

# Administration of the 2011 NSW election and related matters

**Organisation:** Everyone Counts Pty Ltd

**Name:** Mr Mark Radcliffe

**Date Received:** 17/02/2012

# EVERYONE COUNTS SUBMISSION TO THE INQUIRY INTO THE ADMINISTRATION OF THE 2011 NSW ELECTION

Everyone Counts was selected by NSW Election Commission to supply the core software that enabled iVote for the NSW General Election and was used again more recently for the Clarence By-election in November 2011.

In regards to iVote, Everyone Counts fully supports the ***Report on the Conduct of the NSW State Election 2011*** prepared by NSW Electoral Commission and this submission is made solely to address certain public criticisms of iVote that were made at the hearings of the ***Inquiry into the Conduct of the 2010 Victorian State Election*** and in submissions to the ***Inquiry into the conduct of the 2010 Federal Election***.

We assume that these criticisms raised by members of the Computing Research and Education Association of Australasia (CORE) will also be submitted to this inquiry since it is the appropriate forum, however, for completeness, our submission includes the relevant extracts from the CORE statements to the Federal and Victorian inquiries. In particular, there were statements made by CORE and its members that were incorrect and as such we would like to ensure this inquiry is able to make an informed view of iVote based on comment from a range of sources.

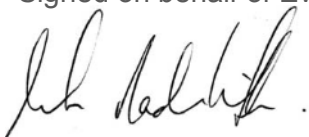
**This submission is made by Everyone Counts Pty Ltd**

PO Box 120, CARLTON NORTH  
VIC 3054

ABN 27 097 697 777

A subsidiary company of Everyone Counts, Inc. of San Diego, California.

Signed on behalf of Everyone Counts Pty Ltd

A handwritten signature in black ink, appearing to read 'Mark Radcliffe', with a period at the end.

Mark Radcliffe  
Business Development Manager (International Sales)

## **Statement made by Dr V. Teague (representing CORE) at the 23 August 2011 hearing of the Inquiry into the conduct of the 2010 Victorian state election and Everyone Counts' Response**

*"I know that you have received a lot of submissions very much in favour of trying to adopt a system something like iVote. I feel that there were serious problems with the iVote project, both in terms of the process, which was not at all transparent and gave very little opportunity for local scrutiny, and in terms of the technical properties of the system itself, at least as far as I could work them out, which was not very far.*

*The New South Wales Electoral Commission recently published some summary reports of the security audits that they had had done on the system, and the security auditors raised some quite serious concerns. In the pre-implementation report — so before voting — they said:*

*... significant security vulnerabilities were highlighted ...*

*In their post-implementation report, which they submitted after the voting period, they said:*

*... some of the risks identified ... remained outstanding during the voting period ...*

*It goes on to say that 43 of the iVote ballots were recorded as having the letter 'N' instead of numeric preferences.*

*From that much information, at least, it appears this is a system that is known to have had significant outstanding security vulnerabilities during the voting period. It is known to have garbled at least 43 votes, and yet it has been variously described by the media and by the New South Wales EC and all kinds of other people as being secure, private and verifiable. It has been trusted for, as far as I know, the uncontested reporting of nearly 47 000 votes. I feel strongly that we should not be emulating this kind of a process."*

### **Everyone Counts' Response**

Everyone Counts will not respond directly to the concerns expressed by Dr Teague regarding transparency as this issue is a matter for our client, the NSW Electoral Commission (NSWEC). However it is worth noting that Everyone Counts strongly supports transparency in elections and as an example of this; the source code to iVote was offered through NSWEC to a member of CORE for review. It should also be noted that the level of documentation provided by NSW Electoral Commission was greater than many of the elections in which our firm has been previously involved.

We would like to make the following observations in regards to Dr Teague's comments about "vulnerabilities" being found during the pre-implementation system security review:

- Firstly, this type of review is typical for an implementation like this as the client needs to be confident that the vendor's voting system has been securely implemented on the client supplied infrastructure. As such it is not unusual for the reviewer to find issues for which they correctly recommend changes to either the configuration of the infrastructure or the voting system. As a result of the iVote security reviews, Everyone Counts made some small software changes at the request of NSWEC and NSWEC also made some changes to their infrastructure.
- It is also important to note that the security reviews were done on Everyone Counts iVote system as installed on the NSW Electoral Commission infrastructure. Therefore the security reviews were in part to ensure that the total combined system was secure, the review was not just about the iVote software.
- It should also be noted that as a normal outcome of a security review of the nature undertaken for the iVote project, additional risks will be raised by the reviewer, which after rational

assessment by the client and voting system vendor, are deemed in terms of consequence and likelihood to be insignificant. It is also normal for such risks to be dealt with by a mitigation approach which, although not eliminating the risk, would mitigate the overall threat to a level where the risks are deemed acceptable. We are aware that NSWEC undertook a very extensive and risk assessment which was carefully reviewed as part of their go-live decision.

