Submission

No 7

Administration of the 2011 NSW election and related matters

Organisation:	Computing Research and Education Association of Australasia
Name:	Dr Roland Wen
Date Received:	17/02/2012

CORE

Computing Research & Education

CORE Submission to the Inquiry into the Administration of the 2011 NSW Election and Related Matters

Problems with the iVote Internet Voting System

Vanessa Teague[1] Roland Wen[2]

[1] vjteague@unimelb.edu.au
Department of Computer Science and Software Engineering
The University of Melbourne

[2] rolandw@cse.unsw.edu.au
School of Computer Science and Engineering
The University of New South Wales

The Computing Research and Education Association of Australasia (CORE) is an association of university departments of computer science in Australia and New Zealand. This submission has been authorised by the President of CORE. The authors are both Computer Science and Engineering researchers whose main interest is in electronic voting and security. We have previously made submissions to parliamentary inquiries examining the problems with e-voting and IT systems used in Australian elections. At present we are collaborating with the Victorian Electoral Commission on its e-voting system.

Executive Summary

In the 2011 State Election the NSWEC ran one of the world's most ambitious Internet voting projects with a system called iVote, provided by US vendor Everyone Counts. The main purpose was to enable vision impaired voters to vote without human assistance, but the project was extended to any voter who was outside NSW on election day. This excellent opportunity to use technology to improve the voting experience for voters with disabilities is an important part of modern electoral reform.

However, widespread Internet voting is extremely difficult to secure and scrutinise. Many security experts believe that it cannot be trusted for public elections [IAVOSS07; VV08]. In this submission we explain the problems with iVote and identify measures that need to be taken to ensure that future Internet voting systems provide stronger protection of voter rights. We aim to maintain the quality and trustworthiness of NSW elections, and ensure that Internet voting is offered only when it does not reduce vote security, vote secrecy or voter independence.

The iVote system had significant security vulnerabilities and reliability failures, one of which is known to have misrecorded votes. The system also experienced failures in authenticating eligible voters. Although the system protected votes in transit across the Internet, there is not enough publicly available information to establish whether vote privacy and anonymity were adequately protected at the Electoral Commission. iVote also had reduced safeguards against general IT security vulnerabilities because the part of the system intended to detect external hacking was "not implemented as per design" [PWC11a]. Although there are well-known measures to mitigate many of these problems, the iVote system does not contain such countermeasures in the design.

Moreover it is evident that poor practice was employed in implementing iVote, which resulted in defects (and likely vulnerabilities) being introduced but not being identified until too late. The audit and evaluation processes were given inadequate time and attention, which means that iVote may have experienced incidents during the election beyond those which were known and reported by the auditor or by the NSWEC. The security audit commissioned by the NSWEC in advance of deployment [PWC11b] found that

> *"Significant security vulnerabilities were highlighted."*

A summary report from PWC after the election [PWC11a] stated,

> *"some of the risks identified by third party security experts and NSWEC remained outstanding during the voting period."*

It is of grave concern that the project went ahead despite known outstanding security vulnerabilities. There is no further public information on the nature of the vulnerabilities so we do not know what the effects may have been. A security vulnerability in a voting system could possibly represent an opportunity for someone to vote fraudulently, expose the votes of others, or manipulate the results of the election.

Another serious concern is the poor transparency of the iVote system and related processes. Minimal information has been released about the system itself, the audit and evaluation processes, and the incidents that occurred during the election. This prevents experts, voters and the Parliament from accurately evaluating the iVote project's shortcomings and understanding the implications for the integrity of NSW State Elections.

Some vulnerabilities are inherent to Internet voting and cannot be fixed with current technology. Many other problems can be attributed to shortcomings in the governance of the iVote project. The NSW Parliament initially legislated for a modest Internet voting project with a small number of eligible users, mostly vision impaired. Late in the project, the scope was enormously expanded to include anyone absent from NSW on polling day. There was inadequate planning to establish and enforce strong security, reliability and transparency requirements, in line with international standards. Much of the legislation attempting to establish these things is either vague or misguided.

Furthermore, there was insufficient expertise and resources at NSWEC to provide rigorous oversight and strong accountability of the third parties responsible for designing, developing and evaluating iVote. For example, like other systems from Everyone Counts, iVote provided each voter with a "receipt value" after voting. The NSWEC's website incorrectly stated during the NSW State election that the receipt value "confirms there has been no tampering to the vote", though this was replaced with a more accurate and much weaker claim for the Clarence by-election.

Our main recommendations are listed here, then explained in more detail later in our submission.

Recommendations

Recommendation 1. ***Internet voting should be offered only to those voters whose vote security, secrecy and independence it does not reduce.***

This may include vision impaired voters but does not include those who could independently and successfully use paper-based voting.

See Section 2.

Recommendation 2. ***The principles of transparency and openness to scrutiny that already apply to other forms of voting must apply just as strongly to electronic voting. Achieving the same standard of transparency as traditional voting methods requires planning and support for openness to counter the inherently non-transparent nature of IT systems.***

This means that as much as possible of the system's technical details (including source code) and documentation (including documentation on the development processes and reports on the audit and evaluation) must be available to scrutineers, security experts and the public. This level of transparency should be an enforced condition of the initial tender and contract.

