1 July 2016

Submission to:

The Executive Officer
Electoral Matters Committee
Parliament House, Spring Street
EAST MELBOURNE VIC 3002

Response to: Inquiry into Electronic Voting

Author: Ralph McKay, Founder BigPulse.com

Contents

About the author

Founder and Managing Director of Sydney-based BigPulse.com – a leading international online election service provider with a global reputation for voting technology and security excellence. For over fifteen years McKay has directed BigPulse's continuous online voting technology R&D activity. He has been directly responsible for many voting technology innovations, for the management of many thousands of online elections and the smooth operation of over 30,000 voting projects in 35 countries. BigPulse technology has harvested and counted over 12 million high security votes – approximately 1.5 million votes in the last 12 months, at peak times managing several hundred elections simultaneously with diverse and complex configurations. There is no evidence of security breaches, lost or miscounted votes. The depth and success of this experience is unique in Australia, possibly the world.

Scope of this submission

The author provides an independent critique of the NSW Electoral Commission's (NSWEC) venture into electronic voting using its *iVote*® technology and comments on related security issues.

Summary

Remote online voting is safe for non-government elections. However all independent well informed experts in electronic voting agree that no one in the world has yet demonstrated a practical safe solution for remote online voting in government elections. For example: https://www.verifiedvoting.org/projects/internet-voting-statement/

The NSWEC's iVote technology is exceptional only in that it contains unnecessary fundamental design flaws in the critical area of vote verification which amplify the risks. It is apparent the purpose of the unusual design feature in iVote is to create an illusion of rigor to satisfy the vast majority of uninformed electors. The design blocks the ability to discover accidental and deliberate vote corruption. It appears to be a strategy to minimise the risk of reputation damage to the NSWEC and iVote.

The ongoing use and promotion of iVote to other electoral authorities is a serious danger to our democracy.

The quality of the NSWEC's iVote technology can be assessed from publicly available documents describing iVote as used in the 2015 NSW State Election. It is not necessary to have access to the iVote technology or performance data to understand that the iVote technology is unsafe for use in government elections. The NSWEC has not released data that would assist in quantifying the scale of security failures. This suggests transparency will damage the reputation of the NSWEC and its iVote technology and throw doubt on the integrity of the 2015 State Election.

There is compelling evidence that the NSWEC covered up an extraordinary security failure with iVote in the 2015 State Election which potentially endangered the safety of the most vulnerable NSW electors – that is, any coercion exposed electors who are also at risk of domestic violence. iVote enabled any coercers to discover without effort when they were tricked by the coerced secretly re-voting – thus exposing the most vulnerable voters to retribution from unstable coercers.

At many stages in the vote harvest process secret votes were processed in an unencrypted state. Vote integrity relied on the trust of both known and unknown people at different stages in the process – secret votes could have been observed and or changed, undetected.

Any election criminals or state-backed cyber armies interested in interfering in the election had ample opportunity to do so under cover of darkness, with a low chance of detection – encouraged by the strange iVote design which ensured that an effective vote audit was impossible.

There is no limit to the number of election criminals from anywhere in the world who can simultaneously attempt to interfere in an unverifiable online government election. The effective competing electors controlling the result may be out of sight.

The iVote verification standard as seen in the 2015 State Election is amateur in comparison with best practice in the well-established non-government online election industry. Both the iVote "vote-as-cast verification" and "vote counted verification" were “black box” services – not genuine verification services. Standard best practice techniques for measuring the integrity of the votes counted were ignored without explanation.

The iVote "vote-as-cast verification" process was clumsy, few could be expected to use it – apparently just 1.7 per cent did use it. All who did use it exposed their vote to loss of secrecy and none received a genuine verification that their vote was recorded as intended.

The iVote verification service contained a serious “late vote not verifiable” risk hole – not even verifiable in a black box sense.

The "vote counted verification" service did not genuinely confirm that any authentic votes were actually counted. It used a trust the black box style confirmation. iVote scores at best 2 out of 10 when measured with a robust election vote count verification protocol (for example www.bigpulse.com/verificationprotocol). A negative score would be more appropriate if adjusted for the risk iVote created for any coercion-driven re-voters.

The vast majority, if not all, leading network security scientists around the world with a specialised interest in electronic voting are united in their view that no one has a practical safe solution for remote online secret voting in government elections. It’s apparent that the few independent scientists with opposing views have limited experience and knowledge of electronic voting. There are no scientific papers published in respected journals which conclude that a known practical safe solution exists for remote secret online voting in government elections.