In regard to the issue of 43 iVote ballots having a preference mark “N” or similar instead of an acceptable preference mark we would like to make the following comments.

- All 43 ballots with preference mark “N” were captured by the iVote system exactly as displayed when the voter submitted their ballot. That is to say the elector was shown the ballot prior to submission with the “N” characters displayed and also with a warning message that it was an informal ballot and would not be counted, the elector ignored the warning and clicked ‘submit’ to complete their vote. This means the system faithfully captured the vote as cast. It should also be noted that it was always possible for the voter to return to the beginning of the ballot and re-enter their preferences correctly before clicking ‘submit’.
- Notwithstanding the above comment, Everyone Counts acknowledges the iVote software allowed, in certain very limited circumstances (typically when voting over a very poor internet connection), the voter to generate a ballot for submission which was not as they may have originally intended. Everyone Counts in conjunction with the NSW Electoral Commission has now made minor changes to the iVote interface software to prevent this issue occurring again. This change has been used at the Clarence By-election and no problems of this nature were experienced.
- Everyone Counts is also aware from data made publically available by the NSW Electoral Commission, that the rejection rate for iVote ballots was very much lower than the rejection rate for other types of remote voting such as postal votes.

## **Statements made in the CORE Submission to the Inquiry into the 2010 Federal Election and Everyone Counts’ Response**

### **Statement from CORE**

*“The recent trend at both state and federal level to entrust electronic voting to secretive private vendors is not consistent with the degree of transparency we expect for Australian elections. Whether the integrity or privacy of the systems meets our expectations is unclear because we have no details about them. For example the NSW iVote project has been carried out in a clandestine manner. Neither the iVote system nor any associated documentation has been made available for scrutiny by e-voting experts and the public. The NSW Electoral Commission intends to release only the auditor’s final report, but on its own this will provide little if any evidence of iVote’s security.”*

### **Everyone Counts’ Response**

The implied characterisation of Everyone Counts as “secretive” is unfounded and strongly rejected by our firm.

It is also our view that the audit and reviews undertaken by the NSWEC during the iVote project were rigorous and in excess of many of the client projects we have been involved with in the past. The “warts and all” level of openness that was clearly displayed in the review documentation

published by NSWEC also shows the highly contentious statement that “*the NSW iVote project has been carried out in a clandestine manner*” to be without foundation.

Whether CORE is an appropriate body to adjudicate on the integrity and privacy of electronic voting in Australia is not a decision for Everyone Counts, but we certainly support transparency in elections and encourage our clients to maintain election transparency when introducing electronic voting. We would work with any competent organisation our client nominated to undertake a review of our system.

### **Statement from CORE**

*“The NSW iVote system used weak authentication comprising an 8 digit user ID number and a short 6 digit PIN. This very low standard is not even acceptable for Internet banking. Banks in Australia typically require longer (and hence stronger) passwords, and many already use security tokens. It is telling that at least one of the submissions to this inquiry advocating federal Internet voting cited the increased convenience of not having to find a witness, as would be required for postal voting (Kennedy, 2011). It is absurd to deploy a less secure voting channel than postal voting and encourage people to use it instead of postal voting by reducing the authentication requirements below what would normally be required for postal voting.*

*In comparison, Internet voting in Estonia uses the strongest form of voter authentication: each individual owns a smart card (and a smart card reader) which contains a private key for which the electoral authorities know the corresponding public key. This provides a technical solution with a high degree of security. It also allows the vote to be digitally signed, which makes it much more difficult to modify undetectably after casting. Although this method would obviously be expensive to roll out to the general population in Australia, it may be feasible to implement for small, specific voter groups who are targeted for Internet voting, such as visually impaired or Antarctic voters. This and other options for strong voter authentication must be considered in order to evaluate the appropriate trade-offs between different costs and different security guarantees.*

*Another issue is authentication of the voting server to the voters, i.e. protecting the voters from being misdirected to a bogus website and hence prevented from casting a real vote.”*

### **Everyone Counts’ Response**

Our software system that ran iVote can support a variety of approaches to voter authentication including smart cards similar to those used in Estonia. The requirement from NSWEC specified the use of 8-digit iVote numbers and a 6-digit PIN, which we understand to be their determination on the compromise between security and useability.