See Section 4.

Recommendation 3. ***A voting system should, as much as possible, provide evidence to voters that their votes are cast as they intended and properly included, and evidence to scrutineers and observers that all votes are properly***

printed or properly electronically tallied. This strong verification mechanism should be publicly explained and its limitations clearly stated.

At the very least, a system should not be advertised as providing this evidence when it does not.

See Section 2.2.

Recommendation 4. ***Vote secrecy (privacy and anonymity) should be protected as effectively as possible and its limitations clearly stated.***

This includes secrecy from other people using the same computer, outside attackers on the Internet, and inside attackers who are employees of the NSWEC or its partners.

See Section 2.4.

Recommendation 5. ***Election IT systems must be developed using best practices for failure-critical systems rather than standard practices for commercial IT systems.***

1. *The systems must have comprehensive and ongoing risk assessments.*
2. *The development process must use rigorous, well-established software engineering practices that are specifically designed for failure-critical systems.*
3. *The development process must produce comprehensive and objective evidence that the systems are secure and reliable.*
4. *Electoral commissions must be given the necessary resources, support and expertise to establish, implement and manage best practice election IT systems development.*

Recommendation 6. ***Election IT systems and the development processes employed must undergo rigorous, ongoing audits conducted by a range of independent experts with extensive knowledge and experience covering areas including cryptography, security, software engineering, failure-critical systems and election technology.***

There should be ample time for all audit recommendations to be properly implemented and for the system to be re-evaluated.

Recommendation 7. ***There should be a far-reaching, in depth and public review of the iVote project and the NSWEC's approach to procuring and evaluating IT systems in general.***

This review should cover:

1. *how widely Internet voting should be offered,*
2. *the security and transparency requirements for election IT systems and how the project will satisfy them,*
3. *the governance, procurement and evaluation of IT systems,*

4. *what external oversight must be provided.*

The review recommendations must be implemented well before any future Internet voting system is used or procured.

Contents

1 Introduction and Background on iVote

For many voters with vision or motor disabilities, iVote represented their first opportunity to vote without the explicit help of another person. Providing independent voting options for disabled voters is important. Equally important is that these voters are provided with the best possible technology to protect the secrecy and integrity of their votes, and that they are aware of the limitations so that they can make an informed choice. But there are many serious problems with iVote of which the public has not been made aware.

One of the most prominent messages on the website of the iVote vendor, Everyone Counts, is about their success in the NSW State Election. The advertisement reads "Secure, transparent, UNCONTESTED." However the evidence demonstrates that iVote was neither secure nor transparent. If the results had been contested, we do not believe there would have been strong enough evidence that the iVote results were correct.

In this submission we describe these issues with iVote, make recommendations on how to address some of them, and explain which ones are inherent in Internet voting. We examine problems with security and reliability (Section 2), the audit and evaluation process (Section 3), transparency and scrutiny (Section 4), and project governance (Section 5). We also explain in detail the ease with which vote tampering can occur (Section 6).

2 Security and Reliability

The main problem in electronic voting is that a computer may not necessarily be doing what the user thinks it is doing. Although people can watch the screen or listen to audio outputs, they cannot directly observe the actual electronic data being produced, recorded or transferred by the computer. A program that appears to behave correctly could in fact be misrecording votes, exposing their privacy or (in the case of a server) modifying or deleting them. Allowing voters to query the system, or scrutineers to observe it at the electoral commission, does not solve the problem that they cannot actually observe the electronic votes. Errors could be caused by accidental hardware or software errors, by deliberate manipulation from insiders such as programmers or electoral officials, or by external hacking. In any of these cases, there is no reason to suppose that such errors would be detected.

Internet voting is much harder to secure than other online applications such as Internet banking, because of the strong requirements of a secret ballot. With Internet banking, the transactions are not secret from the banks. This enables banks to monitor their clients' transactions and to use this monitoring to detect and deter fraud. Nonetheless incidents of cyber fraud and extensive, large-scale failures frequently occur and are reported in the media. Ultimately confidence in Internet banking arises from the fact that banks provide regular statements that enable users to verify and dispute any incorrect, fraudulent or missing transactions. Such open verification is not possible with secret ballot voting, where each person's vote must remain secret, even from the NSWEC.

The insecurity of a voting system, electronic or otherwise, is a very serious concern. A security vulnerability could represent an opportunity for someone to vote fraudulently, expose the votes of others, or manipulate the results of the election. What amplifies the risk with e-voting is the ease with which electronic data can be maliciously or inadvertently altered on a large scale and in an undetectable manner. Many international security experts believe that Internet voting cannot be adequately secured for public elections [IAVOSS07; VV08].

2.1 Vote Integrity Problems

One of the most serious reported incidents with iVote was that it misrecorded 43 votes [PWC11a]. Voters were instructed that one way to enter their preferences was to navigate to each of their chosen candidates in turn and enter the letter 'N', and that the system would then transform the 'N' into the next numerical preference. This user interface was intended to help prevent voters from casting informal votes, but in this case mishandled these votes so that they did not reflect the way that the voters intended to vote. Indeed, several of the affected votes were determined to be informal and were hence not counted at all. The Electoral Commissioner determined the intent of the remainder of these votes.