The PWC Electoral Commission NSW Post Implementation Review of the iVote Project FINAL Report dated July 2015, did not:

- comment on the suitability of the technology for future elections
- comment on the absence of best practice in iVote’s vote counted verification technology
- comment on the majority of security holes in iVote’s verification technology
- verify that the votes counted were free of corruption
- confirm that the technology could be trusted to harvest and count votes accurately
- mention the re-voting security issue discovered and reported by the author which exposed vulnerable coercion-driven re-voters to abuse or potential domestic violence (which suggests the NSWEC did not record it as an incident).

However, the PWC audit report did mention:

- many reported security incidents, including exposure to a 'FREAK' attack, https://www.eff.org/deeplinks/2015/04/new-south-wales-attacks-researchers-who-warned-internet-voting-vulnerabilities
- removal of Lockdown so that the Spanish-based Scytl supplier of the core technology could fix an issue
- a requirement to re-encrypted PIN hashes
- time discrepancies in technology components which could have caused votes to be rejected
- an incident which appears to imply that the existence re-voting is acknowledged.

The last point on re-voting is significant because the NSWEC has not released statistics on re-voting and any re-voting implies vulnerable voters were exposed to the serious flaw in iVote's anti-coercion mechanism – a flaw which the NSWEC has declined to confirm or deny.

In contrast to the author's observations, leading scientific opinion, and the less than satisfying audit report:

- the former NSW Electoral Commissioner Colin Barry, proclaimed iVote "a great success" immediately after the 2015 Election.
- NSWEC representatives made public statements such as, "*People's vote is completely secret. It's fully encrypted and safeguarded, it can't be tampered, and for the first time people can actually after they've voted go into the system and check to see how they voted just to make sure everything was as they intended.*" (http://www.abc.net.au/news/2015-02-04/computer-voting-may-feature-in-march-nsw-election/6068290).
- Following the July 2016 Federal Election the Prime Minister Malcolm Turnbull and Opposition Leader Bill Shorten united in calling for the Australian Electoral Commission (AEC) to adopt online voting.
- The NSWEC was awarded the 2016 Australian Government ICT Awards Service Delivery category for its iVote® System in the 2015 NSW State General Election. https://www.scytl.com/en/news/ivote-recognised-for-its-innovation-and-excellence-in-the-2016-australian-government-ict-awards/.
- Both the NSWEC and its Spanish-based supplier are promoting the technology as leading edge voting technology to other electoral authorities while leveraging off the Australian Government's award endorsement.
- The Spanish-based supplier's website promotes its association with the NSWEC as, "clearly leading the way in Internet Voting and eDemocracy" with reference to the Australian Government's endorsement.

iVote is not a "leading" or "breakthrough" voting technology. The "breakthrough" is that the NSWEC has effectively become a flag bearer for a foreign-based electronic voting company in a business licence arrangement which appears attractive for both organizations. The known security risks to democracy remain unsolved, in fact amplified with iVote.

However the NSWEC downplayed, hushed or covered up iVote security risks and failures – apparently in favour of reputation, marketing and commercial objectives. Success was measured as the number of votes harvested and voter satisfaction. About the same number of voters would have been satisfied even if the ballot made no attempt to record the vote coupled with an illusion of vote capture. This point is obvious from the tiny 1.7 per cent reported as having used the verification service and the fact that most electors will feel they can trust electoral authorities in Australia.

It is safe to assume that few if any of the 1.7 per cent of electors who used the verification service understood that the iVote verification process was technically incapable of providing secure vote confirmation. Further very few electors using iVote will have understood the ease with which cyber election criminals can penetrate insecure personal voting devices and secretly corrupt votes or compromise vote secrecy.

The ease with which ordinary electors can be misled about electronic vote security is illustrated by the number of IT professionals who display ignorance on the topic. One such example is a recent publication by Associate Professor David Glance, the Director of the UWA Centre for Software Practice, a UWA research and development centre: http://theconversation.com/despite-experts-fears-australia-should-be-moving-to-electronic-online-voting-61832 Dr Glance has a distinguished career in medical and IT areas but apparently no peer reviewed publications related to electronic voting. In his essay published in The Conversation, Dr Glance argues in favour of introducing online voting in Government elections yet glosses over the intractable security issues. His solution to coercion risk is to allege it does not exist in Australia, citing lack of evidence in postal voting. However he did not cite any rigorous studies confirming it does not exist. Coercion by nature is not easily detected – particularly in a domestic environment. Dr Glance suggested that blockchain voting technologies will solve the vote security issues. However he appears to not understand that blockchain voting does not solve any of the most intractable security issues. For example, the risk of vote corruption within personal devices, loss of anonymity, coercion and vote buying risks all remain in blockchain systems. Transparent verification of votes counted – a standard feature of established leading edge voting systems – does not require use of a blockchain technology. There are likely to be new risks associated with blockchain voting not yet understood.

