total number of participants will not exceed 3,000.

2.2.5 The successful tenderer will supply, install and support the voting application, and provide an interface for AEC staff to set up data for the election.

2.2.6 A module is required to print ballot papers

2.2.7 A module is required to extract Senate ballot paper data in a format suitable for upload into Central Senate Scrutiny System (CSSS – defined under Clause 2.12 Output below).

2.2.8 The voting process is explained in general terms below.

2.2.9 It is Most Important that a 'turn key' application be offered that will require minimal involvement of AEC's and Defence's information technology staff.

2.2.10 Tenderers must provide costings for the offered solution in the Pricing Schedule at TRS 4.

2.2.11 Tenderers must include the total cost for development of the software to final acceptance for implementation.

- a) If the tenderer proposes that software costs are to be met through a license agreement full details and costs of the licensing proposal must be provided.

2.3 High Level Process Diagram

2.3.1 A high level process diagram is at Attachment 1.

2.4 The Registration Process

2.4.1 Defence will provide AEC with details of ADF personnel who are deployed to areas that are covered by the trial, together with completed application forms from each person.

2.4.2 These personnel will be identified on AEC's electoral roll as Remote Electronic Voters (REV). It is expected that these voters will be given access to the voting application.

2.4.3 In providing access to the voting application, the following details will be recorded. Note that this list is not definitive:

- a) Voter identification number (extracted from the roll system);
- b) Name;
- c) Date of birth; and
- d) Division and State for which the voter is enrolled

2.4.4 It is Most Important that the offered system complies with the process detailed in this Clause 2.4.

2.4.5 Where the offered system includes a variation to this process, Tenderers must clearly explain the:

- a) differences;
- b) impact on the proposed process; and
- c) technical and/or administrative benefits.

2.5 The Voting Process

2.5.1 The voting process will be as follows:

- a) The REV will access the DRN and navigate to the voting application.
- b) The REV will identify himself or herself to the application, and authenticate his or her identity.
- c) The application will ask the REV to confirm that they have not previously voted in this election.
- d) The appropriate ballot papers will be presented to the REV for the House of Representatives, the Senate, and if applicable for any Referendum.
- e) The REV will make their selections, and the application will ask the REV to confirm their selections before casting the vote.
- f) The vote is cast.

g) The REV is provided with a receipt or similar that will verify to them that their vote has been accepted by the application and recorded for later counting.

h) The REV will exit the application.

2.5.2 It is Most Important that the offered system complies with the process detailed at Clause 2.5.1.

2.5.3 In relation to the receipt or similar mentioned at Clause 2.5.1 (g), it is Most Important that Tenderers explain how the receipt or similar can be used by the REV to verify that they have voted.

2.5.4 Where the offered system includes a variation to this process, Tenderers must clearly explain the:

- a) differences;
- b) impact on the proposed process; and
- c) technical and/or administrative benefits.

2.6 Equipment

2.6.1 The AEC proposes to provide 2 x HP/Compaq DL380 (or equivalent) servers on which the voting system is to be installed.

2.6.2 This equipment will be located in the AEC's Data Centre, in a rack which will be reserved exclusively for this project. The rack will also contain backup hardware, network switches, routers, firewalls, and encryption hardware all required for this project, all provided by the AEC.

2.6.3 The AEC prefers that the system is designed to run on a Windows Server 2003 environment, and the AEC will provide the hardware configured with a base installation of the operating system.

2.6.4 It is Essential that Tenderers advise the compatibility of their offered system with this hardware and software configuration.

2.6.5 Where the offered system is not compatible with this configuration, or where an alternative configuration will result in significantly better performance, it is Essential that Tenderers explain the optimum hardware and software configuration required.

2.6.6 In the event that the hardware detailed in Clause 2.6.1 is not suitable, it is Essential that Tenderers provide costs for alternative hardware in TRS4.

2.6.7 Where the server environment detailed in 2.6.3 is not suitable, it is Essential that Tenderers provide costs for any alternative operating system licences in TRS4.

- a) Such costs are to include installation of the server environment by the successful Tenderer.

2.6.8 AEC reserves the right at its sole discretion to accept the offer of alternative hardware and/or operating system, or to acquire appropriate hardware and/or operating system itself.

2.6.9 It is Essential that Tenderers install the system on the configured servers in accordance with the provided documentation.

2.6.10 For security purposes, AEC technical staff will be present at all times during the installation of the system. This will be both to provide the mandatory escort services, and also to ensure that the installation and the documentation are 100% compatible.

2.7 Security issues

2.7.1 Consultation

2.7.2 It is Essential that Tenderers agree to consult with staff of the Information Systems Division (ISD) Department of Defence on security issues, or as otherwise required by the Chief Information Officer's Group (CIOG), Department of Defence.

2.7.3 The purpose of this consultation is to satisfy ISD and CIOG that the offered systems pose no threat to the DRN, the security of deployed personnel or any other Defence interests.

2.7.4 Identification and Authentication

2.7.5 When a REV accesses the voting application, they must identify themselves, then provide some details that will authenticate their identity to the application.

2.7.6 Identification may be by means of the REV's name and date of birth, or by their employer identification number.

2.7.7 Authentication may be by providing something the REV knows, such as the answer to a specific question, or by providing something that the application has issued, such as a password.

2.7.8 It is Essential that Tenderers provide one or more methods of identification and authentication for consideration by the AEC.

2.7.9 In the event that the offered system will issue an authentication method, such as a password, it is Essential that Tenderers:

- a) Provide a method of reissuing the password or other item, should the REV lose the initially issued item; and
- b) Explain how a bulk issue, such as a contingent of ADF personnel being deployed at the same time, would be handled, including printing and mailing of the item.

2.7.10 Security of the votes

2.7.11 The AEC requires that the system offered guarantees the security of the votes cast, both in transmission through the DRN and the connection with AEC, and on the server. AEC envisages that such security may be via software encryption, however other solutions will be considered.

2.7.12 Security of the votes also includes the concept of not associating a vote with the person who cast the vote, in any way that will enable the person's intentions to be known.

2.7.13 It is Essential that Tenderers detail the method they are proposing for ensuring the security of votes cast, from the time of casting until the AEC is ready to process the stored votes.

2.7.14 It is also Essential that Tenderers explain the methodology for ensuring the security of the votes during processing, that is, during the period where votes will be printed and/or loaded into a data format, as explained below.

2.7.15 Encryption

2.7.16 Target workstations on the DRN must have compatibility with the product in relation to encryption and decryption algorithms. Where Defence's systems are not compatible in this area, ISD will work with the successful Tenderer to resolve the issue.

2.7.17 It is Essential that Tenderers agree to working with the ISD to resolve software encryption issues.

2.8 Systems issues

2.8.1 Bandwidth

2.8.2 The bandwidth of the DRN varies significantly in many of the areas where remote electronic voting will take place, and can be as low as 56 kb.

2.8.3 It is Essential that Tenderers explain how their software can perform on a network with such varied, and in places, restricted bandwidth.

2.8.4 It is Essential that Tenderers detail the size of the traffic that their software will generate for a single voter, using the worst case scenario of ballot paper sizes as explained in clause 2.11 below.

2.8.5 Bandwidth and network issues may cause the connectivity between the voter's workstation and the application server to be lost during voting.

2.8.6 It is Essential that Tenderers explain how their software would handle such circumstances detailed in Clause 2.8.5, and what recovery actions, if any, would enable the voting process to be completed. An explanation of what would happen to voting receipts that have not been delivered must be included.

2.8.7 Performance

2.8.8 As this is a trial involving ADF personnel around the world, the actual number of concurrent users cannot be reliably estimated. However, it can be safely expected that concurrent users will not exceed 500.

2.8.9 It is Essential that Tenderers detail the system response time in the event that concurrent users reaches 500.

2.8.10 Where this response time is adversely affected by the equipment mentioned in Clause 2.6, Tenderers must detail the changes necessary to that equipment to allow sub-second response times in the event that concurrent users reaches 500.