To compound the problem, the iVote back end did not have robust input validation and error reporting functions to identify invalid votes and gracefully handle such scenarios. In fact it appears the system simply ignored those misrecorded votes when printing, with no notification. The problem was discovered only when "it was observed that an output file of the votes from the iVote system did not appear to agree with the number of votes actually printed" [PWC11a].

This flaw shows how a single, minor software bug potentially has the power to corrupt votes without being detected by voters. In this case the bug seems to have been detected by the NSWEC only because the votes it produced were invalid. This raises an important question: Suppose the same piece of code had instead malfunctioned in a way that produced valid votes that differed from what the voters requested. How would such a malfunction have been detected? From the information available, it seems that it would not have been. If this is correct then this raises serious concerns about the integrity of the votes recorded by iVote.

2.2 Vote Verifiability Problems

Some Internet voting systems such as Helios [Adi08] give each voter strong evidence that their vote was expressed in the way that they intended and recorded correctly. These verifiable systems enable voters to detect integrity failures such as the misrecorded votes described above. In addition these systems provide scrutineers and observers with a mathematical proof that every recorded vote was accurately printed or electronically tallied. This complete evidence of correctness is sometimes called 'strong verification' or 'end-to-end verifiability'. Although these systems do not defend perfectly against all vulnerabilities, and do not scale efficiently to large numbers of voters, they do demonstrate that small-scale Internet elections can provide good evidence of their correctness.

An independent report for the NSWEC advised that "NSWEC should define a strong verification solution from vendors, some of whom have not made use of more modern techniques for REV [Remote Electronic Voting]" [NB09]. However, although iVote issued voters with a receipt number for the ostensible purpose of allowing them to later "verify" their vote, these receipt numbers provide no meaningful verifiability.

iVote's Approved Procedures [NSWEC11d, 4.8.2(3)] reads: "When the voter's iVote is decrypted, it will reproduce the same receipt number that confirms there has been no tampering to the vote." In fact if the vote was tampered with at the voter's PC or modified in transit then both the initial and the decrypted vote would automatically have the same (incorrect) receipt number, which the voter would have no way of distinguishing from the correct one. If the server was hacked or manipulated, it too could send the voter an incorrect initial receipt number, which would subsequently reappear at the "confirmation" step. Either way, the vote could be tampered with while the "receipt confirmation" appeared to work perfectly well. Furthermore, this provides no evidence about the correctness of the NSWEC's internal processes after the confirmation step – the receipt says nothing about vote tampering after confirmation but before printing of the vote. Hence we do not believe that iVote satisfied the legislative requirement to "provide for the authentication of the eligible elector's vote"[1].

In particular, the demonstration of vote tampering that we describe under 'Vote Tampering Case Study' below would simply produce two equal receipt numbers that were incorrect but indistinguishable from correct ones. The voter would have no way of noticing.

Although the same verification mechanism was used for the Clarence by-election, the verification claim on NSWEC's website was significantly weaker and made no mention of "confirming that there has been no tampering to the vote" [NSWEC11d], but instead that it "indicates that their vote was included in the final count" [NSWEC11c]. We note with interest that "elector verification of preferences" was among the future enhancements proposed for iVote in a presentation made to the NSW Parliament in November 2011 [NSWEC11a].

Recommendation 3. ***A voting system should, as much as possible, provide evidence to voters that their votes are cast as they intended and properly included, and evidence to scrutineers and observers that all votes are properly printed or properly electronically tallied. This strong verification mechanism should be publicly explained and its limitations clearly stated.***

At the very least, a system should not be advertised as providing this evidence when it does not.

[1] Note on terminology: In some parts of the iVote supporting legislation, for example [NSW12, pt 5 div 12A s 120AC(2)(c)], this requirement is referred to as 'authentication' of the vote. The usual terminology is 'verifiability'. This avoids confusion with the term 'authentication' of a voter, meaning that the voter is genuine and eligible to vote.

2.3 Voter Authentication Problems

iVote experienced a failure in issuing incorrect iVote numbers (containing seven digits instead of eight) to 1026 voters [PWC11a]. These numbers were used to authenticate voters, in conjunction with a PIN. To compound the problem, voters were able to cast votes using these incorrect iVote numbers. Consequently 182 voters who did so were notified that they had to recast their votes. The PWC post implementation report stated that "The iVote system didn't prevent the 7 digit number from being used however this was not discovered during testing and relied on 8 digit iVote numbers being set up correctly" [PWC11a].

Strong authentication in Internet voting systems is critical for preventing ineligible people from voting, and eligible voters from casting more than one vote. As with the vote integrity problem in Section 2.1, this elementary flaw reflects systemic failures in implementation, testing and auditing. An undetected error in the authentication module of the iVote system would have serious implications for the integrity of the election.

