

## **INQUIRY INTO THE 2015 NSW STATE ELECTION**

**Organisation:** ScytI Australia Pty Ltd  
**Name:** Mr Sam Campbell  
**Position:** Director  
**Date Received:** 23/08/2015



**ScytI Australia Pty. Ltd.**

Submission to the

**Joint Standing Committee on Electoral Matters**

for the

**Inquiry into the 2015 NSW state election**

This submission is made on behalf of ScytI Australia Pty. Ltd.,  
a wholly owned subsidiary of ScytI Secure Electronic Voting S.A.  
PO Box 7529,  
Baulkham Hills,  
NSW 2153

Sam Campbell  
Director, ScytI Australia Pty. Ltd.  
20 / August / 2015

## 1 Introduction

ScytI Australia Pty. Ltd. is pleased to make this submission to the Parliament of New South Wales Joint Standing Committee on Electoral Matters for the purposes of its 'Inquiry into the 2015 NSW state election'. This submission is primarily directed at (b) The administration of and practices associated with the electoral laws.

This submission will cover the following topics:

- An overview of ScytI – who we are
- Overview of the iVote project
- iVote during the election
- Other matters
- Conclusion

Further to this written submission, ScytI will be pleased to respond to any questions the Committee may raise during its enquiry, either to explain this submission further or to respond to other matters as they arise.

## 2 ScytI Overview

### *ScytI background*

ScytI is the global leader in secure election modernisation solutions. ScytI has capitalised on over 18 years of research to develop election-specific cryptographic security technology. ScytI's solutions have been successfully used in over 20 countries throughout the world over the last 10 years, including Canada, the United States, Mexico, Ecuador, France, Norway, Switzerland, Bosnia-Herzegovina, the UAE, South Africa, India and Australia. ScytI is headquartered in Barcelona, Spain with strategic offices in Canada, the United States, Peru, Greece and Australia as well as many additional field offices.

ScytI was formed as a spin-off from a leading research group at the Universitat Autònoma de Barcelona (Spain). This group, funded by the Spanish Government's Ministry of Science and Technology, has pioneered the research on e-voting security in Europe since 1994 and has produced significant scientific results, including over 30 scientific papers published in international journals, as well as the first two European Ph.D. theses on electronic voting security, by Prof. Joan Borrell and ScytI's founder Dr. Andreu Riera (in 1996 and 1999, respectively). This research group also participated in the first Internet binding election in Europe (i.e., the 1997 election to the Presidency of the IEEE IT Spanish chapter).

One of ScytI's key differentiators is its unique election security technology, which derives from over eighteen years of pioneering R&D and is protected by a portfolio of international patents. The e-voting cryptographic protocols developed by ScytI provide elections with the highest levels of security, in terms of voter privacy, ballot box integrity, and voter-verifiability. ScytI's solutions can also address

specific needs of disabled citizens and enable them to participate in elections without any assistance, completely guaranteeing their privacy.

ScytI has customers both in the public and private sectors. The former are local, State (regional), and federal governments which licence ScytI's e-voting products to securely carry out their elections, referenda, voter registration and other electoral modernisation processes by appropriate use of technology. The latter are large corporations and organizations that choose ScytI's technology to carry out electoral/consultation processes such as labour union elections or shareholders' meetings. Some of these customers represent leading references in the electoral modernisation field (e.g., governments in Australia, United States, United Kingdom, France, Austria, Switzerland, Spain, Finland, Norway, and more).

### ***ScytI around the world***

ScytI has run numerous projects around the world where its customers are looking to modernise their electoral processes, as shown in the figure below, some of which represent breakthrough projects for the electoral modernisation industry.



ScytI has a strong internal focus on ground breaking research efforts, which is accompanied by a view to assist its customers modernise the electoral process through the appropriate use of technology.

ScytI has used its skills, tools and capabilities to assist the NSW Electoral Commission to deliver the iVote project, and the world's largest Government internet delivered binding election.

### 3 iVote Project overview

#### *The iVote system*

The iVote system was used to collect over 280,000 electronic ballots from voters during the 2015 state general election. The iVote system collected votes securely from the voters device (laptop, mobile, tablet, telephone) and transmitted them via the internet to the NSW hosted electronic ballot box. The voters had the option of verifying their votes within the system to ensure their intention is properly recorded in the vote (Cast-as-Intended). The voter could then validate that their vote was decrypted by the system.

