Scytl
Innovating Democracy

Scytl Australia Pty. Ltd.
PO Box 7529, Baulkham Hills, NSW 2153
www.scytl.com

25 August 2016

Mr Jason Arditi,
A/Director,
Committee on Electoral Matters
electoralmatters@parliament.nsw.gov.au

Re: Inquiry into the 2015 NSW state election
Response to questions on notice

Dear Mr. Arditi,

I thank the Committee for the opportunity to respond to these matters that arose during the recent public hearings for the Inquiry into the 2015 NSW state election.

I address the questions immediately below, with the exception of the response to the submission by Dr Teague and Professor Gore, which is responded to as an attachment. In addition to this, in reading my transcript, I was of the feeling that Scytl may have been understood by the committee to have been 'running the iVote system', which was outside Scytl scope. For the purposes of clarity an overview statement is provided within the attachment to this letter.

In general, references I made to iVote in my statement may be looked at as references to the 'iVote Core Voting System' or iVote CVS, which is the software application provided to the NSW Electoral Commission by Scytl. Within Scytl the iVote CVS is commonly referred to as iVote.

> ***The Hon. Robert Borsak:*** There is another acronym in your submission, EMA. What is that?
>
> ***Response:*** EMA is the NSWEC Election Management Application. It is a NSWEC designed and operated system that interacts with the iVote system.
>
> ***The Chair:*** I will ask you to take on notice to comprehensively write back to this Committee specifically on the allegations raised by Dr Teague and Professor Gore.
>
> ***Response:*** Please refer to the attached response which addresses the allegations raised by Dr Teague and Professor Gore in their submission.
>
> ***The Hon. Courtney Houssos:*** Who were the interested parties?
>
> ***The Hon. Courtney Houssos:*** Who selected the interested parties and what was the process for establishing who they should be?
>
> ***Response:*** This question relates to the interested parties who compared the data in the iVote CVS ballot box and the Verification system at what was known as the Verification

event. The event was organised by the NSWEC, and I expect they can provide more detail about that event, who attended, and the process around it.

My understanding is that the attendees included staff from 2 universities from Sydney (Macquarie and UNSW) and scrutineers from 2 political parties.

The Hon. Dr Peter Phelps: What level of technical sophistication would be required to do that? (Regarding the issue of exploiting the Piwik vulnerability)

Response: This question is answered in the response provided to the allegations of Dr Teague and Professor Gore as an attachment to this letter.

Please contact me if any of this requires further clarification.

Yours Sincerely,

Sam Campbell,
Director,

Scytl Australia Pty. Ltd.

1 Introduction

This document is a response to the following question on notice from the NSW Inquiry into the 2015 State Election:

> ***The Chair:*** I will ask you to take on notice to comprehensively write back to this Committee specifically on the allegations raised by Dr Teague and Professor Gore.

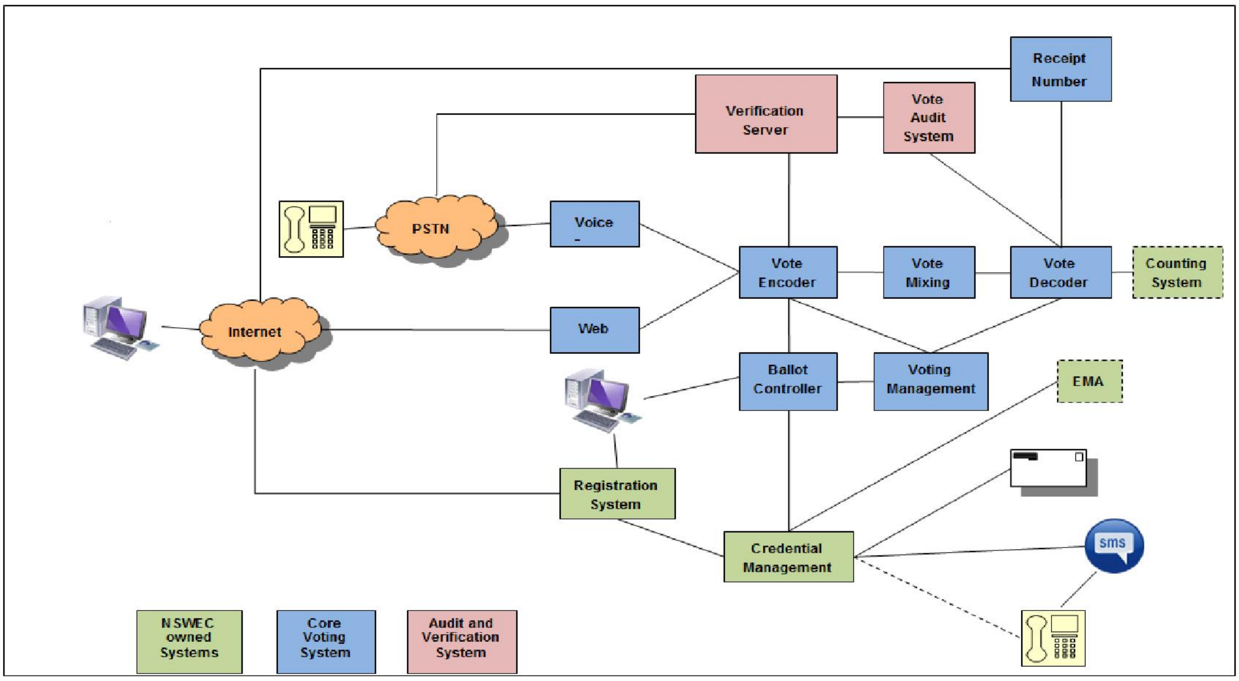
An introductory section is provided below to demonstrate the specific items provided by Scytl to the NSW Electoral Commission.