2.8.11 It is Highly Desirable that Tenderers offer suggestions for achieving low response times in a cost effective manner.

2.8.12 For the purposes of this Clause, 'response time' does not include network transmission time.

2.8.13 Compatibility

2.8.14 The voting application will reside on stand-alone servers in AEC's data centre, and be connected with the Defence Restricted Network (DRN) via the Intra-government Communications Network (ICON). The connection will include hardware encryption.

2.8.15 Configurations for each of Defence's various software levels currently in use are detailed at Attachment 4 [not attached for the purpose of the evaluation].

2.8.16 It is Essential that Tenderers detail the compatibility or otherwise of the offered system with Defence's various software levels.

2.8.17 In order to demonstrate the compatibility of the offered software with Defence's software levels, it is Essential that Tenderers provide a pilot installation of the offered software for testing during the evaluation period.

2.8.18 The pilot installation may be resident on a tenderer's server, with access over the Internet. In such a circumstance, all elements of the offered system must be available, including any proposed software encryption.

2.8.19 The pilot installation is not required to replicate an Australian federal election, but simply to demonstrate the level of compatibility with Defence's systems.

2.8.20 Tenderers will be advised of a time line for availability of the pilot installation, with a minimum of 5 working days notice. The pilot installation is to be available for a minimum of 5 working days.

2.8.21 It is Essential that Tenderers agree to the time frame detailed in Clause 2.8.20.

2.9 System Certification

2.9.1 It is Essential that the final system offered be independently audited to verify that the system is secure and accurate.

2.9.2 This audit will include the production of the printed output and the data extraction for upload into the CSSS.

2.9.3 For this purpose, the source code and other documents and equipment will be required to be made available to an independent auditor.

2.9.4 The independent auditor will be contracted to the AEC, and the terms of that contract will include confidentiality.

2.9.5 Tenderers must:

- a) indicate their agreement to participate in such an audit by way of the provision of the necessary source code, documents and equipment; and
- b) indicate any potential constraints on such an audit.

2.9.6 As well as the independent audit, Defence may require that the final system be audited by their staff or nominee. Should this occur, the audit would be by a discrete area within Defence or CIOG, or their nominee, and the staff involved will be required to meet the same confidentiality as the independent auditor.

2.9.7 It is Essential that Tenderers agree to having Defence or CIOG personnel, or their nominee, audit the system, should this be required.

2.9.8 In addition, the system is required to be audited to ascertain compliance with the relevant Chapters of ACSI 33. Again, the auditor will be required to meet the same confidentiality as the independent auditor.

- a) The Australian Government Information and Communications Technology Security Manual, also known as ACSI 33, can be found at: http://www.dsd.gov.au/_lib/pdf_doc/acsi33/acsi33_u.pdf

2.9.9 It is Essential that Tenderers agree to an ACSI 33 audit being undertaken by a person or organisation nominated by the AEC.

2.9.10 The AEC and Defence, as appropriate, will be responsible for the costs of conducting these audits.

2.9.11 If there are any costs for Tenderers in participating in these audits, it is Essential that Tenderers submit in the Pricing Schedule at TRS 4 details of those costs.

a) Where a cost is offered in the Pricing Schedule at TRS4, Tenderers must provide complete details of the reason for the cost and what it covers.

2.9.12 Tenderers should note that where their response to this Clause 2.9 results in a potentially ineffective audit of the system, they may be excluded from further consideration.

2.10 Documentation

2.10.1 It is Essential that the Contractor develops, in conjunction with AEC, a systems design specification. This specification must include details of the software, and any hardware provided as part of the solution.

2.10.2 In the event that the Contractor provides an alternative operating system as detailed in Clause 2.6.7 above, it is Essential that the Contractor provides comprehensive manuals for that operating system.

2.10.3 It is Essential that the Contractor develops and provides administration user guides both for technical staff and for election management staff.

a) The technical documentation must be comprehensive, particularly with regards to installing the system, maintaining the system throughout the entire project and performing routine maintenance such as backups.

b) It should also include details of how to pro-actively monitor both the health and performance of the system.

c) Full documentation of how to recover from critical errors should be provided. Such scenarios should include, but may not be limited to, total hardware failure, database corruption, application crashing, and restoration of data from backup media.

2.10.4 It is Essential that the Contractor develops and provides a user guide for voters.

2.10.5 It is Essential that documentation required by this clause be supplied in hardcopy and softcopy.

2.10.6 As this documentation will be developed for the AEC as part of this acquisition, with the exception of the operating system manuals, the ownership of the intellectual property will be vested in the AEC. It is Most Important that Tenderers state their level of compliance with this Sub-Clause 2.10.6.

2.10.7 Tenderers must include costs for this documentation, if applicable, in TRS 4.

a) Costs for the operating system manuals should be included in the cost of the operating system.

2.11 Election Setup

2.11.1 This clause outlines, in general terms, the elements that make up a federal election, and details the requirements to allow setup of the data for a federal election.

2.11.2 See Clause 2.14 for the timeframe for the next election, and for a potential timetable once an election is announced.

2.11.3 It is Essential that the election setup be undertaken by AEC officials to provide a level of confidence that this is within AEC's control.

2.11.4 Australia's federal elections generally consist of electing a member for each of the 150 House of Representatives electorates, and of electing Senators for each State and Territory.

2.11.5 At any federal election, a Referendum may also occur.

a) A Referendum consists of one or more questions, and for each of the questions, the elector must respond 'YES' or 'NO'.

2.11.6 Generally, if there are multiple Referendum questions, they are presented on a single ballot paper, but on some occasions, such multiple questions have been presented on multiple ballot papers.

2.11.7 Voting for the House of Representatives requires each candidate to be numbered from 1 up to the total number of candidates.

2.11.8 Voting for the Senate can be either:

- a) Marking a single preference for a group 'above the line' (ATL); or
- b) Numbering each box 'below the line' (BTL) from 1 up to the total number of candidates.

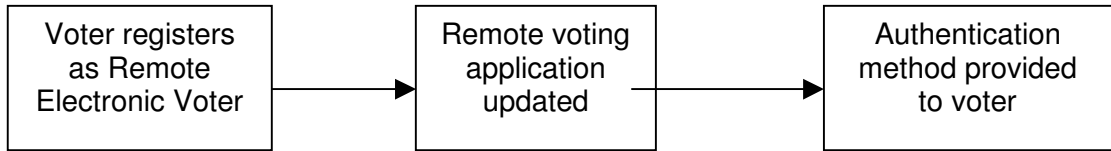
2.11.9 At the 2004 election for the House of Representatives, there were an average of 7.3 candidates per electorate. The maximum in any single electorate was 14.

2.11.10 The number of candidates and groups for the Senate ballot papers for the 2004 election is listed in the table below.

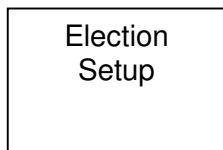
a) Note that the groups refer to lists of grouped candidates for whom a vote can be cast above the line.