2.4 Vote Secrecy Issues

iVote's supporting legislation includes a requirement that iVote must provide "for the secrecy of the eligible elector's vote" [NSW12, pt 5 div 12A s 120AC(2)(d)]. However iVote only provided weak protection. Although the system used encryption to temporarily protect vote privacy over the Internet, it did not use appropriate encryption to protect vote privacy at all times, as Internet voting systems should. As a result an (internal or external) attacker who compromised the server could link every iVote vote with the voter's iVote Number[2].

Vote secrecy then depends entirely on strict procedures at the NSWEC to prevent the possibility of an iVote number from being traced back to the voter's identity. However the authentication problem above strongly suggests that this is in fact possible and was done. The NSWEC was able to identify votes cast using incorrect iVote numbers, and then trace these back to the voters in order to notify them of the problem. In essence this means that it is possible to trace the votes to the voters in a similar fashion to the UK ballot with traceable serial numbers. Such traceability contravenes the anonymity of the secret ballot and was universally rejected by all Australian jurisdictions over 150 years ago.

Some degree of vote traceability is probably unavoidable in Internet voting. However, the system should be designed so that tracing votes requires access to a large number of different data sets on computers administered by different organisations. At the very least the possibility of such tracing should be clearly publicly explained. The sharing of the election's decryption key among several officials is one part of achieving vote privacy [NSWEC11a], but does not address the issue described above.

[2] Technical note: The established method is to use public-key encryption to encrypt the vote on the client side, so that the vote remains private until final decryption after the anonymisation process. Instead iVote only used SSL/TLS encryption to maintain vote privacy in transit, meaning that the vote was no longer private when received by the NSWEC servers.

Recommendation 4. ***Vote secrecy (privacy and anonymity) should be protected as effectively as possible and its limitations clearly stated.***

This includes secrecy from other people using the same computer, outside attackers on the Internet, and inside attackers who are employees of the NSWEC or its partners.

2.5 Vulnerability to Hacking Attacks

In addition to unique election threats, Internet voting systems are also vulnerable to the same general security threats as any other online system. Best of breed Internet voting schemes use strong verifiability and secrecy techniques that offer some degree of protection for the votes even in the event of system breaches. Considering the weak verifiability and secrecy measures used by iVote, it is especially critical to harden iVote's defences against general hacking attacks by outsiders and insiders (possibly third parties working for the NSWEC).

However it appears that iVote did not have appropriate defences against such attacks. For example "The Intrusion Protection System (IPS) was not implemented as per design due to time constraints on the advice of a third party. Mitigation was achieved through alternative alerting systems" [PWC11a]. Although the alternative alerting systems were not explained, they clearly would have provided reduced capabilities at detecting attacks compared to an IPS.

Considering the known security vulnerabilities of iVote, we recommend that its scope be reconsidered.

Recommendation 1. ***Internet voting should be offered only to those voters whose vote security, secrecy and independence it does not reduce.***

This may include vision impaired voters but does not include those who could independently and successfully use paper-based voting.

2.6 Poor Technology and Practices

We have already written that Internet elections are inherently difficult to secure and scrutinise because of the strong requirements of the secret ballot. However, many of the above security and reliability issues with iVote were caused by the use of poor technology and the application of poor engineering practices in developing this technology.

Currently best of breed e-voting technology uses advanced cryptographic techniques to provide strong vote secrecy and verifiability at the same time; some other solutions make a trade-off and provide either one or the other; iVote provided neither. Such fundamental design omissions leave iVote inherently susceptible to a wide range of vulnerabilities that cannot easily be mitigated. Bolt-on remedies tend to be ineffective and complicated.

Many of the reported incidents that occurred were due to elementary errors in the development process. The fact that such defects were introduced but not detected before iVote went live indicates deficient software engineering standards in the implementation, testing and quality control. Indeed the post implementation audit acknowledged that the "compressed timeframe resulted in incomplete documentation, restricted test case formulation and compressed testing activities" [PWC11a]. These provide strong indications that these shortcomings in the development practices are systemic, and so it is likely infeasible to substantially improve the quality of iVote retrospectively.

Note that patching individual defects as they are identified in an intrinsically fragile system is not an adequate solution. Well-established software engineering best practices for failure-critical systems focus on preventing the introduction of bugs, because it is notoriously difficult to detect bugs. Furthermore these best practices include building in graceful fallbacks in the event of failures as part of the software design. Given the absence of system reporting for the 'N' in the ballots problem, this does not appear to have been done for iVote.

Recommendation 5. ***Election IT systems must be developed using best practices for failure-critical systems rather than standard practices for commercial IT systems.***

1. *The systems must have comprehensive and ongoing risk assessments.*
2. *The development process must use rigorous, well-established software engineering practices that are specifically designed for failure-critical systems.*
3. *The development process must produce comprehensive and objective evidence that the systems are secure and reliable.*
4. *Electoral commissions must be given the necessary resources, support and expertise to establish, implement and manage best practice election IT systems development.*

3 Audit and Evaluation

The NSWEC engaged Price Waterhouse Coopers (PWC) to audit the system, and other third parties to perform penetration testing, code reviews and cryptography reviews. Although PWC's overall audit reports have been published on the NSWEC website, none of the other evaluations are public.