In this regard the project certainly met the expectations of useability and there were also no incidents of this authentication being breached, as no voter contacted the NSWEC saying that their iVote had already been voted when they hadn’t actually voted.

Should NSWEC determine that stronger authentication is appropriate for future use of iVote, this is readily accommodated within the current iVote software.

The final issue raised, of voters being misdirected to a bogus website (“Phishing”), is a common threat on the internet. We are aware that NSWEC took a number of steps to mitigate this including registering URLs similar to iVote.nsw.gov.au and providing many links to electors who registered for iVote and on the NSWEC website and also in print and other media publicising the election. Being within a government domain, it is very difficult to ‘hijack’ the correct domain name for iVote at

nsw.gov.au and also the EV SSL Certificates used by the iVote system provide tamper evidence to any attempts at DNS hijacking (changing internet routing directions).

If any attempts had been made to create a bogus website and direct voters to it, this would have meant many voters receiving fake email trying to direct them to the bogus site and would not have gone undetected.

### **Statement from CORE**

*“There is no justification available to the public as to whether the NSW iVote system adequately protected vote privacy. The system used an ordinary “secure” webpage, so the vote was encrypted by the voter’s computer only in an ephemeral way that was decrypted immediately upon reaching the server. As a result anyone who gained access (authorised or not) to the electoral commission’s systems could potentially have discovered how every iVote user voted. This means that vote privacy was entirely dependent on electoral commission procedures for preventing a person’s iVote ID from being linked to their identity. Details on these procedures are not in the public domain and may never be disclosed, meaning that there is no publicly available evidence that vote privacy was preserved.*

*It is important to note that this vulnerability could have been countered with standard cryptographic techniques that are already employed by many Internet voting systems. Hence the iVote system clearly falls well short of providing what is widely recognised as being the minimum level of vote privacy protection.”*

### **Everyone Counts’ Response**

The statement above refers to the encryption on the voter’s computer as being “only in an ephemeral way”. The encryption referred to here is SSL, which is the commonly used standard for banking and e-commerce sites around the world and, whilst NSWEC may not have specifically published all the details of the systems security, it is our view there were strong cryptographic and procedural protections in place to maintain the privacy of the vote. These included locking out all access to the system as a security measure during voting. The final lock-down only allowed the Electoral Commissioner or iVote Manager, combined with another person, to be able to allow access to the core voting system infrastructure. Additionally, before the encrypted ballots can be decrypted using a quorum of the keys held by a panel of five ‘electoral judges’ appointed by the Commissioner; the encrypted votes are shuffled in a way that they cannot be linked to the voter who cast the ballot.

While some voting systems do encrypt data before transporting and then don’t decrypt until the end, this is not true of all voting systems and there are limitations to the usability for the voter with the client based encryption approach, particularly for a system that allows both phone and web based voting.

### **Statement from CORE**

*“The most difficult part of an Internet voting system to secure is the voter’s client machine. Ordinary PCs are notoriously insecure, and we would have to expect that many voters would cast their vote from a machine infected with malware or (legitimately or not) controlled by another person. If the machine used to cast the vote runs a program other than the intended program, it could submit a vote completely different from the one the voter requested. There would be no obvious way for the*

voter to detect this. A procedure for querying the computer would not prove anything, because a computer running malware could simply respond with a lie to the query, and tell the voter that it had submitted the correct vote when it had actually submitted something different. For example, a recent challenge to the Estonian voting system consisted of demonstrating a program that could present the appearance of a successful voting experience for a particular candidate, while actually casting a vote for a different one (Rikken, 2011). This was not a security vulnerability in the voting software itself, but a response to the inherent vulnerability of an ordinary PC.

<continues with more details>...”

### **Everyone Counts’ Response**

The sort of attack described above is commonly known as a “Man in the browser attack” and it is a generic threat on the internet. Typically, a voter’s PC is infected with a virus (malicious programming code) by the PC user opening attachments from SPAM emails or visiting malicious web-sites. There are many protections against this in the form of anti-virus and firewall software, with most PCs being delivered with such software and many good anti-virus/firewall packages being available free of charge on the internet.

