Scytl
Innovating Democracy

[redacted]

www.scytl.com

3 March 2020

Elspeth Dyer,
Committee Manager,
Legislative Assembly Committees
electoralmatters@parliament.nsw.gov.au

Re: Inquiry into the 2019 NSW state election
Response to questions on notice

Dear Ms. Dyer,

I thank the Committee for the opportunity to respond to these matters that arose during the recent public hearings for the Inquiry into the 2019 NSW state election.

In this document I will respond on the following topics, as requested by the Committee:

1. Responsible disclosure, update to opening statement.
2. The Hon. Ben Franklin: The NSW iVote protocol – review of vulnerability.
3. The Hon. Ben Franklin: Regarding Alerts in the event of compromise
4. The Hon. Ben Franklin: Regarding analogous discussion regarding internet voting and postal voting.
5. The Hon. Peter Primrose: Regarding "… whether or not you can give us, acting in that environment, a 100 per cent guarantee that vulnerabilities are not being caused to your system as a consequence of the Electoral Commission not being compliant with the New South Wales Government's own cybersecurity requirements."
6. Verification
    - How many people downloaded the verification app after using iVote
    - How many people attempted to verify their vote through the app?

I address the questions below, as well as through attachments to this document. Please contact me if any of this requires further clarification.

Yours Sincerely,

Sam Campbell,
Director, Scytl Australia Pty. Ltd.

1 Responsible disclosure

This is an update to my opening statement.

During my opening statement I discussed responsible disclosure and a little of the Scytl experience. I would like to update that statement with a correction. To date Scytl has had the following responsible disclosure events:

- Submissions to Scytl under the Swiss Post source code access program.
- Submissions to Scytl under the Swiss Post Public Intrusion Test (the PIT).
- A single submission to Scytl under the Scytl Online Voting Source Code Access Agreement for iVote in Australia. This was made by Associate Professor Teague.
- A single submission by a researcher made to Scytl during the NSW election 2019, where the researcher approached Scytl directly based on a finding in Switzerland to see if the finding was relevant for 'other deployments'. This was not under a formal responsible disclosure program, the disclosure was found to be not relevant to NSW, and was performed in a responsible manner by the discloser.

In the EU, The European Union Agency for Cybersecurity (ENISA) defines responsible disclosure as follows:

> *Security researchers should make reasonable effort to privately contact the vendor and give them the opportunity to diagnose and fix the problem before publicly disclosing it to the public. Diagnosing and fixing the issue might require extensive testing on behalf of the organisation/ company and several rounds of communication between the concerned parties. The timeline of the corrective measures need to be confirmed prior to disclosure, so that both parties coordinate their efforts and work as closely as possible for fixing the issue. Organisations/ companies are strongly advised to acknowledge the researchers' contribution and provide incentives to the researchers for following a responsible and coordinated disclosure.*[1]

In order for Scytl to be able to patch or mend a vulnerability found by a third party, Scytl needs time to evaluate the vulnerability to determine if it is in fact a vulnerability or not, and to then determine the impact of that vulnerability and an appropriate remedy. As the developer of Scytl Online Voting product, contained within iVote, Scytl is responsible for the development of patches.

The Australian Signals Directorate's (ASD) website articulates their policy on Responsible Release Principles for Cyber Security Vulnerabilities, and on this page eight essential principles are listed – with number one being "security first"[2].

By means of a responsible disclosure, patches and other mitigation measures are available before information on a vulnerability is made generally available to the public. In order to be able to develop a patch, or remedy, Scytl must first be informed of the vulnerability - for example by the person or group who believe that they have discovered that vulnerability.

By way of comparison, Google Project Zero (a programme for reporting vulnerabilities) has a 90-day disclosure deadline and their widely recognised policy is documented on their website[3].

1.1 Disclosures, timing, and iVote

Scytl notes the following timeline relating to disclosures related to the use of iVote:

- 11/3/2019: iVote goes live in NSW.

[1] hhttps://www.enisa.europa.eu/publications/info-notes/responsible-vulnerability-disclosure-and-response-matter, 2/March/2020
[2] https://www.asd.gov.au/publications/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities 2/March/2020
[3] https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html

- 12/3/2019: The paper “Trapdoor commitments in the SwissPost e-voting shuffle proof” by Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague, is published which describes an issue in the Swiss Post Scytl online voting system.

  This paper was forwarded prior to publication to Scytl by a customer, as no copy was sent directly to Scytl by the authors.