2 The iVote system and the iVote Core Voting System (iVote CVS)

The following diagram shows the iVote system as described in the iVote system description from the NSWEC website[1]. The iVote system comprises the iVote Core Voting System, the Audit and Verification system, and other NSW owned systems.

Scytl was responsible for supplying the iVote Core Voting System (the blue component in the diagram below) to the NSW Electoral Commission. Other items in the overall system were provided by the NSW Electoral Commission.

NSWEC was responsible for running the iVote system. Scytl supplied the application and consulting services to the NSWEC to implement the iVote CVS.



For further information regarding the iVote system, including the iVote CVS, Scytl recommends review of the extensive documentation available on the NSW Electoral Commission public website:

http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports

http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports/ivote_sge_2015_specifications

[1] http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/175758/iVote_System_Overview_v3.pdf

3 Allegations raised by Dr Teague and Professor Gore

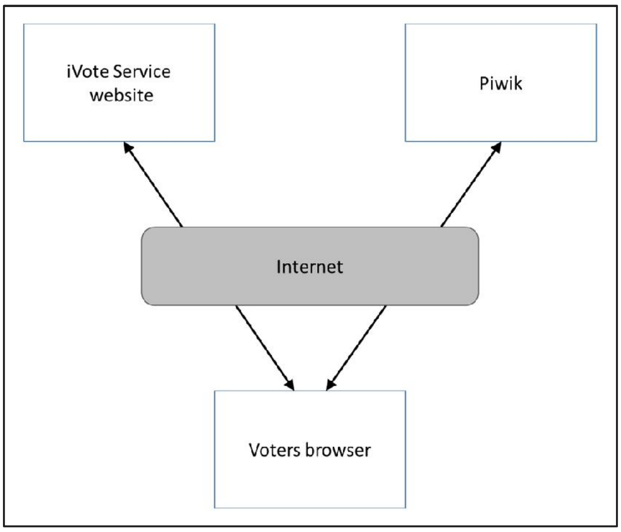
The following addresses allegations made by Dr Teague and Professor Gore in their submission to the Committee[2] and their testimony. Scytl has pulled out the allegations to which we believe the Committee is referring and respond individually.

3.1 Allegation - The specific security concern raised.

With reference to the paper that Dr Teague and Assoc. Professor Halderman released describing the specific vulnerability, Scytl understands this to be:

> *"…discovered a critical security flaw that would allow a network-based attacker to exploit the recently discovered FREAK attack to defeat TLS and inject malicious code into browsers during voting …"*[3]

It is important to understand that the issue was discovered in the network protocol used by the server that hosted the Piwik service, which was not one of the iVote servers, nor was it managed by the NSWEC for the internet voting system. The voting client, which runs in the voters web browser made a call to the Piwik Service, which loaded code from the Piwik service provider into the voters browser. The communications can be seen in the diagram below.



The issue identified by Teague and Halderman was only present in the Piwik application providers infrastructure, not the infrastructure of iVote or that under control of the NSWEC.

Exploiting the vulnerability

In order to exploit the vulnerability in the Piwik infrastructure, an attacker must insert himself into the communications path between the Voters Browser and the Piwik server, and exploit the bug in the https protocol. Possibilities to get into this communication path include:

- hijacking the local network connection of the voter (the coffee shop example)
- intercepting the communications of a router between the browser and the Piwik server
- having control of the Piwik server
- having control of the voting client within the voters browser

[2] https://www.parliament.nsw.gov.au/committees/DBAssets/InquirySubmission/Summary/48691/Submission 02 - Dr Teague and Prof Gore.PDF
[3] http://arxiv.org/abs/1504.05646

Once the attacker has access to the communication channel between Piwik and the voters browser, the exploitation of that vulnerability then requires that code is loaded into the voters browser to run in the background and vary the voters vote.