There were a number of problems with the iVote audit and evaluation processes. These contributed to the security and reliability issues we discussed above being overlooked or not adequately addressed.

The audit was performed in a short time frame immediately prior to the election. This was despite advice that "the NSWEC should seek to open its REV systems as much as possible and engage concerned IT experts to play a productive role in the system before it goes live. Part of a REV feasibility really needs to include expert scrutiny of the system and its provider at an early enough juncture so that any concerns can be properly addressed" [NB09]. The post implementation audit noted that the short time frame "did restrict the quality and timeliness of documentation available for our review. In addition the project team dispersed shortly after the election resulting in limited availability of key project staff to respond to questions" [PWC11a].

According to the pre implementation audit, the first cycle of security testing took place during February 2011 and found "significant security vulnerabilities where [sic] highlighted in the preliminary Stratsec report" [PWC11b]. The second cycle was scheduled to be performed on 7 March 2011. The post implementation audit stated "In the time prior to 'go live' on 14 March 2011, a number of risks were addressed and security testing re-performed. However some of risks identified by third party security experts and NSWEC remained outstanding during the voting period" [PWC11a].

Neither audit report gives any further detail. We do not know whether the identified vulnerabilities affected the privacy of the votes, the authentication of voters, the integrity of the votes, or something else. We do not know which vulnerabilities were addressed and which ones "remained outstanding during the voting period". We do know that this sort of language is not the norm for security audits, and that fielding a system with known security vulnerabilities could potentially affect the integrity of the election results.

There are also questions over whether the auditor and other parties involved in the evaluation were suitably qualified to assess iVote and understand the risks. Remarkably, despite the incidents that occurred (which were evidently overlooked by the audit) and their own findings of outstanding vulnerabilities, the auditor made an overall positive summary of the integrity of iVote: "During the course of our review nothing came to our attention that would indicate that votes cast via the iVote system were not recorded, extracted and printed accurately" [PWC11a]. Also the auditor seem satisfied that "a report from the system indicated that no tampering had occurred". This runs contrary to the warning from the iVote feasibility study that "An important feature of new REV systems is their ability to demonstrate that, for example, if there were some small anomalies, the system audit trail should be able to convincingly prove the limited scope of any problems. It is not sufficient for the system to "self-check" nor for the system to publish very simple reports showing "all is well" and "no errors". Such self-check reports can be easily produced fraudulently" [NSWEC10].

Recommendation 6. ***Election IT systems and the development processes employed must undergo rigorous, ongoing audits conducted by a range of independent experts with extensive knowledge and experience covering areas including cryptography, security, software engineering, failure-critical systems and election technology.***

There should be ample time for all audit recommendations to be properly implemented and for the system to be re-evaluated.

4 Transparency and Scrutiny

Paid auditors are not a substitute for wider transparency and openness to scrutiny. We would not entrust the scrutiny of paper-based voting to a private auditor and nor should we do so for electronic voting. Strong transparency is vitally important for three main reasons:

1. In a particular election, transparency gives everyone confidence that the announced outcome was correct.

2. In a particular election, transparency enables scrutiny by the public and by candidates who may wish to challenge the outcome in the event of perceived irregularities.

3. In the debate about the use of technology for elections, transparency gives the public the opportunity to have an informed objective debate about the security properties of a particular system and the implications for how widely it should be deployed.

For all these reasons it is disappointing that almost no detailed information about iVote is available to the public or to scrutineers. In particular, we have requested the security audits and been told that these will not be made available. Our request for the 'iVote standard' was similarly rejected. Without open discussion based on accurate information about iVote's security, or even the iVote standard to which the system was expected to conform, there is no firm basis on which the system can be trusted, or on which the Parliament can make an informed decision about whether iVote should be redeployed.

Importantly, there was no opportunity for scrutineers to conduct a meaningful examination of iVote or the processes for its development and evaluation. This may have had consequences in the closely contested seat of Balmain, where the 900 votes cast using iVote were numerous enough to make a difference to the outcome in that seat. It would be interesting to know when information about the insecurity of iVote and the misrecording of 43 votes was conveyed to the candidates or scrutineers. Was it as soon as the information was available to the NSWEC, or only when the reports were published on the NSWEC website months after the election?

This lack of transparency goes against the international consensus about transparency in electronic voting. For example, the Council of Europe's "Guidelines on the transparency of e-enabled elections" state:

"Access to documentation including minutes, certification, testing and audit reports as well as detailed system's documentation explaining in details the operation of the system, is essential for domestic and international observers" [COE10b].

Furthermore the NSWEC's commissioned independent study advised that "The electronic system, then, needs to be provided to the public in a way that matches the openness of the paper system. Indeed, this open approach has already led to better electronic voting schemes: 'Experts and all other interested parties are in fact encouraged to evaluate and criticize the scheme. The intent is to expose any flaws or weaknesses, and subsequently work towards improving the scheme. This is in contrast with the trend of most other poll station electronic voting systems, whose proprietors have claimed that it is necessary to keep the details secret for purposes of securing intellectual property' " [NB09].