  Scytl analysis showed that this vulnerability existed in the NSW iVote system. Processes were in place however to restrict the ability to exploit the vulnerability to a trusted insider with broad system access and credentials[4]. Further the vulnerability existed in the offline mixing process (air-gapped system(s)) which is not utilised until the end of the election.

- 15/3/2019: Scytl delivered a patch to NSWEC to apply to the offline iVote systems to eliminate the vulnerability above.
- 23/3/2019: Election day
- 24/3/2019: NSWEC issued a press release, indicating that a further weakness identified by the researchers in the Swiss Post system is not relevant to the iVote system[5].
- 25/3/19: The researchers Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague published a second paper “How not to prove your election outcome”[6] detailing a further vulnerability claim. This is the vulnerability that the NSWEC press release (the previous day) referred to.

  This paper was forwarded prior to publication to Scytl by a customer, as no copy was sent directly to Scytl by the authors.

  Scytl analysis showed that the NSWEC iVote system was not vulnerable due to architectural differences between the NSW iVote system and the Swiss Post system that the researchers were unaware of.

  The vulnerability described would always be detected if exploited.

At no time during these events did the researchers communicate directly with Scytl about the matters above.

The following timeline relates to the disclosure under the iVote responsible disclosure program:

- 29/9/2019: Teague notified Scytl of an issue under the responsible disclosure program[7]
- 14/11/2019: 45 days elapsed since the submission
- 18/11/2019: First sitting of JSCEM hearing into the 2019 state election
- 24/11/2019: Scytl published response to the submission Scytl analysis showed that the issue could not be exploited without detection and was not scalable.

1.2 Source code access – iVote

The following data relates to the Scytl Online Voting Source Code Access programme in Australia:

- Number of applications to have access to the source code: 74
- Number rejected: 2 (the applicants are non-contactable)
- Number of reports provided to Scytl: 1 (the issue described above)

[4] https://elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSW-Electoral-Commission-iVote-and-Swiss-Post-e-vo
[5] https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSW-Electoral-Commission-iVote-and-Swiss-Post
[6] https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf
[7] https://people.eng.unimelb.edu.au/vjteague/iVoteDecryptionProofCheat.pdf

2 The NSW iVote protocol – review of vulnerability

In response to a request for further detail regarding a question from the Hon. Ben Franklin:

- That is where the cryptography comes in and it is around showing that the data in is effectively the data out, without tying it to an individual. When we reviewed the vulnerability that was found by these researchers, the New South Wales system was protected because of the offline presence of the mix-net. We have a paper that responds to how that works which we can make available…

The paper to which I was referring was the paper regarding how the offline mix-net relates to the vulnerability reported above on the 24/March (the day after the election) that was submitted again by Dr. Teague with additional details the October 14th through the iVote responsible disclosure program. The paper is attached as Addendum 1, and is available at: https://www.scytl.com/wp-content/uploads/2019/11/Scytl_response-_VT_NSW_iVote_Oct2019.pdf

3 Alerts in the event of compromise

In response to a request for further detail regarding a question from the Hon. Ben Franklin:

- There are other things that might trigger other alerts during the election. But, in effect, what happens when your ballot is cast is it goes into a secure ballot box and in that secure ballot box your ballot is signed and encrypted and the keys to decrypt that are shared between multiple people. That does not come together until the end of the election. That is something that we responded to in some detail in 2015. There is some documentation about that which we can supply.

The documentation I am referring to above is related to iVote 2015, however the concepts presented are similar between the two systems.

Firstly alerts, and responding on the concept of alerts during the election that the system may have been compromised: The iVote system by Scytl has a collection of cryptographic signatures and encryptions which trigger alerts in the event votes are compromised – from single votes to all those in the electronic ballot box. In addition to this there are various active monitoring points on the system specifically intended to detect attacks during system operation. It is the combination of these alerts which can be checked and monitored by operational staff in order to detect attacks on the system, both in real time and for later audit purposes – much like any other sophisticated computer application. Further detail is suppled in the relevant addendum and the following section.