As a private commercial operation the offshore provider of the core iVote technology can be expected to make best use of its association with the NSWEC. However the NSWEC's first obligation is to protect the integrity of NSW elections, to count all votes securely and maintain the security of vote secrecy. It is difficult to see how the NSWEC fulfilled this obligation in the 2015 State Election.

At many stages from the iVote procurement process through to the end of the NSW 2015 State Election the NSWEC appeared to avoid or discourage independent or public scrutiny of security. This "trust the NSWEC" attitude contributed to poor quality testing and design flaws.

The NSWEC excluded all Australian-based service providers from competing in the iVote procurement process while inviting three offshore-based service providers to compete. The NSWEC demonstrated a "whatever it takes" attitude toward keeping excluded vendors in the dark as to why they were excluded until after the contract was awarded. In reference to BigPulse the NSWEC stated, "*Extensive commentary on security with little attempt to describe relevance to NSWEC requirement"*. The contract was awarded to a Spanish-based supplier that was apparently happy to accept the NSWEC's naively constructed, seriously flawed security standard while rejecting BigPulse – an Australian-based global leader in online voting technology which insisted on a far superior security standard – as a suitable tenderer.

There may be an argument in favour of remote online voting for local government elections, if conducted in a securely verified transparent manner. However coercion risk will need to be accepted along with the possibility of an election re-run because the verification process exposed vote corruption.

The only countries that have tried and not soon discontinued with online voting in government elections for security failures are Switzerland and Estonia.

Phone voting is even less secure.

Electronic voting: comparing non-government and government

Electors frequently ask for online voting in government elections because it is so convenient. Many people have already experienced the simple elegance of online voting in non-government elections, and seen their vote verified. A large number of Australians have voted online many times over many years confident that their vote is secure – particularly on BigPulse technology used by most leading universities, many professional associations and political parties. The most astute voters will be aware that BigPulse technology is capable of issuing secure vote receipts which can be used to verify the integrity of votes counted – a transparent audit.

However, very few electors have a deep appreciation of the risks. If banking can be conducted online then why not government elections? The difference is that money stolen from a personal bank account is readily detected and is replaceable. However lost votes are not in general replaceable, an election re-run will not necessarily reproduce the same result – the process is not reversible, like toothpaste that cannot be put back in the tube. This irreversibility is a consequence of the secret ballot, invented in Australia to protect the integrity of elections.

The important difference between non-government and government secret voting elections is that government elections are likely to offer greater incentive for criminals to interfere with voter intentions and vote secrecy and to engage in vote buying and coercion.

Because of the difficulty in securing remote personal devices to an acceptable standard it must be assumed that when the motivation is high enough that criminal elements and foreign powers will attempt to interfere with voters' voting devices with the intention of secretly viewing or corrupting votes. Therefore a rigorous verification process to detect vote corruption is essential in government elections. (However loss of vote secrecy is hard to detect unless the criminal is caught in the act.) A rigorous vote verification process involves issuing each voter with a uniquely coded real take-home vote receipt followed by the publication after close of voting of all counted vote receipts with unique codes displayed.

Coercion and vote buying risks can be managed to some degree by allowing the coerced to secretly re-vote to trick coercers. However this risk management technique clashes with the vote verification process because verification means a coercer can discover when they were tricked with a secret re-vote. This presents an intractable problem in electronic elections whenever voter coercion or vote buying is a risk that needs to be managed.

In spite of this clash, the NSWEC's iVote system attempted to use low grade vote counted verification and coercion risk management simultaneously in the 2015 NSW State Election. It appears that the NSWEC fell in a trap. Any coercers were able determine after the election closed to voting if they had been tricked with a secret re-vote – betraying the trust of the coerced and creating potential risks to their safety.

A further problem for vendors focused on government online voting is that they are likely to lack experience. They don't have a safe solution for government elections which means very few electoral authorities allow them to get experience. Yet a secure voting system that can be trusted requires many years of intense use in real elections.

For a more detailed comment on electronic voting security in government elections see http://www.bigpulse.com/governmentelections.

iVote vulnerable to vote tampering, vote verification service flawed

The most effective way to inhibit any motivation for criminal interference in an election is to ensure that any vote corruption is easily detected. However iVote was vulnerable to undetectable vote tampering in the March state election.