However, there are electors who’s PC will have one of the many viruses ‘out in the wild’ due to poor usage and maintenance of their PC. No virus has yet been found ‘in the wild’ that is designed to corrupt electronic voting on a PC. Also, should someone write such a virus to try to corrupt electronic voting in NSW, the virus would have to be specifically written with knowledge of the particular election and therefore would have to be deployed within a very short timeframe.

It is worth noting that the Estonian example is misquoted by CORE in that the Estonian university student, who was the subject of the article by Rikken, did not demonstrate a program that could present the appearance of a successful voting experience for a particular candidate, while actually casting a vote for a different one. The student merely raised the hypothetical possibility of this occurring.

A statistical analysis of this hypothetical attack would show that in the short time from when the candidates were known for an election to the close of voting, an attacker would have to create a virus that undetectably infected sufficient PCs to impact the result of the election. Given that a virus infects a computer through the action of the user and cannot be set to infect just computers within a close seat in NSW; even for a close election it would need to infect far more PCs than any of the most rampant computer viruses ever known.

Of course any elector concerned about the security of their PC had the option of using iVote by Phone, which was not subject to this attack, and could also resort to the voting methods they used prior to the introduction of iVote.

In discussions with the Electoral Commission this issue has been likened to the perception of some people that multiple voting in polling places could occur on a massive scale with paper-based mark-off in polling places on polling day.

Notwithstanding the improbability of the “Man in the browser attack”, Everyone Counts recognises the need to allay elector perceptions and consequently; Everyone Counts and NSWEC are discussing potential methods to further eliminate this hypothetical threat from future elections through the use of end to end verifiable voting.



## **Statement from CORE**

*“One serious problem that occurred both in NSW and Victoria’s electronic voting solutions was that a system originally designed and justified on the grounds of giving an independent vote to visually impaired people was later expanded to a much larger population of voters without being redesigned appropriately. In the case of Victoria...”*

*“Similarly, the iVote system in NSW was originally promoted as being for a restricted set of voters and only much later expanded to include a much larger number of overseas and interstate voters, many of whom would have been perfectly capable of completing an early vote or a postal vote. The tradeoffs of security for convenience for this group are completely different from the tradeoffs for the visually impaired, and the implications of security vulnerabilities in the taking of nearly 50000 votes are considerably more serious than in the case of only the few thousand originally expected.”*

## **Everyone Counts’ Response**

Whilst iVote accepted nearly 50,000 votes rather than the 5,000 to 15,000 that was originally expected in the feasibility study, from Everyone Counts’ perspective the security and design of the software were appropriate for 10,000 or 100,000 votes and we are not aware of any significant changes NSWEC would have made knowing they would receive nearly 50,000 votes, other than to increase call-centre staffing.

It should be noted that the addition of interstate and overseas voters was made as an amendment in the house by the then opposition and we understand this was done to address concerns regarding known problems interstate and overseas electors have had voting.

We would also understand that the comment that many of the overseas and interstate users of iVote “would have been perfectly capable of completing an early vote or a postal vote” is incorrect and shows a lack of knowledge of the real issues these voters face. We also note that NSWEC has estimated that at least 20,000 interstate and overseas were enfranchised by iVote. That is these voters would not otherwise have voted had iVote not been available.

## **Statements made in the CORE Supplementary Submission to the Inquiry into the 2010 Federal Election: Best Practices for E-election Systems and Everyone Counts’ Response**

### **Statement from CORE**

*“Rigorous audits conducted by independent experts are also integral to assuring the high quality of e-election systems. Audits for mission critical systems require substantial time, resources and expertise to evaluate both the systems and the development processes.*

*However in many instances the auditing process is not given sufficient care and attention. ... In the case of the NSW iVote system, the feasibility study originally scheduled less than eight days in total for conducting the audit and addressing the findings, with the voting period commencing ten days later (NSWEC, 2010). This was despite the fact that iVote was claimed by the vendor as being “[a]rguably the world’s most far reaching and advanced remote voting solution ever to be offered for a government election” (Everyone Counts, 2011b).*

*It would be unreasonable to expect that major flaws with such a complex system could be discovered and fixed in such a short time frame, and undoubtedly this would place the auditor under*



*enormous pressure not to find problems. Moreover had there been adverse findings, the NSW Electoral Commission would have been conflicted in deciding whether to proceed with using a highly vulnerable system in a mission critical environment, or to abandon the system and potentially disfranchise 50000 voters who planned to use iVote (note that voter registration for iVote was scheduled to open two weeks before the audit was due to be completed)."*

### **Everyone Counts' Response**

Rigorous audits are indeed integral to assuring the quality of electronic voting projects and we are aware of PricewaterhouseCoopers (PwC), the auditor engaged by NSWEC, commencing their audit work in January 2011 and continuing to work with the iVote project throughout the remainder of the project until well after the election was completed.