State / Territory	Candidates	Groups	Ungrouped Candidates
NSW	78	29	4
VIC	65	19	8
QLD	50	21	2
WA	40	15	3
SA	47	16	3
TAS	26	9	4
ACT	13	6	1
NT	11	5	1

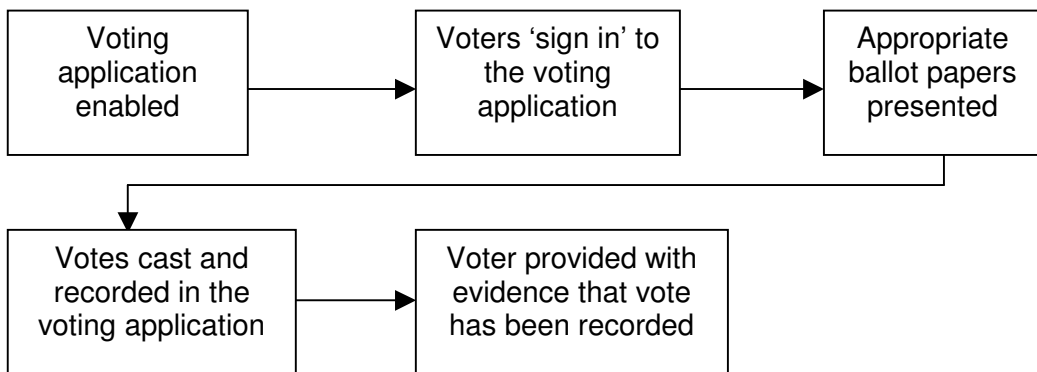
High Level Process Diagram
Electronic Voting for Overseas ADF Personnel
Voter registration



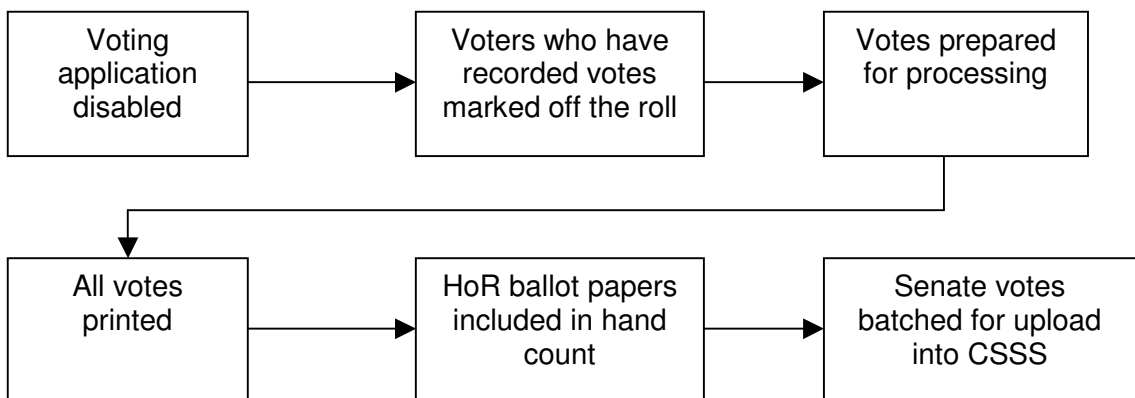
Pre-voting period preparation



Voting period



Post voting period



Note: HoR = House of Representatives
CSSS – Central Senate Scrutiny System

Project Schedule

Item	Start	Finish
Project Initiation	11-Sep-06	
AEC-Defence Consultation		
Defence AEC - initial project meeting	6-Oct-06	6-Oct-06
Project Meetings with Defence Personnel	6-Oct-06	29-Feb-08
Initial Project Board Meeting	18-Dec-06	18-Dec-06
Project Board Meetings	18-Dec-06	29-Feb-08
Legislation		
Develop Amendments	25-Sep-06	6-Dec-06
HoR - Amendments passed	6-Dec-06	
Senate Amendments passed	26-Feb-07	
Assent given	15-Mar-07	
Develop Regulations	1-Dec-06	5-Sep-07
Effective date	1-Aug-07	
Regulations approved	6-Sep-07	
Procurement		
Procurement Process Approval	16-Oct-06	
Develop Statement of Requirements	2-Oct-06	12-Jan-07
Release tender	12-Jan-07	
Tender open	12-Jan-07	30-Jan-07
Industry Briefing	18-Jan-07	18-Jan-07
Tender extension period	31-Jan-07	1-Feb-07
Tender close	1-Feb-07	1-Feb-07
Tender evaluation	2-Feb-07	2-Apr-07
Tender Evaluation - Pilot testing	16-Feb-07	1-Mar-07
Preferred Tenderer selected	3-Apr-07	3-Apr-07
Contract Negotiation	4-Apr-07	15-May-07
FMA 9 and 10 Approvals	15-May-07	15-May-07
Contract signing	18-May-07	18-May-07
System Development/Testing		
Software development		
'End to End' Testing on "Test" environment in Canberra	28-May-07	1-Jun-07
'Field' Testing in North Queensland (Exercise Talisman Sabre)	4-Jun-07	8-Jun-07

Item	Start	Finish
Australian and remote Testing from Canberra, North Queensland, Iraq, Afghanistan, Timor-Leste, Solomon Islands	25-Jun-07	
Testing during Solomon Islands Visit	20-Aug-07	23-Aug-07
Final validation of all DRN terminals	17-Oct-07	
System Audit		
Initiation	4-Jul-07	
Audit	5-Jul-07	31-Aug-07
Audit complete	31-Aug-07	
Certification Issued	14-Sep-07	
Communication		
Initiation	12-Jan-07	12-Jan-07
Plan development	12-Jan-07	26-Jul-07
Final Plan	26-Jul-07	26-Jul-07
Develop Voter Pamphlet	27-Apr-07	20-Sep-07
Solomon Islands promotion	20-Aug-07	23-Aug-07
Timor-Leste promotion	3-Oct-07	5-Oct-07
Registration		
Develop Registration Form	20-Jul-07	12-Sep-07
Registration of REVs	8-Aug-07	1-Nov-07
Pin Issues	5-Oct-07	8-Nov-07
Election Period		
Receive data, load and verify	4-Nov-07	4-Nov-07
Voting Period	5-Nov-07	24-Nov-07
Download and process data	25-Nov-07	25-Nov-07
Dispatch votes	25-Nov-07	
Receipt checking available	26-Nov-07	7-Dec-07
Final disconnect from Defence	7-Dec-07	
Decommissioning	31-May-08	
Project close	31-May-08	

'How to Cast your Vote' Pamphlet

Remote Electronic Voting for ADF personnel

HOW TO CAST YOUR VOTE

In the 2007 Federal Election

As a registered Remote Electronic Voter, you are able to vote in the 2007 federal election, while you are deployed overseas and if you can access the Department of Defence secure DRN.

This leaflet will help you to cast your vote in 7 easy steps.

Step 1 THE ELECTRONIC VOTING WEBSITE

From your Defence intranet browser, go to the internal Defence Remote Electronic Voting Page. The link is located on the main Defweb home page. Follow the prompts. It is likely that you will receive a 'Tip' about Citrix in its full screen mode – click 'OK'

Step 2 LOG IN

Your first name, surname and date of birth, as well as the PIN provided in the letter sent to you are required to log in.

Step 3 HAVE YOU VOTED PREVIOUSLY IN THIS ELECTION?

You can vote only ONCE in a federal election.

If you have already voted in this election by postal vote or at an overseas voting centre, then click on YES, and you will be logged out of the Remote Electronic Voting website.

If you answer NO, the system will display a page 'Detecting browser settings'. Wait, and follow the directions on your screen.

You will see a message box saying "The application provider signature has been verified – Do you want to run the application"

Click 'RUN' to continue voting.

Step 4 HOUSE OF REPRESENTATIVES BALLOT

When the House of Representatives ballot is displayed, you must number the box next to each candidate's name in the order of your choice.

Move the cursor to the box next to the candidate of your FIRST choice, **double click**, and the number 1 will appear. Repeat this process by moving the mouse to the other candidates in order of your choice, **click**, and they will be numbered in consecutive order.

You MUST number EVERY box by clicking with the mouse.

With all boxes numbered, click on NEXT and your selections will be displayed for your review. You may change the order of your preferences by following the instructions. When you have checked that all boxes are numbered according to your choice, click NEXT.

Step 5 THE SENATE BALLOT

You can vote in either one of two ways for the Senate.

Above the line

This method of voting for Senate candidates means you may select a group voting ticket that you wish to adopt as your vote by putting the number '1' in the appropriate square.

By voting 'above the line', you will be choosing to follow the preferences contained in the group voting ticket that the party or group has lodged with the Australian Electoral Commission.

Below the line

This means you decide your order of choice for EVERY candidate listed below the line. You vote by moving the cursor to the candidate of your FIRST choice, click, and the number 1 will appear.

Move the mouse to the other candidates in order of your choice, click, and they will be numbered in consecutive order.

You MUST number EVERY box.

When all boxes are numbered, click on NEXT and your vote will be displayed for your review. You may change the order of preference by following the instructions on the screen.