The widely reported FREAK attack vulnerability demonstrated by J. Alex Halderman and Vanessa Teague, "*The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election", (http://people.eng.unimelb.edu.au/vjteague/iVoteSecurityAnalysis.pdf*) illustrates one of many ways that votes could have be tampered with or observed on voter devices. The NSWEC was clearly aware of the potential for this client side middle-man-attack. The NSWEC obviously attempted to "manage" this client-side risk by offering a separate channel, that is, phone based "vote-as-cast verification" service along with an option for voters to change votes. However this separate "vote-as-cast verification" channel failed in its objective and added further risk.

The iVote "vote-as-cast verification" service was so cumbersome and slow to use it is likely that only a very small fraction of voters successfully used the service. Consequently very few electors if any may have detected any interference of their votes even if FREAK type attack was prevalent.

An informed voter would know that using the "vote-as-cast verification" exposed secret votes to insecure telco network transmission. Any criminal elements with access into telco networks and servers may have harvested unencrypted votes along with attached phone numbers – a further disincentive to use the vote verification service. It is possible that such a harvested list of votes with attached phone numbers exists now with the ever present risk that it may be menacingly published on the internet at any time.

The "vote-as-cast verification" service was disabled at the close of voting. This is interesting because there is no inherent technical reason why votes should not be verifiable as recorded correctly after the vote close time – in fact, it is essential for a genuine audit, that verification of the actual votes counted is permitted after vote close. The sudden closing of the "vote-as-cast verification" service meant that any last minute voters had no chance of using even a flawed vote verification service. This was a very high risk time for vote tampering. Election criminals with appropriate malware could modify last minute votes in secret with virtually no chance of detection. An apparent motive for disabling the "vote-as-cast verification" service immediately after vote close is to avoid the risk that some electors report discrepancies with verified votes at a time when the option to re-vote had lapsed.

The 102 page iVote System Security Implementation Statement attempts to give the impression that votes were securely protected with encryption once within the iVote servers. However this assurance is hollow given one basic observation: Votes were stored with a connection to the voters' personal voting accounts. This is obvious from the fact that a change vote option was offered and the fact that the "vote-as-cast verification" returned unencrypted votes across the telco networks.

Vote counted verification process flawed

To understand the flaw in iVote's vote verification and vote counted services it is helpful to first understand the nature of the electronic vote verification problem and industry best practice for dealing with the problem.

In a practical sense an electronic voting system is a "black-box" to election auditors. No one can be certain that a complex electronic voting system is free of malfunction or corruption simply because the technology appeared to be safe prior to launching the election and all operating procedures appear adequate. For example, remote electronic voting, such as online voting, exposes votes to the risk of malware on elector devices. Phone voting exposes votes to insecure unencrypted transmission through telco networks and servers. Best practice quality electronic voting systems manage this "black box" problem with an elegant transparent audit technique which tests the integrity of the vote counts after the close of voting. The essential idea is easy to understand. Soon after vote close time, and well before any options to challenge the result lapse, electors and auditors are given easy access to a list of all votes counted, each with its unique vote receipt code attached. Electors can then identify their votes in the counted list. This process also enables the vote tallies to be verified independently by anyone with an interest and moderate technical skill. If no one can detect fake or missing votes in this transparent inclusive audit process, then and only then, can the vote count integrity in a government election be considered verified to an acceptable standard.

However there are many ways a transparent audit can be poorly implemented. A seven point Election Vote Count Verification Protocol published by BigPulse at http://www.bigpulse.com/verificationprotocol defines a top level election verification standard. Transparency of vote receipts is listed as process number 4 and weighted by a factor of four in this standard causing an automatic fail whenever it is absent. The remaining six processes listed in the standard relate to verifiability and secrecy protection of vote receipts, the ability to detect fake receipts and ballot presentation integrity.

The most fundamental element in this robust electronic election verification standard – transparency of counted vote receipts – was absent in iVote. The phone voting aspect of iVote scores just 1/10 on this scale if the phone issued receipts are counted as full take home receipts. The online voting aspect of iVote could score at best 2/10 for issuing more secure vote receipts. However the vote secrecy risk associated with the phone voting and phone-based vote verification process further downgrades the quality score.

It is apparent that the NSWEC attempted to replace the requirement to publish a list of vote receipts as the essential verification tool, with a two part "vote-as-cast verification" and "vote counted verification" process. The result of this dumbing down of the verification process is that not a single real vote was genuinely verified as counted. The vote counted verification service did nothing more than confirm that a receipt number was valid. It was a "trust the black box" process that created additional security risks as discussed in this essay under "iVote's anti-coercion : endangering the vulnerable or compromising vote security?".