Although the iVote vendor, Everyone Counts, touts the benefits of transparency, it does not in fact provide it. The Everyone Counts website previously claimed that its system had an 'Open Code Advantage', meaning that the "programming code is available for review by any interested party" [EC11a]. However our request for the source code was rejected and we were informed that this policy is incorrect. Nevertheless a Security Overview White Paper on its website still declares that, "Everyone Counts uses a completely open software system. All of the computer code handling the ballots is available for audit and inspection by independent reviewers. And we build the whole system on open-source software" [EC11b].

After the Clarence by-election, the NSWEC proposed that we inspect the iVote source code by working under the NSWEC. However Everyone Counts drew up a highly onerous non-disclosure agreement. Amongst other problems, the terms of the agreement would potentially have prevented us from writing this submission (unless we invoked parliamentary privilege), performing our regular research on e-voting, or collaborating with other electoral commissions on their e-voting projects. This is completely contrary to the strong transparency and scrutiny that we expect of elections, and the spirit of openness of the democratic process. Furthermore it is inappropriate for experts to have a confidential role in election system auditing. What is necessary is an open process that allows scrutineers, technical experts and members of the public to learn about and comment on the technical details of the system and the audit findings, well in advance of the election.

Election administrators elsewhere have been able to insist on strong transparency and scrutiny for e-voting systems. For example in 2007 the California Secretary of State commissioned a top-to-bottom review of electronic voting machines [CSOS07]. This was a rigorous and extensive review that gave teams of recognised e-voting security experts full access to the systems. Detailed reports were published and the confidentiality agreements provided explicit protections for the experts involved. Several voting machines were decertified as a result of the findings. More recently Norway implemented an Internet voting system in 2011 that provided full transparency of the system, including source code, technical documentation, project management documentation and even the tenders submitted by the vendors [Nor11].

Closer to home, when the ACTEC published the source code for its EVACS system, researchers from the ANU discovered several bugs, which were fixed as a result [ADG+04]. In the most recent Victorian state election, the Victorian Electoral Commission established a "Technical Observer" role which allowed us to examine their polling-station electronic voting project. We were able to make some concrete recommendations about improving its security, including identifying one notable issue which was patched in time for the election [CORE10]. All the above examples show that strong transparency is good for security.

Recommendation 2. ***The principles of transparency and openness to scrutiny that already apply to other forms of voting must apply just as strongly to electronic voting. Achieving the same standard of transparency as traditional voting methods requires planning and support for openness to counter the inherently non-transparent nature of IT systems.***

This means that as much as possible of the system's technical details (including source code) and documentation (including documentation on the development processes and reports on the audit and evaluation) must be available to scrutineers, security experts and the public. This level of transparency should be an enforced condition of the initial tender and contract.

5 Project Governance

Project governance plays a vital role in the success of critical, large-scale projects such as iVote. This is especially so as IT projects are notorious for failures.

Many of the shortcomings of iVote that we have described are likely due to problems with the governance of the iVote project. There were failings in the project management, the decision making process, ensuring accountability and understanding the risks.

The iVote project did not establish and enforce the necessary requirements for an Internet voting system. Well-known issues with security, transparency, scrutiny and evaluation were not addressed, despite the recommendations in the iVote feasibility study [NSWEC10] and independent report [NB09] commissioned by the NSWEC, as well as international standards and guidelines [COE10a; COE10b; USEAC05].

iVote not only failed to satisfy security requirements, but also usability requirements for vision impaired voters. As with every other e-voting system in Australia developed for vision impaired voters, iVote was supposed to provide audio instructions and recordings of candidate names. However the vendor was unable to fulfil this core requirement.

As we have discussed above, there were serious shortcomings in the audit and evaluation process. There was poor planning in engaging suitably qualified experts to perform the audit, and in scheduling adequate time for the audit. In particular, the registration for iVote commenced on 17 February 2011, several weeks before the audit was completed. Thus in the face of adverse findings, the NSWEC would have faced a very difficult decision between proceeding with using a highly vulnerable and unreliable system in a failure-critical environment, or abandoning the system and potentially disfranchising thousands of voters who expected to use iVote and had not made other arrangements.

The third parties engaged by the NSWEC do not appear to have been held accountable for their failures. Indeed despite systemic issues being identified, iVote was used again for the Clarence by-election. It is also worth noting that the iVote supporting legislation does not require the system to be audited for by-elections.

The governance problems in NSW are not isolated to iVote but appear to extend to other IT projects for elections. In the 2003 NSW State Election the NSWEC's counting software suffered from catastrophic failures. In its submission to the JSCEM inquiry, the NSWEC acknowledged that it had "no resources to be able to confidently manage the implementation of a mission critical IT application. IT advice has been provided through external consultancies" [NSWEO05]. The issues with iVote indicate that the NSWEC has not yet managed to address this problem, and that the external consultants still lack the requisite experience and expertise.

Similar governance failures have had devastating consequences in the Netherlands, which was recently forced to abandon e-voting after decades of use: "the public sector became so dependent on the private sector that a situation evolved where Dutch government lost ownership and control over both the e-voting system and the election process" [Oos10].