When you have checked that all boxes are numbered according to your choice, click NEXT.

Your Senate vote will then be cast.

IF THERE IS A REFERENDUM

If a referendum is also being conducted, the screen will now display the referendum question or questions.

Move the cursor to the box beside a question and type 'YES' or 'NO' to signify you agree or disagree.

Click on NEXT to review your typed answer. You may change your answer by following the instructions on the screen.

Click NEXT again and your vote will be cast.

Step 6 YOUR RECEIPT

When you have finished voting, you will be asked for a KEYWORD. Enter an easy-to-remember key word using letters or numbers or any combination thereof, and a receipt will be issued which you can print or write down and keep with this leaflet.

Step 7 CONFIRMING YOUR VOTE

If you want to confirm that your vote has been lodged, you can go to internal Defence Remote Electronic Voting (REV) Page and click on the 'Receipt' link.

If you check before election day, you will be asked for your first name, surname, date of birth and PIN. The system will then only confirm if your vote was cast.

If the system advises that your vote has not been received or that your voting session was not complete, then you should log in again and complete your voting session.

The day after polling day, votes will be accepted by AEC officials. On the following day, you can check to see if your vote was successfully accepted.

Go to the internal REV Page, click 'Receipt' link and you will be asked for first name, surname, date of birth and your KEYWORD, (used to get your receipt). If your vote has been accepted for counting, the system will correctly recreate the receipt that you were issued with after voting.

In the event of errors in receipt checking, please contact your local CIS Support.

Remote Electronic Voting

is a secret ballot.

How you vote is your business. Everyone has the right to the same privacy.

Keep your Remote Electronic PIN confidential.

Cast your vote in private.

NEED HELP?

Contact your local CIS Support.



Application to register for remote electronic voting for the 2007 federal election



Office use only	Date received	SC	ADK	RM	NH
I		GV	N		

Who can register as a remote electronic voter?

You are eligible to register as a remote electronic voter if you are already enrolled and are an Australian defence member or an Australian defence civilian who will be serving in the following operational areas at the time of the 2007 federal election:

- Iraq (AFPO 19 or 20)
- Afghanistan (AFPO 13 or 14)
- Timor-Leste (AFPO 5)
- Solomon Islands (AFPO 11)

You can check your enrolment details at www.aec.gov.au

Remote electronic voting at federal elections

Electors who are registered as remote electronic voters will be mailed a personal identification number (PIN) and a pamphlet entitled 'How to cast your vote at the 2007 federal election'. Access to remote electronic voting will be via the Defence Restricted Network.

Electronic voting will be available from the Monday after the declaration of nominations for the federal election and up to 6pm Western Australian time on polling day.

Remote electronic voters and general postal voters

As a backup measure remote electronic voters will also be registered as general postal voters, and will be mailed postal voting material as soon as practicable after the declaration of nominations for the federal election. In the event that a remote electronic voter cannot access the electronic method for any reason, the postal voting material should be used to cast your vote.

Electors must not vote twice

Electors may vote electronically or by postal vote, but must not use both methods unless there is a reason to believe that the electronic method has not been successful (e.g. loss of connection prior to the completion of the voting process). Only one vote will be counted. An electronic vote will take precedence over a postal vote.

Further information

If you have any queries, please contact the AEC on 13 23 26 or at www.aec.gov.au

The register containing details of registered electronic voters will not be available for public scrutiny.

Returning your form

Fax your application to:

New South Wales	+ 61 2 9281 9384
Victoria	+ 61 3 9285 7167
Queensland	+ 61 7 3832 3058
Western Australia	+ 61 8 6363 8051
South Australia	+ 61 8 8231 2664
Tasmania	+ 61 3 6234 4268
Australian Capital Territory	+ 61 2 6257 6014
Northern Territory	+ 61 8 8981 4725

If completing by hand use: X in the boxes where appropriate, black or blue ink and BLOCK LETTERS. Note: Giving false or misleading information is a serious offence.

1. Name		Mr <input type="checkbox"/>	Mrs <input type="checkbox"/>	Ms <input type="checkbox"/>	Miss <input type="checkbox"/>	Dr <input type="checkbox"/>	Other <input type="checkbox"/>	<input type="text"/>	
		Family name <input type="text"/>							
		Given name(s) <input type="text"/>							
2. Your enrolled address		<input type="text"/>							
		<input type="text"/>					State <input type="text"/>	Postcode <input type="text"/>	
3. Postal address		Operation name		<input type="text"/>			AFPO	<input type="text"/>	
		AUST DEFENCE FORCES		State	NSW	Postcode	2890		
4. Date of birth		Write dates as dd/mm/yyyy		e.g. 25/03/1975		5. Gender		Male <input type="checkbox"/>	Female <input type="checkbox"/>
6. Dates you expect to be serving outside Australia		Expected date of departure		<input type="text"/>		Expected date of return		<input type="text"/>	
7. Contact details (if convenient)		Daytime (or mobile) phone number		<input type="text"/>					
		Email address <input type="text"/>							
8. YOUR DECLARATION		<p>I am currently enrolled and seek to register for remote electronic voting and as a general postal voter.</p> <p>I am a member of the Australian defence force, or an Australian defence civilian who is serving, or may serve, outside Australia in one of the identified operational areas.</p> <p>I authorise the AEC to disclose my personal information to the Department of Defence in order to seek confirmation of my eligibility to participate in the trial of remote electronic voting.</p>							
<small>Authorisation to collect the information on this form is contained in the Commonwealth Electoral Act 1918</small>		Signature of elector					Date <input type="text"/>		

BR029w_0007

© Commonwealth of Australia 2007

Standard AEC Letters

The following standard letters were used to respond to applications for registration as a Remote Electronic Voter.

- En2559 Approval of REV Registration
- En2560 Additional Info REV Registration
- En2561 Rejection of REV Registration
- En2589 Cancellation of REV Registration
- En2590 Amendment of REV Postal Address

Each of these letters is reproduced on the following pages.

En2559 Approval of REV Registration

REV Registration

Approval Ve



Division of Brisbane
GPO Box 222
BRISBANE QLD 4000

Division of Brisbane
488 Queen St
BRISBANE QLD 4000

Telephone: (07) 1111 1111
Facsimile: (07) 2222 2222

FirstNames Surname
Postal Address 1
Postal Address 2
POSTAL ADDRESS 3

Ref No:
Contact: Joe Bloggs

Dear *Title Surname*

REGISTRATION AS A REMOTE ELECTRONIC VOTER

I have approved your application to participate in the trial of remote electronic voting being undertaken for the 2007 federal election.

You are now registered as an electronic voter as well as a general postal voter for the Division of <division name>.

Instructions on how to cast your electronic vote will be sent to you shortly. You will also be issued with a PIN to access the electronic voting system. You should keep your PIN in a safe place and use it when voting is available for the 2007 federal election. The voting period for the election will commence approximately three weeks prior to polling day.

Following the announcement of the federal election, as a remote electronic voter you will also be sent postal voting material which can be used if you are not able to access the Defence Restricted Network. This voting material will be sent to you at <postal address>.

If you record your vote electronically, you should destroy your postal voting material. You can only vote once.

For your vote to count you must either vote electronically before 6:00pm Western Australian time, or complete and post the completed ballot papers before the close of polling as they must be received by me within 13 days after polling day. If the ballot papers are unlikely to reach me before the deadline, the material may be mailed or delivered, before the close of polling, to an Assistant Returning Officer at an Australian diplomatic post that provides a polling service.

If you are unlikely to have access to the electronic voting system or your postal voting material does not reach you before polling day, you may vote at an Australian diplomatic post providing polling services, either in person or by applying for a postal vote through them.

If you make a permanent change to either your residential or postal address you should complete a fresh application for enrolment so that I can update your enrolment details and ensure postal voting material is correctly addressed.