The very low vote verification standard employed by iVote meant that any well executed corruption of vote records or vote counting within the iVote servers, and any corruption of votes in the insecure harvesting process external to the iVote servers not detected by a flawed verification service, remained undetected.

Potential reasons why the NSWEC did not publish the vote receipt list

The issuing of real high quality vote receipts followed by publication of all vote receipts after close of voting is the secure and transparent way to allow verification of the integrity of an electronic election result. The NSWEC did not publish the iVote receipts following the 2015 State Election. Vote receipt transparency is incompatible with coercion driven re-voting, yet iVote attempted to offer a vote counted verification service anyway. So this incompatibility is the real explanation for not publishing the vote receipts in this case.

A (well founded) lack of confidence in system integrity appears to be the explanation:

1. Withholding access to the election vote receipt list eliminates the risk of embarrassment that some electors may discover that their receipt number did not appear in the counted list or the attached vote preferences were incorrect.
2. The insecure manner in which the vote receipts were issued by iVote created a risk that publication of vote receipts could encourage false claims of miscounting or mis-recording.
3. Giving elector access to counted vote receipts will compromise vote secrecy whenever the issued receipt numbers are not securely protected at all times. iVote allowed receipt numbers to be transmitted insecurely over telco networks. Also it is not clear that the NSWEC properly informed voters to keep their receipt number secret, an essential pre-condition before vote receipts can be published.

Misguided priorities

The NSWEC appeared to place a higher priority on avoiding any public perception of a failed voting system than the protection of vote integrity. For example, the iVote security statement states, "*lessons learnt from the international incidents*". One example given is the 2010 Washington, D.C. internet voting trial. In this case the District held a mock election in which the public was invited to attempt to hack into the system. The system was hacked within 48 hours, every vote was changed and almost every secret vote revealed. The intrusion was not detected for nearly two days. The trial was suspended. The District's electoral authority was naive in procurement but wise in testing. Democracy was not compromised.

The NSWEC did not invite the public to rigorously test and attempt to hack into the system prior to live voting. It appears the lesson NSWEC took from Washington, D.C. was to avoid the risk of pre-launch bad press that can follow rigorous public testing of an insecure poorly tested voting system. As a consequence at least one serious risk hole, the FREAK attack risk, was found too late. Serious issues regarding the vote count integrity and protection of vulnerable coerced electors remain unanswered. Inevitably other security flaws remain undetected.

Another example of misguided priorities was the code review policy. The NSWEC invited code reviewers but imposed a strict hush clause preventing reviewers from talking in public about their findings until after the period when the election could legally be challenged. This would have repelled most if not all top code reviewers who may have been interested.

Success appeared to be measured by the number of people using iVote. The NSW Electoral Commissioner Colin Barry, proclaimed "*a great success .. the staggering increase in voters using the iVote system demonstrates that confidence and demand for secure online voting systems is growing despite ill-intended efforts to discredit its integrity*", (Computerworld 31 March, 2015). The ordinary elector has very little understanding of electronic vote security.

Electors however do have a right to expect that the NSWEC does understand the security issues.

The NSWEC EOI documents expressed an interest in licencing iVote to other electoral authorities. This creates the potential for a perception of conflict of interest between vote security for NSW electors and the NSWEC's marketing ambitions and the value of its registered trademark *iVote*®. Transparency in iVote's security flaws will make marketing iVote to other authorities more difficult. The NSWEC has permitted the Spanish-based supplier of the iVote technology Scytl to use the NSWEC logo in its promotional website attached to a glowing description of iVote as a security success, "…*Backed by the implementation of the world´s most advanced and proven security protocols, the staggering figures of over 280,000 online votes, an increase of 500% in adoption, and praise from auditors, security experts and citizens, the iVote® System sets the standard for the world's largest, most accessible and innovative internet voting implementation.."* (http://www.scytl.com/en/customers/). It is unclear how this one-side description of iVote's security features, ignoring obvious iVote testing and security failures, is helpful to NSW electors, taxpayers or democracy.

Anti-coercion management in the NSW Electoral Commission's iVote system – betraying electors' trust, endangering voter safety

Vote corruption and loss of vote secrecy is not the only concern when naïve electoral authorities venture into online voting. Amateur voting systems can also endanger the safety of vulnerable electors. The NSW Electoral Commission fell into this trap attempting to manage coercion risk with its iVote technology in the NSW 2015 State Election.

Any election using remote electronic voting, such as online voting from home or office, which also offers or encourages secret re-voting as a means to manage coercion risk, must not give electors access to a vote-counted verification mechanism otherwise it betrays electors' trust. In a practical sense, coercion driven secret re-voting is incompatible with a transparent vote count audit.