For this reason the attack is not considered straightforward to exploit and scale as it does not depend only on the Piwik vulnerability. If the exploit is tried in a coffee shop where a voter is using an unsecure network link (for example), the only voters intercepted are those within the coffee shop. In order to gain access to all votes as indicated by Teague and Halderman would have required the taking over of the infrastructure where Piwik is hosted, which would be expected to have triggered the detection systems within that environment.

Tricking the voter

Teague and Halderman went further to describe how the voter could go on to verify their vote from a fake verification service so that the voter believes their vote was successfully recorded.

In the event that a fake verification server was built, requiring a new phone number as it was accessed via telephone, and it was used, this would require a third successful exploit by the attacker in a limited period of time, without detection. This increases the complexity of the attack.

Detecting an exploit

The system was designed to provide for voter verifiability of their vote. This characteristic of verifiability allows the voter to confirm that their vote is stored correctly in the verification system. With reference to the diagram at the beginning of this document, the verification system is a NSW provided system.

In the event that a vote were modified via an exploit of the voters browser, as described by Teague and Halderman, the voters verification of this vote would make this clear to the voter as they would detect that their vote had changed.

The NSWEC have spoken to topic of feedback from voters verifying their vote.

In the event that the exploit of the code made by an attacker changes the vote that is stored in the verification server from that stored in the iVote CVS electronic ballot box, this would be detected both during the verification ceremony at the end of the election, showing an inconsistency in the contents of the two systems, as well as at the time of vote submission.

Summary and Recommendation

In summary the attack described by Teague and Halderman is a Man-in-the-middle attack. This form of attack was catered for in the design by providing the voter and the Electoral Commission with various tools to detect this form of attack.

Such an attack was not detected.

Scytl recommends the following to avoid this issue:

- That the option to verify a vote is more positively advertised to the voter
- The phone number and URL for the iVote service are recognisable and advertised in multiple locations so as to avoid them being unclear to the voter.

In response to the question by the Hon. Dr Peter Phelps: What level of technical sophistication would be required to do that? (Regarding the issue of exploiting the Piwik vulnerability), Scytl is of the view that this requires a high level of technical sophistication.

Whilst saying people who could do this Dr Teague has said this is a difficult attack to perform[4].

[4] http://www.abc.net.au/am/content/2015/s4202677.htm - “OCKENDEN: Ms Teague admits that it would be difficult for an attacker to perform, …”

3.2 Allegation – vote manipulation

"Successful manipulation of half that many votes would have altered the outcome of that seat." (Submission by Teague and Gore)

This argument is valid for any kind of election, including paper votes. The question is if there is any evidence that this happened and there is not.

There was a risk raised and it was mitigated quickly following notification, and there is no evidence that this was exploited, and no indications from the verification process between the iVote CVS and the Verification Server that any votes were tampered with.

In addition using the traditional method of comparing results from different voting channels within the elections, there is no evidence that this manipulation happened and to do this with 50% of the vote would be a significant undertaking to not be detected given the description in 3.1 above.

3.3 Allegation – difference between vote tallies

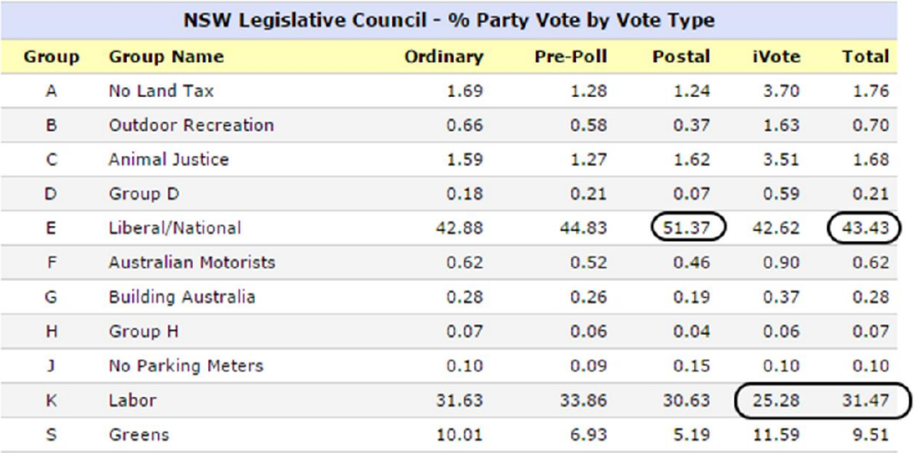
"Some first-preference NSW Legislative Council vote tallies produced by iVote differed notably from those received via paper-based methods." (Submission by Teague and Gore)

It is true that some first-preference vote tallies produced by iVote differed from those in paper based methods. As referenced by Teague and Halderman themselves from Antony Green's blog[5] this can be traced in some measure back to the donkey vote.