Yours sincerely

Divisional Returning Officer

(DATE)

En2560 Additional Info REV Registration



Division of Brisbane
GPO Box 222
BRISBANE QLD 4000

Division of Brisbane
488 Queen St
BRISBANE QLD 4000

Telephone: (07) 1111 1111
Facsimile: (07) 2222 2222

FirstNames Surname
Postal Address 1
Postal Address 2
POSTAL ADDRESS 3

Ref No:
Contact: Joe Bloggs

Dear *Title Surname*

REGISTRATION AS A REMOTE ELECTRONIC VOTER

Recently you applied for registration to participate in the trial of remote electronic voting being undertaken for the 2007 federal election.

Unfortunately, your application cannot be processed as it is missing some detail as indicated below:

- <your signature on the application>
- <an application for electoral enrolment as a check of our records indicates that you are not currently enrolled for the address indicated on your application>

Before I can register you as a remote electronic voter I will require a <fresh fully completed and signed application for registration> <new enrolment form to update your enrolment details>.

If you need any assistance in this matter, please contact this office on the above telephone number.

Yours sincerely

Divisional Returning Officer

DATE

En2561 Rejection of REV Registration



AEC

Australian Electoral Commission

GPO Box 222
BRISBANE QLD 4000

Division of Brisbane
488 Queen St
BRISBANE QLD 4000

Telephone: (07) 1111 1111
Facsimile: (07) 2222 2222

FirstNames Surname
Postal Address 1
Postal Address 2
POSTAL ADDRESS 3
<email address>

Ref No:
Contact: Joe Bloggs

Dear *Title Surname*

REGISTRATION AS A REMOTE ELECTRONIC VOTER

Recently you applied for registration to participate in the remote electronic voting trial being undertaken for the 2007 federal election.

Unfortunately I cannot approve your application because <you are not currently enrolled> OR <your application for registration for the remote electronic voting trial was received after registration closed at 8:00pm on [day date], and as a result you will not be able to cast your vote electronically at this election> OR <the Department of Defence has advised that you will not be deployed in one of the areas of operations identified to take part in the trial> OR <the information you provided indicates that you will not be deployed in one of the areas of operations identified to take part in the trial> OR < information provided on your application indicates you had not left Australia at the cut-off for registration on 17 October 2007, and as a result you will not be eligible to cast your vote electronically at this election >.

(if unenrolled and received before issue of writ)

<If you are eligible for enrolment you should complete and return the enclosed application for electoral enrolment, and should you wish to re-apply for registration as a remote electronic voter you must also complete and return the enclosed registration form.>

OR

(if unenrolled and received on or after issue of writ)

<Enrolment for this election closed at 8pm on [day date]. As your application for enrolment was received after this time, it was unable to be processed for this election and I cannot register you to participate in the remote electronic voting trial.>

OR

(if enrolled but REV registration received after cutoff OR not entitled to REV registration because of country of deployment OR if enrolled but not deployed by cutoff (ie 17/10/2007))

<However, as your registration form entitles you to vote by post, [postal voting material will be sent to you at the above address] OR [I have enclosed postal voting material for you to complete].>

If you use this postal voting material the completed ballot papers must be posted before the close of polling and received by me within 13 days after polling day. If the ballot papers are unlikely to reach me before the deadline, the material may be mailed or delivered, before the close of polling, to an Assistant Returning Officer at an Australian diplomatic post that provides a polling service.

If you are able to access an Australian diplomatic post that provides a polling service, you may prefer to vote there in person. If you receive the postal voting material sent to you from Australia after voting at a diplomatic post, this material should be destroyed.>

If you make a permanent change to either your residential or postal address you should complete a fresh application for enrolment so that I can update your enrolment details and ensure postal voting material is correctly addressed.

OR

(if not deploying until polling day or later)

<Once you leave Australia your application entitles you to registration as a General Postal Voter. If a federal election, by-election or referendum should occur during the time of your deployment you will be mailed postal voting material to [postal address]. However, as you will still be in Australia for the 2007 federal election you will need to either attend a polling place on voting day, have an early vote or apply for a postal vote. Postal vote applications are available from the AECs website at www.aec.gov.au.>

OR

(if unenrolled and no enrolment form received before 8PM on day of issue of writ)

<All eligible people are required to enrol and vote in federal, state and local government elections. You are eligible to enrol and vote in federal election if you are an Australian citizen or a British subject who was enrolled on 25 January 1984, if you are 18 years or older and if you have lived at your address for at least one month.

To help you I have enclosed a partially completed enrolment application. Please check the details carefully, complete any missing information before you sign and return it to me as soon as possible in the reply paid envelope provided.

Remember to keep your enrolment up to date. Every time you move address you need to complete a new enrolment application and send it to the AEC for your current address to be recorded on the electoral roll.>

Yours sincerely

Divisional Returning Officer

DATE

En2589 Cancellation of REV Registration



AEC

Australian Electoral Commission

GPO Box 222
BRISBANE QLD 4000

Division of Brisbane
488 Queen St
BRISBANE QLD 4000

Telephone: (07) 1111 1111
Facsimile: (07) 2222 2222

FirstNames Surname
Postal Address 1
Postal Address 2
POSTAL ADDRESS 3

Ref No:
Contact: Joe Bloggs

Dear *Title Surname*

REGISTRATION AS A REMOTE ELECTRONIC VOTER

I wrote to you recently advising that I had approved your application for registration to participate in the remote electronic voting trial being undertaken for the 2007 federal election.

One of the conditions of registration is deployment in one of four specified areas of operations.

<I have since received advice from the Department of Defence which indicates that you will not be deployed in one of the areas of operations identified to participate in the trial> OR <My records indicate that you have now returned to Australia> OR <My records indicate that you have not yet left Australia and the deployment cut-off for remote electronic voting registration was Wednesday 17 October 2007>.

(If still deployed but not in one of the identified REV areas OR is still deploying to an identified REV area but had not left Australia by issue of writ)

<As a result, I have cancelled your registration as a remote electronic voter, however, you are still registered as a general postal voter and your postal voting material will be mailed to you at <postal address.

For your vote to count you must complete and post the completed ballot papers before the close of polling as they must be received by me within 13 days after polling day. If the ballot papers are unlikely to reach me before the deadline, the material may be mailed or delivered, before the close of polling, to an Assistant Returning Officer at an Australian diplomatic post that provides a polling service.

If your postal voting material does not reach you before polling day, you may vote at an Australian diplomatic post providing polling services, either in person or by applying for a postal vote through them.

If you make a permanent change to either your residential or postal address you should complete a fresh application for enrolment so that I can update your enrolment details and ensure postal voting material is correctly addressed. >

OR

(Returned by issue of writ)

<As a result, I have cancelled your registration as both a remote electronic voter and as a general postal voter. However, if you expect to be deployed again at some time in the future may re-apply for registration as a general postal voter.>

Yours sincerely

Divisional Returning Officer

DATE

En2590 Amendment of REV Postal Address



AEC

Australian Electoral Commission

Division of Brisbane
GPO Box 222
BRISBANE QLD 4000

Division of Brisbane
488 Queen St
BRISBANE QLD 4000

Telephone: (07) 1111 1111
Facsimile: (07) 2222 2222

FirstNames Surname
Postal Address 1
Postal Address 2
POSTAL ADDRESS 3

Ref No:
Contact: Joe Bloggs

Dear *Title Surname*

REGISTRATION AS A REMOTE ELECTRONIC VOTER

I wrote to you recently advising that I have approved your application to participate in the remote electronic voting trial being undertaken for the 2007 federal election.

In addition to being registered for the trial I also advised that you have been registered as a general postal voter and that your postal voting material would be mailed to you at <previous postal address>.

I have since received advice from the Department of Defence that your postal address while on deployment will be <AFPO postal address>. I have updated my records accordingly and your postal voting material will now be mailed to you at this address.

Remember, if you record your vote electronically you should destroy your postal voting material. You can only vote once.