The reason for this incompatibility is that a vote-counted verification mechanism can also be used by coercers to detect when they have been tricked by the coerced secretly re-voting. If other aspects of the voting system are secure the preference selections in the re-vote will remain hidden from the coercer. However the fact that coercers can discover they were tricked betrays the trust of the coercion-driven re-voter. This betrayal of the trust by the electoral authority creates obvious potential for distress and even physical danger for the most vulnerable electors at risk of domestic violence.

Curiously, iVote attempts to offer both coercion risk management along with an obscure form of vote counted verification service – a serious design flaw.

In the lead up to the NSW 2015 State Election the NSWEC released its iVote System Security Implementation Statement which states, "*The iVote® system has an anti-coercion mechanism in that it allows a user to re-vote during the voting period.*"

This option to re-vote encouraged any coerced electors to trick their coercers by re-voting in secret. A re-vote is understood to cause the first vote to be cancelled. A coercer is likely to know the receipt number of the coerced person's first vote but not the re-vote. Receipt numbers are unique to each vote.

iVote also encouraged electors to "verify" which votes were counted using its "vote counted verification" service (https://cvs.ivote.nsw.gov.au/receipts/#/home). The iVote FAQ states, "*How do I know that my vote was counted? From the Monday following Election Day, you can confirm your vote was included in the count by visiting ivote.nsw.gov.au select 'Verify' and enter the receipt number.*"

This means iVote enabled coercers to discover very easily when they were tricked with a re-vote and therefore betrayed the trust of the most vulnerable electors.

The author noticed this iVote design flaw when observing the NSWEC's iVote literature during the vote-counted verification phase of the 2015 State Election. Immediately, that is, on April 5^{h} 2015 and again on April 7th, the author alerted the NSWEC along with a comment on the danger for any coercion-driven re-voters. However the NSWEC did not respond until April 20th and the "vote counted verification" page was not removed. The NSWEC's late response stated,

"*Your comments have been considered but are not of sufficient merit to warrant any changes to the current iVote system. The Commission's position on coercion in iVote is based on the paper prepared by Dr Smith of Sydney University which can be found on our website at http://www.elections.nsw.gov.au/__data/assets/pdf_file/0003/118380/NSWEC_2013_Report_V2.0.pdf.*"

The NSWEC response did not confirm or deny the existence of the design flaw. The response appears to rely solely on the assumption that coercion is not a risk that needs to be managed in NSW state elections. The response was inconsistent with the iVote System Security Implementation Statement which includes the comment,

"*The iVote® system has an anti-coercion mechanism in that it allows a user to re-vote during the voting period.*"

This comment demonstrates that the NSWEC believed coercion was a risk just prior to the 2015 State Election and that there was merit in managing it. Yet just several weeks later, at a time when the "mechanism" was being offered to NSW electors – having just been alerted to the danger it created for electors – the NSWEC apparently then adopted the position that coercion does not exist in NSW, by saying, "*not of sufficient merit to warrant any changes to the current iVote system."*

The NSWEC had received the design flaw alert from the author, and was informed of the danger it presented to vulnerable voters, yet it chose to leave the iVote vote counted service online and operating for many days.

Responding to the danger would have required the NSWEC to immediately remove the iVote "vote counted verification" website many days prior to the heavily advertised cut-off date. However this would have required a public explanation. An honest explanation would have severely damaged the iVote brand name and reputation of the NSWEC. It is difficult to escape the conclusion that the NSWEC placed higher priority on protecting its reputation than eliminating a danger it unwittingly created for the most vulnerable electors.

This behaviour is consistent with many other misplaced priorities in the NSWEC's management of its iVote project which appear to place protection of reputation above vote security and transparency.

The NSWEC's September 2015 submission to the NSW Parliament Electoral Matters Committee Inquiry into the 2015 NSW State Election provides further insight,

"*The Commission sees coercion as a small risk because of the difficulty for any person or organisation to identify those individuals intending to vote remotely and in sufficient numbers, and then successfully subvert their vote to influence an election result. Such coercion would have to be of such a scale that the cost and risk would make it a barely viable option to attempt*."

Here the NSWEC ignores the possibility of coercion within the family home. This is consistent with an apparent strategy to avoid any discussion regarding a serious security flaw related to coercion-driven re-voting endangering voter safety. Moreover in a close election even a few isolated coerced votes can make a difference to the result. Significantly, the NSWEC referred to a "small risk" not a zero risk. With 280,000 electors a "small risk" could in fact represent a large number of people. Media reports have referred to an "epidemic" of domestic violence in the State of NSW. Given the potential for unstable coercers to react on discovering they were tricked, even one person at risk is too many.