As part of the audit process, we are aware that NSWEC engaged various technical specialists to support the audit in regards to a review and control of the source code; review of the cryptography within the system; and penetration testing of the system and the infrastructure upon which it was running.

The audit stream of work did recommend some changes and there was adequate time for appropriate changes to be made.

It is Everyone Counts' view that the audit process proceeded in an orderly manner and was more robust than many processes we have worked with in projects of a similar nature.

### **Statement from CORE**

*"In addition it is common for auditors to lack the necessary expertise and experience.*

*For instance the ACT e-counting system was certified by an independent auditor but still had defects that caused failures during an election. Also the auditor failed to identify other defects that could cause incorrect election results and system crashes. These were elementary bugs that could have been detected using standard testing methods and very simple test cases. The defects were later discovered by researchers from the Australian National University (Goré, 2004).*

*Knowledge and expertise is notably lacking in current security audits, which frequently overlook many of the threats and vulnerabilities that are unique to e-election systems. E-voting security expert Doug Jones suggests that "many of today's security professionals have focused so much on conventional data processing applications using Microsoft Windows in a corporate setting that they are very poorly adapted to examining the security of novel applications outside the Windows domain or outside the commercial data processing domain" (Jones, 2004).*

*As an example the remote voting system for the ADF trial in the 2007 Federal Election had potential security and vote privacy vulnerabilities that were not considered by the auditor (CORE, 2008). Furthermore this had long term consequences extending beyond the ADF trial as NSW later used the same vendor and core system for its iVote project. If the ADF audit had identified the fundamental flaws with the system, then it seems likely that NSW would have chosen a superior system for iVote."*

### **Everyone Counts' Response**

It is our view that NSWEC ensured that appropriate expertise was available for the audit of iVote. We noted that the audit firm of PricewaterhouseCoopers was supported by a specialist company reviewing our source code; another specialist security firm performing penetration testing and a third firm that specialises in cryptography reviewed the cryptography within the iVote system.

The reference to “fundamental flaws” relates to Dr Teague’s assessment of the audit report of eLect usage in 2007 for the AEC’s ADF trial. This assessment appears mostly to be assumptions based on what the audit report did not say. Since NSWEC already had access to these CORE submissions, as well as access to AEC people and documents from the ADF trial, at the time they selected Everyone Counts’ eLect system for iVote; we believe NSWEC was fully informed of these issues and as such satisfied themselves these issues, real or otherwise, were of no material importance for the iVote 2011 project.

### **Statement from CORE**

*“For example it has become the norm for new e-election systems to be developed on a tight schedule and then to be deployed at the most crucial point of the electoral cycle. Given that this leaves little margin for error and that IT projects have the propensity to be delayed, there is a large risk of compromising the quality of these systems. This was the case with the NSW iVote project, where development started only six months before the election. The Internet voting system ended up omitting core functionality such as providing audio instructions for visually impaired voters.”*

### **Everyone Counts’ Response**

This statement is factually incorrect in that:

- Whilst the contract with NSWEC was signed about 8 months prior to the election, the eLect software platform on which iVote is based has been in development for 13 years.
- We have had successful implementations shorter than the 8 month implementation project for iVote and the timeframe was considered more than adequate.
- The internet voting did not omit any specified or core functionality. (Visually impaired users on the internet would be using screen-readers to provide audio or screen-magnifiers. NSWEC recorded audio instructions were only ever intended to be part of telephone voting.)