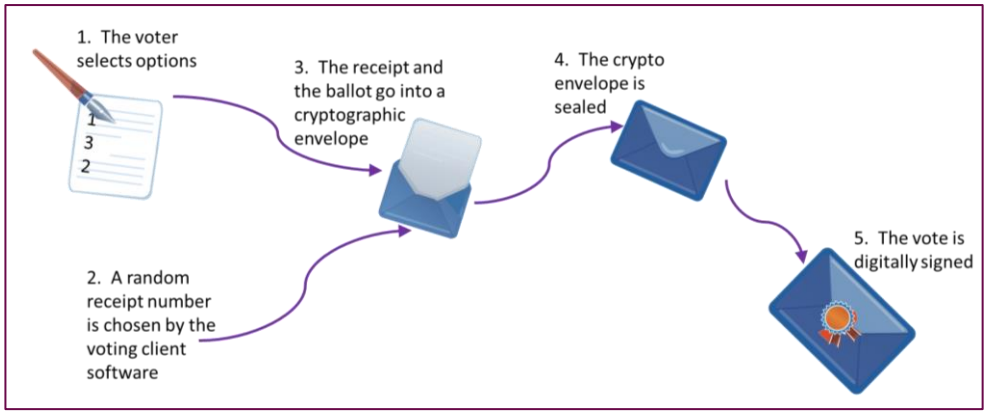
To address the next part of the question I will draw on information supplied in the document “Scytl Australia Pty. Ltd submission to support the Report on the iVote system, Conducted by Mr. Roger Wilkins AO, on behalf of the NSW Electoral Commission in response to the NSW Parliament's Joint Standing Committee on Electoral Matters report on the 2015 State election”, attached to this submission as Addendum 2. The text below has minor edits from the original.

3.1 How is a single ballot protected?

An electronic vote, in terms of the iVote CVS, is a populated electronic ballot paper which reflects the intentions of that voter.

Key information about an electronic vote is:

- The electronic vote is encrypted to the public key of the election – forming the digital envelope
- The digital envelope (containing the electronic vote) is signed by a private key allocated to the voter
- All this happens on the voters voting device, transparently to the voter, through the Scytl JavaScript voting client
- The signed digital envelope holds a discrete secure electronic vote for that specific individual.

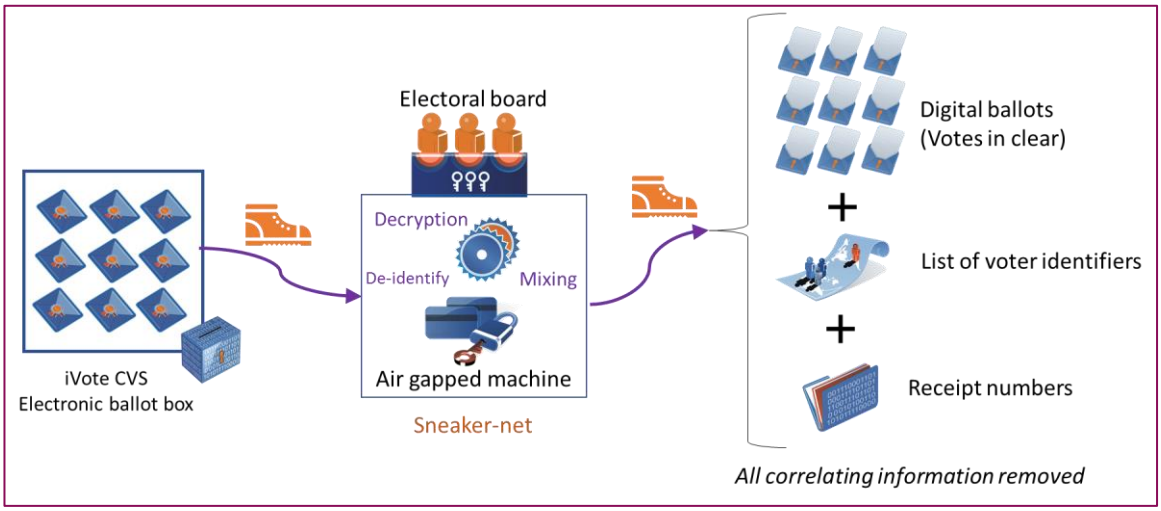


The key here is that every individual ballot is individually encrypted (for confidentiality) and signed (for integrity) within the voters voting device and is itself an identifiable piece of data. If for example a user's key is compromised (say by giving away her voting credential) this affects the one vote of the compromised voter – and not the votes of other voters as they are separately signed by different keys.