It would be unwise to assume that any re-voting was not coercion-driven because there is no way to know for sure why an elector requested a re-vote. The NSWEC has not released statistics on re-voting. However it is very unlikely that with 280,000 remotely harvested votes no elector requested a re-vote. The PWC Electoral Commission NSW Post Implementation Review of the iVote Project FINAL Report mentions an, "*EMA interface for multi vote removals"* incident –"multi vote" appears to confirm the existence of re-voting.

The author has considered the possibility that iVote's vote counted service was deliberately designed to misinform voters when re-voting occurred or that all votes from the same elector were assigned the same receipt number. Both options would be a concern with differing security implications. However the NSWEC has released technical documents which make clear that vote receipts were unique to each vote, as they should be. Further, the fact that the PWC audit report does not mention the re-voting design flaw also indicates it was not recorded as an incident. Therefore the possibility that the NSWEC secretly reacted by causing the iVote vote counted service to deliberately misinform voters, can be ruled out.

The NSWEC was given an obvious hint by the author that its iVote specification was seriously flawed in the lead up to the iVote procurement process. The following rhetorical question, published in the iVote Addendum 1 during the iVote Expression of Interest phase in December 2013, came from the author,

"*Change vote is requested to limit coercion along with the ability to publish receipts. These appear to be conflicting requirements?*"

The hint was ignored. The NSWEC responded at the time with,

"*Voters are able to re-register, cancelling the original vote, and vote again. The receipt number is used to access a vote verification system to check their vote as described in Attachment 1.*"

The response demonstrated that the NSWEC was naïve in its understanding of electronic voting systems and associated risks. The risk was compounded by a procurement process destined to exclude vendors that would not permit such basic security failures.

In a document that attempted to explain why BigPulse, the Australian leader in online voting technology and services, was blocked from competing in the iVote tender the NSWEC stated in reference to BigPulse,

"***Extensive commentary on security with little attempt to describe relevance to NSWEC requirement***"

This document was controversially withheld from BigPulse until after the iVote contract was signed with the Spanish-based supplier.

The NSWEC betrayed the trust of NSW electors by harvesting many votes with an insecure and dangerous voting technology. This betrayal of trust was amplified when the NSWEC chose not to remove the danger when it was discovered. It further betrayed the trust of NSW electors and the NSW Parliament by failing to acknowledge its errors.

iVote technology procurement process concerns

The NSWEC demonstrated a "whatever it takes" attitude toward keeping excluded vendors in the dark as to why they were excluded.

The iVote Expression of Interest ("EOI") documents indicated that up to four vendors could be invited to submit tenders. Yet only three offshore vendors where actually selected to compete for the iVote tender. One of the three vendors included had no obvious history of direct experience with online voting. Many more than four online voting technology vendors, some with many years' experience in the industry, responded to the EOI but were excluded from competing in the tendering process. A fourth tenderer to fill the quota was not permitted. Critically the NSWEC did not request essential information required to assess vendor quality or competitiveness.

BigPulse was one of the local technology vendors that was blocked from tendering. BigPulse made clear in its EOI submission that its technology operated to a higher performance and security standard than specified in the iVote documents – supported by its international reputation for excellence in running online elections. The NSWEC made no attempt to test this claim, the technology was not viewed, analysed or tested, no detailed technical information was requested, no price information requested, no questions were asked. However BigPulse did make clear to the NSWEC that it would not lower its security standard to the level defined in the iVote documentation. BigPulse also commented on inconsistencies with NSWEC's stated objective for a secure voting system and aspects of iVote's specification which clearly defined an insecure voting process and also appeared to contain a fundamental design flaw with its coercion management method.

Expecting that the NSWEC would adhere to the highest standard of integrity in the procurement of a government voting technology the author attempted to obtain an explanation from the NSWEC as to why BigPulse was excluded from competing in the iVote tendering process. This attempt to obtain an explanation raised further concerns about the integrity of the iVote procurement process. It also demonstrated that NSW government agencies can disqualify interested vendors including all Australian-based vendors from a call for tender process without due consideration of a vendor's merit, without providing a timely meaningful explanation, with impunity.

NSW Procurement, the government agency charged with administering the NSW Procurement Guidelines adopted a very soft interpretation of the relevant aspect of the Procurement Tendering Guidelines which as of December 2011 version 3.2 page 45, state,

"If a supplier in a multi-stage process is not invited to participate in the second or subsequent stages of the process, the supplier shall on its request, be provided with a written explanation of the reasons for the decision."