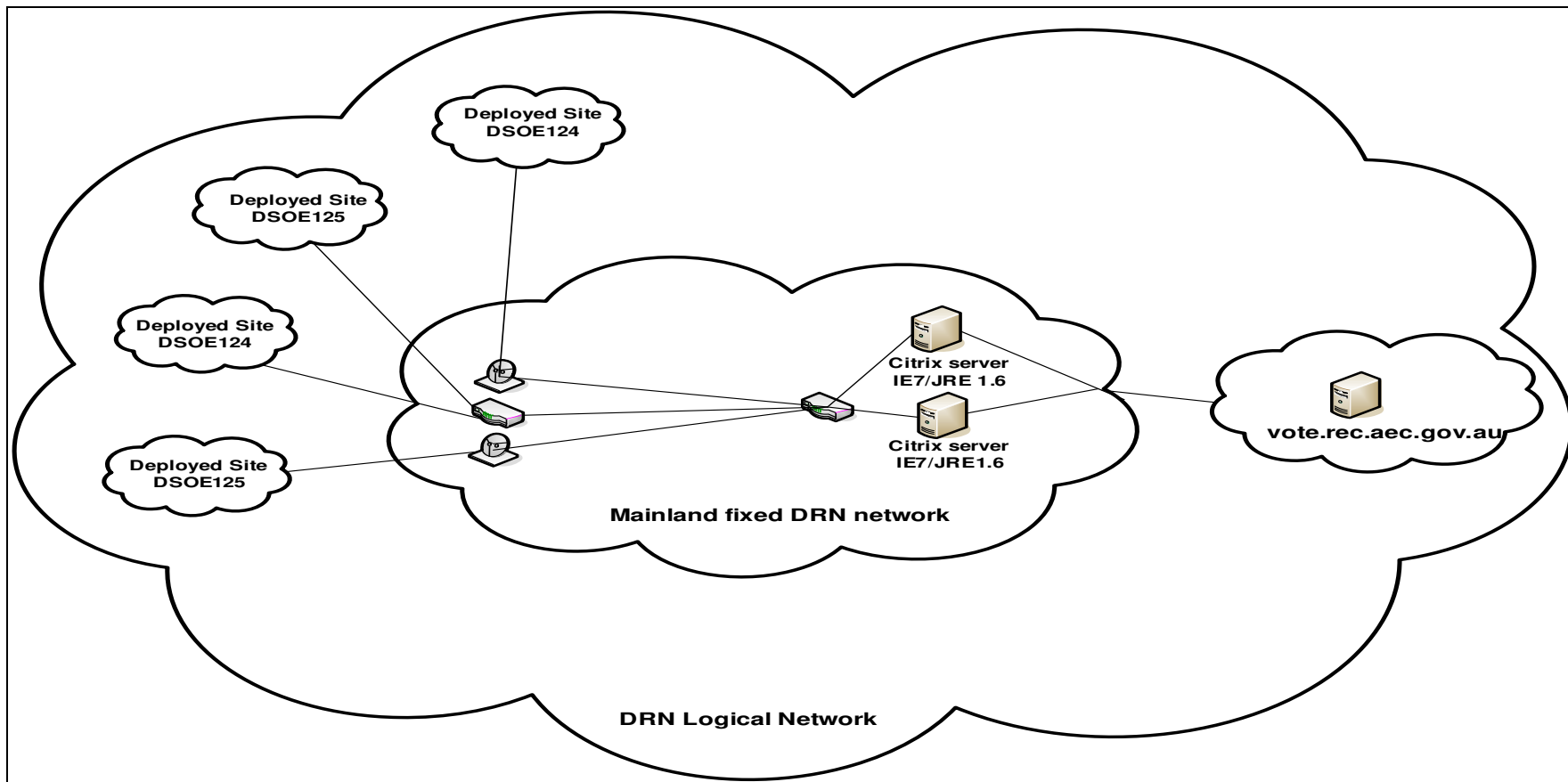
If you make a permanent change to either your residential or postal address you should complete a fresh application for enrolment so that I can update your enrolment details and ensure postal voting material is correctly addressed.

Yours sincerely

Divisional Returning Officer

DATE

Remote Electronic Voting System Architecture



Loading and Checking Procedures – Diacritical Marks

Note:

Of all candidate names for the 2007 federal election, a single name contained a diacritical mark. This was a letter ‘s’ with a ‘cedilla’, as follows:



DATA LOAD


1. Data will be supplied in CSV (comma separated variable) format.
2. For the single diacritical mark, replace the ‘S’ in the candidate’s name with the “HTML Entity Decimal” coding, that is, “Ş”.
3. Proceed with the data load as per the manual.

TESTING

4. Normal testing is to be carried out, with additional attention paid to the correct representation of the cedilla on the relative ballot paper.

Remote Electronic Voter User Questionnaire

2007 FEDERAL ELECTION QUESTIONNAIRE FOR VOTERS REGISTERED FOR REMOTE ELECTRONIC VOTING					
<p>You registered to vote at the 2007 Federal Election using remote electronic voting (REV) on the Defence Restricted Network (DRN). REV is being undertaken on a trial basis for this election, and so your feedback is very valuable to determine how it went.</p> <p>By filling in this questionnaire you will assist the Australia Electoral Commission (AEC) and the Department of Defence to provide feedback on the trial to the Parliament of Australia.</p> <p>Your response is anonymous and will be treated "in confidence"; your name is not required on this questionnaire form, nor on the attached envelope. Please complete and return this questionnaire once you have voted. All questionnaires should be completed and returned in the envelope provided as soon as possible after 24th November, even if you did not vote electronically.</p>					
1. Where were you serving at the time of the election? (tick one)	<input type="checkbox"/> Afghanistan	<input type="checkbox"/> Timor-Leste			
	<input type="checkbox"/> Iraq	<input type="checkbox"/> Solomon Islands			
2. How did you find out about remote electronic voting? (Tick boxes and fill in all relevant boxes. More than one box can be ticked/filled in.)	<input type="checkbox"/> Force preparation training.	<input type="checkbox"/> DRN web-site			
	<input type="checkbox"/> Warning Order	<input type="checkbox"/> Operational Order			
	<input type="checkbox"/> Information from Commanding Officer	<input type="checkbox"/> Other word-of mouth (eg colleagues)			
		<input type="checkbox"/> Other: _____			
3. Did you receive your PIN early enough to allow time to vote? (tick one)	<input type="checkbox"/> Yes (go to Question 4)	<input type="checkbox"/> No (please explain, eg didn't arrive at post in time, couldn't receive mail due to operational reasons)			
	↓				
		(go to Question 15 over page)			
4. Did you need to ask for a replacement PIN? (tick one)	<input type="checkbox"/> Yes (go to Question 5)	<input type="checkbox"/> No (go to Question 6)			
	↓				
		(go to Question 15 over page)			
5. Did you receive your replacement PIN early enough to allow time to vote? (tick one)	<input type="checkbox"/> Yes (go to Question 6)	<input type="checkbox"/> No (please explain, eg didn't arrive at post in time, couldn't receive mail due to operational reasons)			
	↓				
		(go to Question 15 over page)			
6. Did you access the DRN to vote? (tick one)	<input type="checkbox"/> Yes (go to Question 7)	<input type="checkbox"/> No (go to Question 14 over page)			
	↓				
7. How would you rate the following in voting using the DRN:	Rating (circle one)				Comments (Comments are particularly important if you circled 4 or 5)
	very good	neutral	very poor		
a. Availability of the DRN in order to vote?	1	2	3	4	5
b. Clarity of the instruction pamphlet that came with your PIN?	1	2	3	4	5
c. Clarity of the on-screen instructions?	1	2	3	4	5
d. Privacy of the location allocated for voting using the DRN?	1	2	3	4	5
e. The speed with which the DRN allowed you to log on and cast your vote?	1	2	3	4	5

