Submission No 10

INQUIRY INTO THE 2015 NSW STATE ELECTION

Organisation: BigPulse

Name: Mr Ralph McKay

Date Received: 24/08/2015

Submission to: Joint Standing Committee on Electoral Matters, Parliament of New South Wales

Response to: Inquiry into the 2015 NSW state election

From: Ralph McKay, BigPulse.com

24 August 2015

About the author

Ralph McKay is a NSW elector and founder and Managing Director of Sydney-based BigPulse.com – a leading international online election service provider. Representing fifteen years as the head of a continuous online voting technology R&D activity and direct responsibility for the management of many thousands of online elections. BigPulse technology and election management services have been used successfully in over 30,000 voting projects in 35 countries, over 12 million high security votes harvested, 1.5 million votes in the last 12 months. No evidence of security breaches, lost or miscounted votes. This level of practical experience in online voting will be difficult to match anywhere in the world.

General comment

Many people having experienced the simple elegance of online voting in non-government elections, and seen their vote verified, then ask why not online voting for government elections? A large number of Australians have voted online many times over many years confident that their vote is secure – particularly on BigPulse technology.

However there are critical differences with government electronic elections compared to non-government elections which create serious security issues for government voting – especially with remote online voting. Phone voting is even less secure. One of the most intractable security issues in government remote electronic voting is the incompatibility of coercion risk management and the requirement to verify that only valid votes are counted. For a more detailed comment about electronic voting security in government from the author of the essay visit http://www.bigpulse.com/governmentelections.

Summary of the author's observations of the NSWEC's iVote technology

The NSW Electoral Commission's (NSWEC) iVote system employed in the March 2015 state election contained several serious design flaws which compromised vote security and potentially the safety of some vulnerable electors. It is apparent the iVote design attempted to give an appearance of managing two fundamental security issues inherent in the use of remote electronic voting in government elections – coercion risk management and the inability to control the security standard of electors' remote voting devices. However this masking attempt inadvertently increased the overall security risk for the election. These intractable security risks are well known to network security experts specialised in electronic voting but rarely well understood by IT professionals not specialised in electronic voting.

At many stages from the iVote procurement process through to the end of the 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.

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). This statement is misleading. 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 changed and remain undetected.

The integrity of votes harvested by iVote relied heavily on the assumption that no one, from foreign states to lone rogue hackers, with access to appropriate technical resources was motivated to interfere illegally with the NSW March state election.

Both the iVote "vote-as-cast verification" and "vote counted verification" were "black box" services – not genuine verification services.

The iVote "vote-as-cast verification" process was too clumsy to be effective. It compromised vote security and 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 if a single authentic vote was actually counted. On comparison to a robust election vote count verification protocol (for example www.bigpulse.com/verificationprotocol) iVote falls far short of accepted online voting industry standards, scoring at best 2/10.

The iVote attempt at mitigating voter coercion risk by inviting the vulnerable to re-vote in secret was seriously flawed. It clashed with the "vote counted verification" objective. If implemented as expected from its description iVote enabled 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. On the other hand, if actually implemented using one of two possible alternatives it exposed all electors using iVote to undetectable vote override from impersonated re-votes.

The procurement process excluded all but three offshore service providers from tendering while attempting to give an appearance of a merit based process which in fact locked out all local service providers from tendering without due consideration of merit. The NSWEC demonstrated a "whatever it takes" attitude toward keeping excluded vendors in the dark as to why they were excluded. Attempts to hold the NSWEC to account under the NSW Procurement Guidelines revealed that the NSW Procurement agency accepts a very low standard of interpretation in the Guidelines – one that allows agencies to effectively exclude tenderers arbitrarily with impunity.

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

It is not hard to see why the NSWEC did not publish the vote receipts. Vote receipt transparency is incompatible with coercion driven re-voting. However a lack of confidence in system integrity could also be a factor:

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 vote receipts issued by iVote exposed vote receipt transparency to false claims of miscounting or mis-recording.
3. Elector access to counted vote receipts compromises 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.
4. Vote receipt transparency clashes with coercion driven re-voting. A published list of vote receipts reveals which receipt numbers are associated with votes actually counted. This would alert coercers whenever a vulnerable elector re-voted expecting to defeat coercers.

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.

iVote's anti-coercion : endangering the vulnerable or compromising vote security?

Any electronic voting system that enables electors to change their vote expecting to trick coercers, defeats any chance of using a meaningful transparent election verification process. In a practical sense, coercion driven secret re-voting is incompatible with a transparent vote count audit. iVote attempted to offer both coercion risk management along with an obscure form of vote counted verification service. It created more risk than it eliminated.