Regarding the difference of the Labor vote between iVote and overall result, the reference shows that it was 25.28% vs 31.47% respectively, a difference of slightly over 6 percent. However, in the case of Liberal/National, iVote showed 42.62% vs 43.43% showing a very high level of correlation with a variation less than 1%.

Interestingly, from the same table that was referenced by the researchers we can see that when comparing Labor vote between Postal vote and overall result, a difference of less than 1 percent can be seen. This is in stark contrast to the case of Liberal/National, where the postal vote showed a difference approaching 8 percent. This can be seen in the image below.

It appears that the submission by Teague and Halderman highlights a potential bias in the iVote system, and overlooks the same notion when referring to the postal voting system.



NSW Legislative Council - % Party Vote by Vote Type

Group	Group Name	Ordinary	Pre-Poll	Postal	iVote	Total
A	No Land Tax	1.69	1.28	1.24	3.70	1.76
B	Outdoor Recreation	0.66	0.58	0.37	1.63	0.70
C	Animal Justice	1.59	1.27	1.62	3.51	1.68
D	Group D	0.18	0.21	0.07	0.59	0.21
E	Liberal/National	42.88	44.83	51.37	42.62	43.43
F	Australian Motorists	0.62	0.52	0.46	0.90	0.62
G	Building Australia	0.28	0.26	0.19	0.37	0.28
H	Group H	0.07	0.06	0.04	0.06	0.07
J	No Parking Meters	0.10	0.09	0.15	0.10	0.10
K	Labor	31.63	33.86	30.63	25.28	31.47
S	Greens	10.01	6.93	5.19	11.59	9.51

[5] http://blogs.abc.net.au/antonygreen/2015/04/does-electronic-voting-increase-the-donkey-vote.html

3.4 Allegation – privacy breach

"But for this, all Internet votes would have been susceptible to manipulation and privacy breach" (Submission by Teague and Gore)

Privacy breach and integrity breach are a concern present in all elections and especially in remote voting, not only those delivered over the Internet.

Comparing Internet voting and postal voting (both remote voting channels), Scytl is of the view that Internet voting can provide better protection measures than postal. Postal votes are vulnerable to privacy and integrity attacks during delivery and reception as the paper envelopes provide a weak protection to these attacks. Internet votes can be encrypted and digitally signed with the voter device prior to leaving the device and cannot be open or manipulated during the delivery and storage in the servers without detection. iVote encrypts and digitally signs votes in the voter's computer so the content is not visible until the opening ceremony in front of the electoral officials who have the key to decrypt the votes whilst stripping any identifying material from them - thus providing more security protection than postal votes.

Scytl is of the view that susceptibility to attack is far different to actually having some form of manipulation happen and be undetected. It is the detection features of the iVote system that allow the operators to be confident that such an event did not occur.

3.5 Allegation – not as good as postal service

"At present no Internet voting solution exists that provides a degree of security and verifiability as good as postal voting for those who can fill in their own postal vote." (Submission by Teague and Gore)

From the point of view of verifiability, postal votes only allow the voter to be sure that the postal envelope they give to the postal service contains their voter intent, but following this there is no opportunity for further verifiability.

In general Voters cannot verify if their votes have reached the Electoral Commission, they cannot verify if their votes arrive on time for counting, they cannot verify if their votes are eliminated or modified during delivery and they cannot verify if they are placed into the ballot box in time.

Verifiable Internet voting systems can provide better verifiability measures than postal voting. They can allow voters to check if the vote they are casting contains the voter intention (cast-as-intended) and their votes are received and stored in the ballot box for counting (recorded-as-cast). iVote implemented a verification process (call by phone) that allowed voters to check that their votes were received by the Electoral Commission unaltered.

It is Scytl's view that the allegation is not correct and does not provide any accurate analysis that proves it.

3.6 Allegation – Disabled voters rights

"Disabled voters' democratic rights are not improved by providing an accessible remote voting solution that does not protect the integrity or privacy of their vote as well as alternative methods." (Submission by Teague and Gore)

As mentioned above, secure Internet voting systems can provide a higher level of privacy, integrity and verifiability than postal elections.

It is Scytl's view that it does not mean a step back for the democratic rights of this community but the contrary: these system improve accessibility compared to paper based options.