8. Did you complete your vote on DRN? (tick one)	<input type="checkbox"/> Yes (go to Question 9) 	<input type="checkbox"/> No (please explain) <hr/> (go to Question 11)					
9. Did you use the vote checking service before/after voting closed? (tick one)	<input type="checkbox"/> Yes, only before voting closed <input type="checkbox"/> Yes, only after voting closed <input type="checkbox"/> Yes, both before and after	<input type="checkbox"/> No (go to Question 11)					
10. How would you rate:	<table border="1"> <tr> <td>very good</td> <td></td> <td>neutral</td> <td></td> <td>very poor</td> </tr> </table>	very good		neutral		very poor	Comments (Comments are particularly important if you circled 4 or 5)
very good		neutral		very poor			
a. the ease of use of the vote checking service? (circle one)	<table border="1"> <tr> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> </tr> </table>	1	2	3	4	5	
1	2	3	4	5			
b. the value of vote checking service? (circle one)	<table border="1"> <tr> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> </tr> </table>	1	2	3	4	5	
1	2	3	4	5			
11. What is your level of satisfaction with:	<table border="1"> <tr> <td>very satisfied</td> <td></td> <td>neutral</td> <td></td> <td>very dissatisfied</td> </tr> </table>	very satisfied		neutral		very dissatisfied	Comments (Comments are particularly important if you circled 4 or 5)
very satisfied		neutral		very dissatisfied			
<input type="checkbox"/> the level of service remote electronic voting provided? (circle one)	<table border="1"> <tr> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> </tr> </table>	1	2	3	4	5	
1	2	3	4	5			
12. Would you use remote electronic voting at a future Federal Election or referendum? (tick one)	<input type="checkbox"/> Yes	<input type="checkbox"/> No (please explain or provide comment) <hr/>					
13. Please give any other comments or suggestions for future improvement?	<hr/> <hr/>						

Please answer Question 14 if you were issued/reissued a PIN in time and did not access the DRN to vote		
14. What was the reason that you didn't access the DRN to vote? (Tick boxes and fill in all relevant boxes. More than one box can be ticked/filled in.)	<input type="checkbox"/> DRN was down when I had time to vote <input type="checkbox"/> Queue to access the DRN too long when I had time to vote <input type="checkbox"/> DRN was otherwise not available when I had time to vote	<input type="checkbox"/> Operational reasons prevented me from accessing the DRN <input type="checkbox"/> I chose not to access the DRN to vote <input type="checkbox"/> Other: <hr/> (go to Question 16)

Please answer Question 15 if you did not complete a vote using remote electronic voting on the DRN.		
15. Did you cast a vote in the 2007 Federal Election? (tick one)	<input type="checkbox"/> Yes, I cast a postal vote <input type="checkbox"/> Yes, I cast a vote another way (please give details) <hr/>	<input type="checkbox"/> No, I chose not to vote <input type="checkbox"/> No, I was unable to cast a vote (please give details) <hr/>

Focus Group Questions

DROs Staff

- The process for registering ADF personnel for remote electronic voting. Can you comment on:
 - Any issues that you encountered.
 - How these issues might be overcome in the future.
- The receipt of votes cast via remote electronic voting in print format and vote receipt and processing. Can you comment on:
 - The timeliness with which you received these votes?
 - Did you encounter any issues with timeliness?
 - How might timeliness be improved in the future?
 - With respect to the processing of these votes, can you comment on:
 - Instructions contained within the envelope with the votes. Were the instructions clear and sufficient. Any suggestions for improvements?
 - Did you also note the instructions sent in the Election Bulletin? Did this assist?
 - Mark back process in dec scrutiny. Did any issues arise?
 - Inclusion of the votes in the postal scrutiny?
 - Did you find any issues overall with ensuring that individual's votes were secret.
 - Extra workload associated with the remote electronic voting.

**Independent Trial Evaluation
Summary of Findings and Recommendations**

Note that references in this table refer to paragraphs in the report “Evaluation of the remote electronic voting trial for overseas based ADF personnel electors at the 2007 Federal Election”.

Key Findings	In any future implementation of REV, the following considerations are recommended:
<p>3.1 Take-up for the use of REV</p> <ul style="list-style-type: none"> ▪ 2012 ADF personnel applied for REV registration and were eligible to vote using REV, representing 80% of ADF personnel deployed to the trial areas. The variations in take-up across locations varied only marginally. 	
<ul style="list-style-type: none"> ▪ The AEC faced a number of challenges in registering eligible electors and ensuring that they remained eligible, impacting particularly on workloads in DOs at one of their busiest times. These included the following: <ul style="list-style-type: none"> ○ Due to security restrictions on REV registrations on RMANS, DO staff were unable to easily browse to identify registration details that might need amending, only able to execute amendments through a detailed set of instructions. ○ The AEC did not realise until after it received initial REV applications that AFPO addresses were not being provided and would be needed to reach registrants. This required the form to be modified and reissued to guide the applicant. For applications already received, they were investigated and 	<ul style="list-style-type: none"> a) registration should be encouraged as part of the preparation for overseas deployment; b) a fresh enrolment application should be encouraged from those seeking REV registration at the time of completing the REV/GPV registration form; c) all those who are registered and are expected to be overseas at the time based on the dates on their registration form, should be potentially eligible to cast a vote electronically – the registration form should be amended to guide registration to fill in specific dates to facilitate this; d) the AEC should investigate whether there is any feasible

Key Findings	In any future implementation of REV, the following considerations are recommended:
<p>the registration details amended in RMANS.</p> <ul style="list-style-type: none"> ○ Initially Defence did not advise that the trial would be restricted to certain AFPO addresses, and then only advised of five of the six AFPO addresses, requiring DOs to initially reject some REV registrants and then to reaccept some of these at a later date. ○ Defence could not provide the AEC with a list of ADF personnel eligible for REV registration, relying on the AEC to send them a list of potentially eligible REV registrants on which Defence checked and provided feedback. ○ Many of the REV applicants were not enrolled for the address they claimed on their REV application form. 	<p>means to exclude those who have returned to Australia earlier than the date on their REV application form, and prevent them from casting an electronic vote should they attempt to do so when in Australia, if this is consistent with Government's decision on eligibility;</p>
<ul style="list-style-type: none"> ▪ 75% of REV registrants cast a vote using REV. This varied considerably across locations from 92% of registrants deployed to the Solomon Islands down to 52% of registrants deployed to Timor-Leste. ▪ The main nominated reason for poor take-up of REV in Timor-Leste was operational reasons. 	
<ul style="list-style-type: none"> ▪ 4.6% of survey respondents (twenty) commented on the time it took to receive their PINs, preventing a number of them from voting using REV. 	<ul style="list-style-type: none"> e) the method to most effectively distribute PINs to REV registrants in time to vote should be investigated; f) full overseas addresses should be included in the REV/GPV application form to speed mail delivery;

Key Findings	In any future implementation of REV, the following considerations are recommended:
<ul style="list-style-type: none"> ▪ The number of deployed personnel known to cast a vote at this election is significantly higher at 1740 (or 50% of total) when compared with those for the 2004 Federal Election when only 311 (or 23% of total) were known to vote. 	
<p>3.2 Communication Strategy to Inform Users</p> <ul style="list-style-type: none"> ▪ Defence took primary responsibility for developing and implementing the communication strategy. The AEC undertook supplementary activities including visits to Timor-Leste and the Solomon Islands, provision of information on REV on the AEC web-site, joint media releases with Defence, and participation in a video conference with commanding officers in the areas of operation. ▪ The two main means by which REV registrants found out about the trial was mainly through Force preparation training, secondly from information from commanding officers and thirdly through word-of-mouth. It indicates the importance of providing commanding officers with sufficient information to pass on to the personnel under their command. 	<p>g) the AEC should provide Defence with feedback on the key means by which REV registrants found out about the trial, urging them to take it into account in future implementations of REV;</p>
<p>3.3 Use of Postal Voting by Registrants</p> <ul style="list-style-type: none"> ▪ Casting a postal vote was still a popular means of casting a vote even for those who were REV registered and could not, or chose not to, cast a REV vote. However, for every seven REV votes cast, one postal vote was cast. 	<p>h) the AEC should maintain GPV registration for REV ADF registrants, allowing REV registrants an alternative means of casting a vote if unable to cast their vote electronically;</p>