The iVote System Security Implementation Statement states, "*The iVote® system has an anti-coercion mechanism in that it allows a user to re-vote during the voting period.*" If the iVote "vote counted verification" service was implemented as described then iVote exposed unsuspecting vulnerable coerced re-voters to the danger that their coercers could easily discover when they were tricked by a "secret" re-vote. If not implemented as described then the "vote counted verification" service either deliberately misinformed electors about their vote counted status when re-votes occurred or it used a trick idea that confirmed to electors which receipt numbers were included in the count but not which vote preferences were actually counted. Both possible variations from the expected implementation would also expose all electors using iVote, not just the coerced re-voting electors, to the risk that votes were secretly replaced by impersonator re-votes. If the trick idea was used coerced re-voters were exposed to additional risk in the event of a security breach. This observation follows automatically from the fact that iVote offered re-voting as an anti-coercion mechanism together with a "vote counted verification" service.

The option to re-vote encouraged 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, unless iVote assigned the same receipt number to first votes and any re-votes by the same elector.

Normally with electronic voting it is considered essential that each vote be assigned a unique receipt number or better a receipt code. If iVote did assign a unique receipt number to each vote and the "vote counted verification" service did provide the correct response on which receipt numbers were associated with counted votes then it enabled coercers to discover very easily when they were tricked with a re-vote and therefore betray the trust of the most vulnerable electors.

Obviously coercion-driven re-voting relies on the assumption that coercers cannot discover when they have been tricked with a re-vote.

Curiously iVote permitted coercion-driven re-voting while also encouraging 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.*"

The author alerted the NSWEC to a concern for the safety of any coercion driven re-voters on April 5th and again on April 7th. 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 that the safety of coerced re-voters was at risk at any stage or how it avoided such risk. The response appears to rely on the assumption that coercion is not a risk that needs to be managed in NSW state elections. Yet the iVote System Security Implementation Statement states, "*The iVote® system has an anti-coercion mechanism in that it allows a user to re-vote during the voting period.*"

Why did the NSWEC not remove its "vote counted verification" service after receiving the alert of the author? There are a number of possible explanations:

1. Maybe no one re-voted. (Well informed vulnerable electors could perceive privacy risks attached to re-voting with iVote. However it appears unlikely that no re-votes were recorded and it would be unwise to assume that any re-voting recorded was unrelated to coercion management).

2. Perhaps iVote's "vote counted verification" service was designed to incorrectly inform that cancelled votes were actually counted, or was quickly amended to misinform after receiving the author's alert. However this kind of misreporting causes other problems. Did the NSWEC warn re-voters to expect the verification service to misinform on cancelled votes? This design would also mean that the verification service would not alert any of the 280,000 electors if an impersonator re-voted in their name. In fact this design could replace the incentive to coerce electors with an incentive to re-vote as an impersonator. Anyone inclined to illegally vote many times, with access to the necessary personal data of other voters, could request one or more re-vote accounts. So the method of issuing re-vote accounts is critical in this case.

3. There is another possibility. Perhaps iVote issued the same receipt number for all votes believed to be submitted by the same elector. If vote receipt numbers were unique to electors, not votes, it would mean the "vote counted verification" service would not even attempt to inform electors who re-voted which vote was actually counted, but it would trick the coercers. This method would also expose the coerced re-voter to greater risk if receipt numbers with attached votes were exposed in a secrecy breach because in this case the coercer will be holding the same receipt number as the coerced. The use of repeated receipt numbers also exposes all electors to the impersonator risk, as with possibility 2.

The iVote security statement does appear to provide a hint that the receipt numbers may not have been unique for each vote with the comment, "*When voting using iVote®, electors are given a unique receipt number.*" The use of the word "electors" in this statement rather than the expected "votes" gives the impression that the receipt numbers were unique to the electors not the votes. If this is the case then re-votes were assigned the same receipt number as the first (coerced) vote. However this may be just poor drafting.

There is a further hint in iVote that receipt numbers may not be unique to each vote. The "vote counted verification" service invited electors to enter the vote receipt number into a webpage which replied, "*Confirmed. The voting receipt number listed below was included in the count.*" This statement will always be true regardless of which votes with the same receipt number were counted! However the more direct response of, "The vote linked to this receipt number was included in the count" cannot be used if more than one vote can have the same receipt number. Again it may be just poor drafting.

The NSWEC was given an obvious hint that its iVote specification was seriously flawed in the leadup 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 NSWEC responded, "*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 iVote anti-coercion mechanism created more risk than it eliminated.

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 [redacted] 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. [redacted] asked the author to hold off a while until he investigated and reported back. By "hold off" the author understood [redacted] 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 [redacted] 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 [redacted] 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