By contrast, the Victorian Electoral Commission is currently collaborating with local and international e-voting experts to develop a supervised e-voting system. The project has commenced years before the next election is due (2014) and the system will be genuinely verifiable and have openly published source code. After careful consideration, the VEC has recognised that this is the best way to ensure the system provides strong security guarantees, is highly transparent and undergoes thorough scrutiny. Importantly, this collaboration will also help to ensure in-house expertise and understanding of the system.

Although the NSWEC may be following standard guidelines for IT project governance, this is inadequate given the NSWEC's critical role in preserving democracy. It has built public confidence in manual election procedures over many years. The NSWEC has highlighted the rapid changes associated with the use of IT systems in election administration [NSWEC11b]. In order to ensure that the quality and trustworthiness of elections is maintained, it is essential to carefully examine the broad implications of electronic systems on elections, and how these systems are procured and used.

Recommendation 7. ***There should be a far-reaching, in depth and public review of the iVote project and the NSWEC's approach to procuring and evaluating IT systems in general.***

This review should cover:

1. *how widely Internet voting should be offered,*
2. *the security and transparency requirements for election IT systems and how the project will satisfy them,*
3. *the governance, procurement and evaluation of IT systems,*
4. *what external oversight must be provided.*

The review recommendations must be implemented well before any future Internet voting system is used or procured.

6 Vote Tampering Case Study

When a sighted voter fills out their own postal ballot, they can check for themselves that it reflects their intended vote. Blind or vision impaired voters generally have to trust another person to write out their vote in the way that they request. Everyone who uses postal voting has to place some degree of trust in some parts of the transmission and delivery system, and the extent to which this trust is warranted depends greatly on where they post their vote. It is understandable that many voters and NSWEC officials want to reduce or avoid this dependence on other people or on the postal service in the recording and delivery of votes. However, iVote is also vulnerable to deliberate or accidental misrecording of votes. Indeed, electronic systems are inherently more vulnerable to misrecording of votes because even sighted voters cannot directly observe the electronic vote that is recorded and transmitted on their behalf.

In February 2011 Paavo Pihelgas, an Estonian student, demonstrated a vulnerability of the Estonian Internet voting system to vote tampering by a program running on the voter's machine[3]. The program presented a user interface that looked exactly like the interface of the legitimate voting software, but when the voter entered their preferred vote, the program substituted a different vote. Since the Estonian voting software has no meaningful verification, this was undetectable by the voter.

Exactly the same vulnerability applies to iVote. Indeed, we have produced a demonstration version that looks exactly like the iVote practice website. (We could just as easily have made a version that looks like the real voting website, but wanted to avoid making a tool that could be used to manipulate real votes. We emphasise that producing such a tool would be very straightforward and could be done by an Australian undergraduate student or even a gifted high school student.) In order to exploit this vulnerability, someone would have to install the program on the voter's computer[4].

Although Estonian media coverage focused on propagating the program as a virus or worm, or via long-distance hacking, it would work just as well if installed by less glamorous means. Many people have completely legitimate administrator privileges on machines that others might use to vote. For example, system administrators at workplaces or public libraries, or other family members who use the same computer, could all easily install such a program. The level of expertise required to write the program would not be high, and it would be close to impossible to detect if installed by someone with legitimate access to the voting machine.

We have thus demonstrated that an individual's vote can be tampered with easily and undetectably. It is debatable whether it would be feasible to distribute the attack remotely on a large scale without detection. There are numerous examples of hacking, phishing attacks, worms and viruses that have compromised many thousands of machines, but obviously there is no evidence about the ones that remain undetected. We reiterate that iVote's "receipt" mechanism does nothing to address this vulnerability.

We have shown that the system is manipulable. Ultimately the trade-off between accessibility and manipulability is for the Parliament and NSWEC to decide. There is an argument that for blind voters, the vulnerability is not significantly worse than that which they would have to face when asking someone else to fill out a paper ballot. However, the same argument does not apply to sighted voters who are interstate or overseas—for them, iVote is more susceptible than postal voting to undetectable tampering with the vote.

[3] The story is available online from the Estonian public broadcaster and from the Supreme Court, who dismissed the case on legal rather than technical grounds:
http://news.err.ee/Sci-Tech/ed695579-af05-48ab-8cc0-3085e5f0c56c
http://news.err.ee/politics/bbb598aa-586b-4981-9f7e-88273b5a25c0
http://www.nc.ee/?id=1235

[4] Technical point: for some forms of attack such as phishing, the attacker would also have to install a certificate or certificate authority to subvert the https (SSL or TLS) protocol's identification of the correct server. This would be straightforward for administrators of the PC, but certainly more difficult for remote attackers. Other forms of attack, such as propagating a virus or worm that corrupted the PC or browser, could just as easily bypass the certificate mechanism altogether.

7 Conclusion

There are good reasons that most of the world's other advanced democracies have rejected widespread Internet voting. The serious nature and large number of problems with the iVote system and the overall iVote project highlight these reasons, and demonstrate the need to exercise far greater caution. Internet voting can play an important role in improving the voting experience for voters who genuinely have no other option to cast a secret ballot. However any such system must be managed, designed, developed and scrutinised to the highest possible standard in order to protect these voters and the overall integrity of the democratic process. Importantly, the risks and limitations must be thoroughly assessed and made explicit to the public, in order to promote open and robust discussion, and to enable eligible voters to decide whether to accept the risks or choose another voting option.