Key Findings	In any future implementation of REV, the following considerations are recommended:
<p>3.4 User Acceptance of REV</p> <p>Overall satisfaction with the level of service REV provided</p> <ul style="list-style-type: none"> ▪ There was a high level of user satisfaction with the level of service that REV provided, with 86% of survey respondents being <i>satisfied</i> or <i>very satisfied</i> with the level of service, and with 79% of respondents being <i>very satisfied</i>. ▪ The levels of satisfaction in Iraq were significant lower than at the other locations, with only 78% of respondents being <i>satisfied</i> or <i>very satisfied</i> with the level of service provided, possibly because of lack of access to information about candidates and parties. ▪ Only 3.6% of respondents indicated that were not willing to use REV again, and a quarter of these said that was because they would be back in Australia at the next election. ▪ Lack of privacy in casting their vote, speed of logging on and casting their vote, and lack of knowledge of the candidates and party preferences were the main reasons nominated by the 11 respondents (out of 316) who were <i>dissatisfied</i> or <i>very dissatisfied</i> with the level of service REV provided. 	
<p>Opportunity to vote electronically</p> <ul style="list-style-type: none"> ▪ 91% of respondents considered the opportunity to vote electronically as <i>(very) good</i>, with 70% considering the opportunity to be <i>very good</i>. There was only marginal variation on this aspect across locations. 	

Key Findings	In any future implementation of REV, the following considerations are recommended:
<p>Clarity of the instruction pamphlet</p> <ul style="list-style-type: none"> 86% of respondents considered the clarity of the instruction pamphlet as <i>(very) good</i>, with 50% considering the clarity to be <i>very good</i>. There was slightly lower ratings of these aspects in Iraq and Afghanistan, because of a greater proportion of those were <i>neutral</i> in their ratings, but no indications of why this may be the case. 	
<p>Clarity of on-screen instructions</p> <ul style="list-style-type: none"> 89% of respondents considered the clarity of the instruction pamphlet as <i>(very) good</i>, with 46% considering the clarity to be <i>very good</i>. There was only marginal variation on this aspect across locations. The relatively high level of rating of the clarity of on-screen instructions, may have been responsible for the lower than average level of invalid REV votes cast – 3.4% compared 4.0% overall for HoR ballot papers, and 1.3% compared with 2.6% overall for Senate ballot papers. 	
<p>Ability to cast a vote in private</p> <ul style="list-style-type: none"> 84% of respondents considered their ability to cast a vote in private as <i>(very) good</i>, with 55% considering privacy to be <i>very good</i>. Most of those who rated privacy as <i>(very) poor</i> were deployed in Afghanistan and in Timor-Leste, with this view formed because the terminals were reported to be located in busy offices or open spaces. 	<p>i) Defence specifically reinforce with base and camp commanders the need to facilitate privacy in casting a vote;</p>

Key Findings	In any future implementation of REV, the following considerations are recommended:
<p>Speed that voters were able to log on and cast their vote</p> <ul style="list-style-type: none"> ▪ 62% of respondents considered the speed with which they were able to log on and cast their vote as <i>(very) good</i>, with 36% considering the clarity to be <i>very good</i>. There was a relatively high proportion of those rating the speed as <i>(very) poor</i> in the Solomon Islands and Afghanistan. ▪ The speed of the DRN was overall very good, with an average of 8.6 minutes taken to vote, once the voter had logged on but, as there were reported variation in the speed, voter expectations may not have been met uniformly. This includes the time it took to read the instructions and complete the detail. 	<p>j) Provide advice to REV registrations that the DRN may vary in terms of the speed with which they can cast their vote;</p>
<p>Vote checking service</p> <ul style="list-style-type: none"> ▪ Only 16% of voters checked their votes. 85% of these rated its ease of use as <i>(very) good</i>, and 76% of these rated its value as <i>(very) good</i>. ▪ The ability to check votes was clearly very valued by those who had rated it as <i>(very) good</i>. 	<p>k) the AEC maintain the vote checking facility as a feature of REV.</p>
<p>3.5 Exercise by Discretion by REV voters</p> <ul style="list-style-type: none"> ▪ While 3.2% of voters voted below-the-line (BTL) on the Senate ballot paper in the 2004 Federal Election, 5.2% of REV voters voted BTL in the 2007 Federal Election. ▪ BTL voting varies across locations with the rating of the speed of logging on casting a vote – that is, in locations with more respondents reporting poor DRN speeds, the rate of BTL voting is lower. 	

Key Findings	In any future implementation of REV, the following considerations are recommended:
<ul style="list-style-type: none"> ▪ A few respondents indicated that they wanted access to how-to-vote and candidate information. 	l) provide candidates and registered parties with feedback from the REV trial on voters' seeking information on local candidates and how-to-vote;
<ul style="list-style-type: none"> ▪ A few respondents indicated that they wanted information on party abbreviations on the ballot paper and how their preferences would be distributed. 	m) the AEC draw REV registrants' attention to its web-site information on GVT and nomination information on candidates.
<p>3.6 Cost of the Trial</p> <ul style="list-style-type: none"> ▪ The cost per REV vote cast was \$521. Forecasting of any future implementation of the trial at the next election, is contingent on Government's decisions in this regard including the scope, but is likely to cost less per vote to implement, provided the number of electors eligible to vote using REV does not decrease. 	
<p>4. Compliance with Legislation</p> <ul style="list-style-type: none"> ▪ Most of the sections and regulations relating to REV for ADF personnel deployed overseas were fully complied with. ▪ Based on the survey of REV respondents, in Afghanistan and Timor-Leste, not all REV voters considered that they had privacy in casting their vote. Commanding officers were reminded of their obligations to ensure privacy in voting. Ensuring that DRN terminals were placed in a way that promoted privacy, was not in the direct control of the AEC. If REV voting was extended in the future, the need to facilitate privacy should be reinforced with commanders (see Recommendation (i)). 	

Key Findings	In any future implementation of REV, the following considerations are recommended:
<ul style="list-style-type: none"> ▪ It is estimated that approximately 45 REV registered ADF personnel may have returned to Australia prior to polling day – there was a risk that these REV registrants may have voted on the DRN in Australia, but no evidence that this occurred. A previous recommendation (Recommendation (d)) suggesting that the AEC investigate ways to exclude those who return to Australia earlier than that specified on their REV registration, from casting a REV vote when in Australia (if not eligible to do so in a future implementation), could minimise this risk in any future implementation of REV. 	
<p>5.1 Procedures to manage the risks of Electoral Offences</p> <ul style="list-style-type: none"> ▪ The AEC put in place a range of controls to minimise the risks of electoral offences associated with the REV system and their use. These were subject to an independent audit with a satisfactory outcome. ▪ The AEC put in place methods to ensure that only the REV vote was counted even if the person voted using both REV and GPV. 	
<ul style="list-style-type: none"> ▪ One DRO, in receipt of two post pack bags of REV votes claimed not to have received the list of voters with GPV certificates attached. ▪ 1.9% of REV voters also cast a GPV vote. 	<ul style="list-style-type: none"> n) include a copy of voter lists with GPV certificates in each bag of REV votes dispatched from National Office to DROs, with second or subsequent copies clearly marked “duplicate” or “copy only”; o) emphasise to REV voters that casting a vote using the REV excludes them from casting a vote any other way,

Key Findings	In any future implementation of REV, the following considerations are recommended:
	and so they should discard any GPV that arrives;
<ul style="list-style-type: none"> ▪ The risk of substitution of votes during transportation of votes between National Office and the DOs was managed through the use of tamper-evident packaging. The use of watermarked paper on which vote is printed was suggested as a further risk management aid. 	p) use watermarked or other security paper for printing record of votes;
<ul style="list-style-type: none"> ▪ The colour and size of the printed votes made it difficult to distinguish between HoR and Senate ballot papers, and increased the risk of not including the print-out in the count. 	q) use different colour paper for HoR and Senate printed votes.
<p>5.2 Allegations of Electoral Fraud arising from the REV Trial</p> <p>There have been no allegations of electoral fraud arising from the trial nor have there been any complaints related to the REV trial.</p>	