The NSW Procurement agency confirmed that the explanation must also be timely citing another aspect of the Guidelines, "*Agencies are expected to promptly and adequately investigate and respond to complaints."*

Yet NSW Procurement permitted the NSWEC to interpret the Guidelines in a manner which allowed it to withhold any form of meaningful explanation for why it excluded interested vendors until the contract was awarded many months later – preventing any chance of scrutiny of a suspect procurement process until it was too late.

The following summary illustrates inconsistencies in statements made by the NSWEC and a "whatever it takes" attitude to avoiding scrutiny:

1. NSWEC first declined to send any form of debrief until after contract signing quoting a NSW Procurement Guideline which appeared to support its position.

2. The author then raised the matter with the NSW Procurement agency which immediately confirmed that the NSWEC had quoted an inappropriate Guideline. The appropriate Guideline in fact required a prompt written explanation.

3. Following an intervention from NSW Procurement the NSWEC responded again (without apology for its previous misguided response) and quoted the appropriate Guideline. However this "explanation" was simply a verbose assurance from the NSWEC that its iVote evaluation process can be trusted along with a score assigned in four categories with no detail provided to justify the scoring. An interesting comment included in the response was, "*The use of weights ensures that a higher final score was awarded to responses that scored highly in the areas considered by the Steering Committee to be most important*." This statement gave an impression that the NSWEC guided its undisclosed "independent" evaluators with a weighting system that produced the desired short list for the tendering process. The NSWEC response also indicated this was the final and full explanation required under the Procurement Guidelines (which it later referred to as "preliminary").

4. A formal complaint was submitted to the NSWEC. The NSWEC responded answering no questions and referred to a "debrief" opportunity as the end of the procurement process – essentially an admission that the full explanation had not yet been provided as required under the Guidelines.

5. Gareth Ward MP Chair of the Joint Standing Committee on Electoral Matters attempted to assist by writing to the Electoral Commissioner. This letter featured a copy of the appropriate section of the Guidelines and included many questions drafted by the author. The Commissioner's response to Mr Ward answered no questions and did not comment on the Guidelines. However the Commissioner did state in this letter, "*I would recommend that you should not engage with Mr McKay as we are still in the middle of the procurement process.*" The Commissioner was clearly aware at this time that the complaint against the NSWEC centred on its failure to comply with the Guidelines and that the NSWEC had an obligation under the NSW Procurement Guidelines to "engage" by providing the requested explanation promptly and in writing. The impact of this letter from the Electoral Commissioner was to discouraged communications with a member of parliament seeking to assist with concerns over a procurement process under his watch.

6. The author requested that NSW Procurement confirm that it still stands by earlier written advice as to the appropriate Guideline. Surprisingly, the request was referred to the team manager who refused to confirm or deny. This stonewall response appeared to occur after the time of lodging the formal complaint with the NSWEC. A diary note of the conversation was sent to NSW Procurement which produced a near immediate phone call response from NSW Procurement Executive Director Paul Dobing. He expressed concern and stated the matter had come to his attention for the first time that day. He confirmed emphatically that the NSWEC was required to provide the requested written explanation. Mr Dobing asked the author to hold off a while until he investigated and reported back. By "hold off" the author understood Mr Dobing meant not to make the matter public (or possibly report to another agency) until he had looked into it. He sent an email which stated, *"I will look into the matters you raised and come back to you with an initial response early next week."* No further response was received until six days later in response to a reminder email from the author. It appeared Mr Dobing was satisfied that the NSWEC need not provide any further detailed explanation. His intervention had the impact of assisting the NSWEC in delaying its debriefing response until after contract signing.

7. With the assistance of Mr Dobing the NSWEC offered a face to face meeting involving the attendance of several senior public servants. The offer was declined as it appeared to be an attempt to evade the NSWEC's obligation to a send a written explanation prior to awarding the contact and a delaying tactic.

8. The requested written explanation (225 words) was sent just six days after the proposed date of this meeting, that is, the same day the NSWEC announced the contract was awarded. Apparently the NSWEC was on the verge of securing the iVote contract at the time of suggesting an expensive and time consuming meeting as an alternative to sending the short 225 written explanation. The commentary in this delayed explanation (debrief) misrepresented the information available to NSWEC in BigPulse's EOI submission. The following comment included in the explanation, "*Extensive commentary on security with little attempt to describe relevance to NSWEC requirement"* illustrates the low priority the NSWEC placed on vote security and its lack of interest in exploring security concerns raised by local experts.

9. From the outset the NSWEC stated it would not send the explanation until after contract signing. And this in fact is what it did, in spite of 60 documents and over 20,000 words attempting to hold it to account under the NSW Procurement Guidelines.

End