References

[ADG+04] Pietro Abate, Jeremy Dawson, Rajeev Goré, Matt Gray, Michael Norrish and Andrew Slater. *Formal Methods Applied To Electronic Voting Systems.* Tech. rep. College of Engineering and Computer Science, The Australian National University, 2004.
URL: http://users.cecs.anu.edu.au/~rpg/EVoting/.

[Adi08] Ben Adida. 'Helios: Web-based Open-Audit Voting'. In: *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA.* Ed. by Paul C. van Oorschot. USENIX Association, 2008, pp. 335–348.

[COE10a] Council of Europe. *Guidelines on certification of e-voting systems.* 2010.
URL: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf.

[COE10b] Council of Europe. *Guidelines on transparency of e-enabled elections.* 2010.
URL: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf.

[CORE10] Computing Research and Education Association of Australasia. *Report on the VEC-Scytl Electronic Voting System for the 2010 Victorian Election.* 2010.
URL: http://www.vec.vic.gov.au/files/EAV-CORE-Report.pdf.

[CSOS07] California Secretary of State. *Top-to-Bottom Review.* 2007.
URL: http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm.

[EC11a] Everyone Counts. *Open Code Advantage*. 2011.
URL: `http://www.webcitation.org/61FD3s3ze`.

[EC11b] Everyone Counts. *Security Overview*. White Paper. 2011.
URL: `http://www.everyonecounts.com/whitepapers/SecurityOverviewEveryoneCounts.pdf`.

[IAVOSS07] International Association for Voting Systems Sciences. *Dagstuhl Accord on Electronic Voting*. 2007.
URL: `http://www.dagstuhlaccord.org/`.

[NB09] Frank Nesci and Craig Burton. *Alternative Voting Methods for Vision Impaired Electors*. New South Wales Electoral Commission, 2009.

[Nor11] Norwegian Ministry of Local Government and Regional Development. *Norway E-vote 2011 Project*. 2011.
URL: `http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html`.

[NSW12] Parliament of New South Wales. *Parliamentary Electorates and Elections Act 1912 (NSW)*. 1912.
URL: `http://www.legislation.nsw.gov.au/maintop/view/inforce/act+41+1912+cd+0+N`.

[NSWEC10] New South Wales Electoral Commission. *Report on the Feasibility of Providing iVote Remote Electronic Voting System*. 2010.
URL: `http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/84498/20100723_NSWEC_iVote_Feasibility_Report_.pdf`.

[NSWEC11a] New South Wales Electoral Commission. *Technology Assisted Voting: NSW State General Election 26 March 2011 (presentation)*. 10 November 2011.
URL: `http://www.elections.nsw.gov.au/__data/assets/pdf_file/0009/96066/Parliamentary_Presentation_10_Nov_2011_v4.pdf`.

[NSWEC11b] New South Wales Electoral Commission. *Report on the Conduct of the NSW State Election 2011*. 2011.
URL: `http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/96297/SGE_2010-2011_Amended.pdf`.

[NSWEC11c] New South Wales Electoral Commission. *Technology Assisted Voting Approved Procedures for Clarence by-election*. 2011.
URL: `http://www.elections.nsw.gov.au/__data/assets/pdf_file/0011/95843/iVote_Approved_Procedures_-_Clarence_v4_-_Final_as_signed.pdf`.

[NSWEC11d] New South Wales Electoral Commission. *Technology Assisted Voting Approved Procedures for NSW State General Election 2011*. 2011.
URL: `http://www.elections.nsw.gov.au/__data/assets/pdf_file/0012/91011/iVote_Approved_Procedures.pdf`.

[NSWEO05] New South Wales Electoral Office. *Submission 10, Inquiry into the Administration of the 2003 NSW Election.* Joint Standing Committee on Electoral Matters, Parliament of New South Wales, 2005.
URL: `http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/6bd39b93036026cfca25784800104d5f/$FILE/SUB10%20-%20SEO.PDF`.

[Oos10] Anne-Marie Oostveen. 'Outsourcing Democracy: Losing Control of E-Voting in the Netherlands'. In: *Policy & Internet* 2.4 (2010), pp. 201–220.
URL: `http://www.psocommons.org/policyandinternet/vol2/iss4/art8`.

[PWC11a] PricewaterhouseCoopers. *Technology Assisted Voting Audit: iVote Post Implementation Report.* 2011.
URL: `http://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/93481/iVote_Audit_report_PIR_Final.pdf`.

[PWC11b] PricewaterhouseCoopers. *Technology Assisted Voting Audit: iVote Pre Implementation Report.* 2011.
URL: `http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/93480/iVote_Audit_report_pre_imp_7_March.pdf`.

[USEAC05] United States Election Assistance Commission. *Voluntary Voting System Guidelines.* 2005.
URL: `http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx`.

[VV08] Verified Voting. *Computer Technologists' Statement on Internet Voting.* 2008.
URL: `http://verifiedvoting.org/downloads/InternetVotingStatement.pdf`.