3.2 Decrypting the votes – preserving privacy

Also described in my evidence to the Committee was the concept of a single key split between multiple people. This is described here in more detail:

> At the end of the voting process, the election is closed and the iVote system stops receiving votes. The electronic ballot box is then transferred to air-gapped (offline) machine(s) where votes are anonymised using a mixing protocol and only then decrypted – refer to the image below. The purpose of the mixing protocol is to ensure that the ballots can be safely decrypted without compromising the privacy of voters. To achieve this, the correlation between the voter and their electronic ballot is removed.



- Ballot box integrity control: Each ballot is checked for authenticity by validating that their electronic signatures are valid. Ballots that fail are reported and isolated.
- Reconstruction of Election key: The election private key is reconstructed from the smartcards that hold the shares. To proceed, a quorum of the key components is required. Each of these key components is held by a different individual, such as the Electoral Commissioner and others appointed to this task.

- Ballot mixing: In 2015 valid electronic votes had their digital signatures detached. Then a shuffling process took place to randomise the order of the votes in the system – this removes any relationship to the voter based on the order of being read into computer memory and so forth. In the 2019 solution this shuffling process was replaced by a mix-net which cryptographically mixes the ballots, removes the voters identity, and shows mathematical proofs to demonstrate that the 'ballots in are the ballots out'
- Receipt number retrieval: The random receipt number is retrieved from each electronic vote for publishing following the election.
- Export of results: The results are then exported from the offline machine, and can be included in the count by the NSWEC.

This mixing of the ballot box assists with preserving the privacy of the individual voter by separating the vote from the individual's identifier.

The receipt numbers are then published to a receipt number lookup tool on the NSWEC website at the close of the election – this provides the voter with the ability to lookup their receipt number and gain comfort that their vote was successfully decrypted.

4 Discussion comparing postal ballot to internet ballot

In response to a request for further detail regarding a question from the Hon. Ben Franklin:

- I guess the contention from the evidence that we have heard from the last two sessions is that they are not analogous at all because with the postal vote system there are a range of individuals and every single vote goes through its own individual channel, whereas here everything goes through the same channel. Therefore the capacity for manipulation or for security breaches is apparent, is substantial, in their mind. That has been the evidence for the last two hours. I would be interested if you can dispel that for us so that we can be comfortable and confident in the software that you provide.

During the 2 hours of evidence preceding the Scytl session a number of areas were covered. I could not help but notice that we heard about the Canadian experience, however my takeaway from that section was about elections in which Scytl was not involved.

I was also reminded that a vulnerability must be exploitable before it becomes a weakness in a system – if a vulnerability cannot be exploited with any scale, and will be detected any time someone tries to exploit it, then the weakness presented is very low – and this is what we saw with events related to iVote.

Scytl believe that having governments run online voting systems, generally to collect ballots that would otherwise be postal or for voters with disabilities, allows not only the collection of those ballots – but does allow governments to build up a body of knowledge in their staff to be able to use and understand these systems when they need to.

Remote online voting (Internet voting) is a means of collecting remote ballots as opposed to ballots that can be captured in an attendance setting. It is the collection of remote ballots that has some inherent associated risks, as opposed to the collection of ballots in an attendance setting – in a polling booth. The Scytl Online Voting Software when used in the iVote system is not designed to completely solve risks associated with remote voting, although it has some features that enhance the ballot collection from standard postal voting.

Features of iVote that can enhance the confidence of a voter that their vote is counted is:

- The ability to verify their vote with the Verification App (nearly 50% of voters verified their vote)
- The ability to use the receipt number to validate that their vote was decrypted at the end of the election and included into the count.

So from a voter perspective there are features that cannot be evident in a postal voting system to enhance the voter's confidence. This is known as individual verifiability in the industry.

Similarly there are technical features that the Electoral Commission can use to ensure the anonymity of the voter is preserved, such as the mix-net which mixes the votes, whilst simultaneously separating the votes from the voters identification and generating a mathematical proof that that has been performed accurately. This is the universal verifiability property of the system.

"… its own individual channel, whereas here everything goes through the same channel…"

Scytl sees that this part of the questions can be seen in two ways – within which of the two systems does 'everything go through the same channel'? The internet is an interconnected network of computers through which a vote passes to be stored in a digital ballot box. Depending on the source of the vote (ie: where the voter connects to the internet) there are a myriad of paths through which the vote could travel before it comes to the central server. This is very similar to the postal network – depending on which post box the voter places his postal ballot in, there are a myriad of ways the ballot can get back to the electoral commission for opening.