### **Statement from CORE**

*“Furthermore sudden changes to a system can drastically alter the risk profile. For instance the NSW iVote system was originally restricted to a small group of voters but was later expanded to include interstate and overseas voters. As a result of this major change in scope almost 50000 votes were cast over the Internet, which was ten times the number anticipated and posed substantially greater risks. Even in one of the largest landslide elections in Australian history, this could still have had potentially devastating impacts in affecting important outcomes, most notably the result in the tightly contested seat of Balmain. In much closer elections such as the 2010 Federal Election, similar scope changes could have implications for the integrity of overall election results.*

*Therefore careful and continual risk assessments that emphasise election quality must form the basis for all decisions about commissioning the development of new e-election systems, or upgrades and modifications to existing systems including their intended usage. These assessments need to follow best practice for e-election systems and exceed standards such as AS/NZS ISO 27001 (Information Security Management Systems), which only specify minimum acceptable practice for general IT systems.”*

## **Everyone Counts' Response**

We agree that “careful and continual risk assessments that emphasise election quality must form the basis for all decisions” and in our business we do make careful and continual risk assessments. To the extent that we are aware, NSWEC also made careful and continual risk assessments to ensure the quality of the iVote part of the election.

## **Statement from CORE**

*“A common argument for concealing source code and other system details is that “security through obscurity” is needed to ensure the security of e-election systems. But this is widely recognised by security experts as misguided (Mercuri and Neumann, 2003).*

*In contrast widespread analysis of source code increases the likelihood of identifying and rectifying vulnerabilities. Indeed some vendors incorporate open source software components into their systems and are enthusiastic in promoting the benefits. The NSW iVote vendor is one example (Everyone Counts, 2011a), though their commitment to open source software did not extend to openness of the iVote source code.”*

## **Everyone Counts' Response**

The openness of the iVote source code is a complex issue as Dr Teague notes in her testimony to the Inquiry into the conduct of the 2010 Victorian state election: *“And the source code, yes. This is a very vexed issue, and not just to me. This issue is being batted back and forwards throughout North America and Europe and everywhere else.”*

The challenge with true open source is that while widespread analysis of source code increases the likelihood of identifying vulnerabilities, the ability to rectify those vulnerabilities relies on them being reported to the Electoral Commission rather than being exploited or kept secret by the discoverer. Many, if not most of the world's most security sensitive and secure applications are not open source.

Our policy is to disclose the source code to any client or to third-parties that our client (NSWEC in this case) wishes to review the software source code for them.

It should be noted, Everyone Counts, through NSWEC, has offered the iVote source code to a member of CORE for review. At this time the offer has not been taken up.

**Appendix: CORE submissions to date** (prior to Feb 2012 and the NSW JSCEM Inquiry):

1. 2011 Submission to Victorian JSCEM – Inquiry into 2010 Victorian election  
[www.parliament.vic.gov.au/images/stories/committees/emc/2010\\_Election/submissions/13\\_VTeague EMC Inquiry No.6.pdf](http://www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/submissions/13_VTeague EMC Inquiry No.6.pdf)
  - a. SCYTL response - [www.vec.vic.gov.au/files/EAV-Scytl-CORE-Report.pdf](http://www.vec.vic.gov.au/files/EAV-Scytl-CORE-Report.pdf)
  - b. Transcript of hearing -  
[www.parliament.vic.gov.au/images/stories/committees/emc/2010\\_Election/Corrected\\_Evidence\\_2010\\_Vic\\_State\\_Election\\_23\\_August.pdf](http://www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/Corrected_Evidence_2010_Vic_State_Election_23_August.pdf) (from page 34)
2. 2011 Submission to Federal JSCEM – Inquiry into 2010 Federal election  
[www.aph.gov.au/house/committee/em/elect10/subs/Sub101.pdf](http://www.aph.gov.au/house/committee/em/elect10/subs/Sub101.pdf)
  - a. Supplementary document on best practices -  
[www.aph.gov.au/house/committee/em/elect10/subs/Sub101.1.pdf](http://www.aph.gov.au/house/committee/em/elect10/subs/Sub101.1.pdf)
3. 2008 Submissions to Federal JSCEM on AEC 2007 trials
  - a. [www.aph.gov.au/house/committee/em/elect07/subs/sub116.pdf](http://www.aph.gov.au/house/committee/em/elect07/subs/sub116.pdf)
  - b. [www.aph.gov.au/house/committee/em/elect07/subs/sub116\\_1.pdf](http://www.aph.gov.au/house/committee/em/elect07/subs/sub116_1.pdf)
  - c. [www.aph.gov.au/house/committee/em/elect07/subs/Sub116\\_2.pdf](http://www.aph.gov.au/house/committee/em/elect07/subs/Sub116_2.pdf)