- Some parallels:
  - Both networks converge to a central point
  - Both networks have the feature that someone could intercept the ballot (however this can only be detected in iVote)
  - The voters ballot is placed into an envelope (paper and glue or cryptographic)
  - The envelope is signed by the voter (handwriting or cryptographic)
- Some differences:
  - In postal voting:
    - the vote is protected with a paper envelope, offering a low level of protection
    - the voters envelope is signed with a handwritten signature
    - if the postal worker intercepts a ballot they can potentially read and/or change the content with little chance the voter will discover this
    - there are a large number of actors involved allowing bad actors access to the process, with low oversight of an individuals actions
  - In iVote:
    - the vote is protected by high security encryption, offering a high level of protection
    - the vote is signed by a voters digital signature which is extremely difficult to forge
    - if an attacker on the network intercepts a ballot they cannot read the content, and if they prevent the vote from getting to the server, the voter will be able to detect this.
    - there are a small number of players involved allowing oversight across individuals involved in the process
    - the systems support controls which record evidence of actions by operators

In Austria in 2016, "Austria […] delayed a re-run of a presidential election as faulty glue on postal ballots […] The result of the first election in May […] had already been scrapped due to irregularities in counting the postal ballots"[8].

[8] https://www.reuters.com/article/us-austria-election/austrian-election-re-run-comes-unstuck-in-postal-ballot-setback-idUSKCN11I0NA 2/March/2018

A challenge Scytl faces, along with other proponents of electronic voting systems, is the ease with which 'the postal ballot system' is understood both by the person in the street and the policy maker. In general the person in the street can understand the risks of postal voting.

Online voting, such as with iVote, is difficult to understand for anyone who does not have advanced knowledge about computer engineering, cryptography and other advanced concepts – this is why Scytl has invested heavily in the cryptographic basis of the product and the logging features. It is these features that are intended to build a product that stands up to scrutiny from others who can then act as a proxy to the general publics need for confidence.

Online voting systems such as iVote are not designed to be a replacement to an attendance voting system using a public ballot box, but they are designed to supplement and potentially replace a postal voting system by increasing the accessibility for remote voters.

5 A 100% Guarantee

In response to a question from The Hon. Peter Primrose:

- Regarding "… whether or not you can give us, acting in that environment, a 100 per cent guarantee that vulnerabilities are not being caused to your system as a consequence of the Electoral Commission not being compliant with the New South Wales Government's own cybersecurity requirements."

Scytl is not aware of any specific detail relating to the level of compliance of the NSW Electoral Commission, further than the statement quoted by Mr. Primrose. Scytl is however aware that a Government departments IT systems are many and varied - in the case of the NSW Electoral Commission these will cover staff desktops, electoral systems, finance systems, and other systems including the iVote system. When a department is not compliant, say for example with the 'New South Wales Governments cybersecurity requirements', it is not necessarily evident that all systems are not compliant, simply that there is some non-compliance.

The level of compliance with the New South Wales Governments cybersecurity requirements is a question for the Commission.

That said, there is evidence on the NSWEC website that audits and security related activities were performed against the iVote environment – refer initially to the report of Price Waterhouse Coopers available on the NSWEC website:

> https://www.elections.nsw.gov.au/getmedia/b2280c43-a129-47ca-bd75-f9c98887736b/2019-State-Elections-iVote-review-(post-election-report)-June-17-2019-redactions-v2-3-draft-Copy_Redacted(1)

Scytl does not give a "100 per cent guarantee" that vulnerabilities do not exist – in our software, or in the support infrastructure provided by others and so on – what we do provide is software that has been extensively tested over many years that continues be researched and enhanced to improve and to be able to make attempts to exploit the software apparent to observers using many defensive techniques – defense in depth if you will. This is much like the postal voting system, attendance voting situations, and management of the extensive operations that go into electoral management. Further the software includes verifiability processes as previously described to show that ballots are not tampered with.

When the iVote system makes available information to indicate some unexpected activity, extensive audit logs are in place to allow investigators to look into what may have gone wrong – this allows the Commission to make decisions, or recommendations, as the case may be. Not unlike other systems in use during elections.

6 Verification

In response to requests for further detail regarding:

- How many people downloaded the verification app after using iVote
- How many people attempted to verify their vote through the app

Scytl refers the Committee to please take this question up with the NSW Electoral Commission as the Verification App was made available through the Google store and the Apple App store through the NSW Electoral Commission account. As such Scytl does not have access to this information.

-- Document ends --