The iVote system comprises a number of components, including the Registration System, Audit and Verification Systems and the iVote Core Voting System (the iVoteCVS). ScytI was contracted by the NSW Electoral Commission (NSWEC) to produce the iVoteCVS, the component of the iVote system concerned primarily with the following functions:

- Collection of the vote (web, mobile and IVR interface)
- Storage of the vote
- 'Mixing' of the vote
- Decryption of the vote
- Publishing of the vote to NSWEC business systems
- Publishing of the vote receipt numbers

An overview of the system is available on the NSWEC website. Key components were produced by different suppliers contracted to the NSWEC – from the non iVoteCVS components of the voting system, to infrastructure, to audit, to threat assessment and system integration with the NSWEC providing the system architecture and the project 'glue' in the middle.

#### *The Project*

The production of the iVoteCVS component of the voting system was completed by ScytI's development labs based in Spain, using ScytI's e-voting cryptographic framework as the foundation of the cryptographic parts of the iVoteCVS technologies where possible, and developing new specific parts to meet the design requested by NSWEC. The protocol to protect the vote within the browser, including protecting the privacy of the voter and associated features, is the leading edge in security for electronic ballot technology at the time of its implementation.

The iVoteCVS system was delivered to NSWEC who conducted audits through independent groups, as well as extensive usability and functionality testing, leveraging the specialist capabilities of groups in differing areas of the system. An example of this is the use of blind testers to ensure that the user interface best meets their requirements, whilst still meeting ScytI technical requirements for security and NSWEC requirements for a voting system.

The iVoteCVS was operated by NSWEC agents, with support and review of alerts supplied by ScytI amongst others during the election period.

### ***Facts and Figures***

The iVote system was operational for the early voting period, as well as part of Election Day – the 16<sup>th</sup> March 2015 to the 28<sup>th</sup> March 2015.

- Number of valid votes collected by the iVote system: 283,669 votes
- Voting channels available: Internet and IVR
- Highest number of votes taken in one day: > 50,000
- The day with the highest number of votes: Friday 27<sup>th</sup> March (the day prior to Election Day)
- Valid voter groups:
  - The Visually impaired
  - Those with a disability
  - Those who live in remote locations; or
  - Those who are going to be outside NSW on Election Day.
- ~97% of users voted 'Very Satisfied' or 'Fairly Satisfied' on their experience with iVote

## **4 During the election**

ScytI supported the NSWEC operation of the system throughout the electoral period. The NSWEC ran various monitoring systems itself and through partners to maintain a view on the operation of the environment. During the voting period the iVoteCVS remained operational and responsive to voter interactions, with the exception of two brief outages.

### ***Outage 1 – ATL boxes.***

It was found that there was an error in the display of the ballot paper on the iVoteCVS website, the error being that two columns were missing the Above the Line (ATL) boxes at the top of those columns. The error was the result of an incorrect configuration file (EML datafile) being used as the configuration for the election. The EML datafile comes from the NSWEC EMA system which is not part of the iVote system.

Upon notification of the error by NSWEC, ScytI was able to analyse the problem and recommend to the NSWEC a remediation plan. This remediation plan was tested extensively on a separate system to validate that the change could be made simply and did not introduce any issues. Following that the plan was reviewed by NSWEC specialists and management, who then approved and implemented it.

Whilst an unfortunate error, it is ScytI's understanding from observing the electoral process among differing electoral bodies, that the issue of incorrect ballot papers is not particularly unusual. In the case of a standard paper ballot, when there is an error on the paper, it is usual to destroy the affected ballot papers, leading to reprints and potentially significant delays.

### *Outage 2 – Piwik.*

There was a second outage, as a result of a perceived threat found in the Piwik service, a service chosen by NSWEC and integrated into the iVote system as an external component for another supplier for the purpose of understanding such things as system response times, client browser devices and compatibility issues. During the voting process ScytI was made aware by the NSWEC that they had been advised there was a vulnerability in the Piwik service, and that this should be de-commissioned from the production iVote site. Because of this vulnerability it was understood that there was the possibility to attack the iVoteCVS component of the voting system.

ScytI and others assisted NSWEC to analyse the problem and recommended to the NSWEC a plan for the deactivation of the service, which was trivial as it was a 'Yes / No' configuration control. The plan for the de-commissioning of the service was then reviewed by NSWEC specialists and management, who then approved and implemented the plan.

The perceived threat was reported in the press on Saturday evening by two presenters who were travelling Victoria and the ACT giving lectures on electronic voting. The presenters at no stage communicated with ScytI directly, although ScytI was a subject of their lectures in Melbourne and Canberra. Further it is understood that at no stage did the presenters communicate directly with the NSWEC prior to the release of the information to the media. In ScytI's view the threat was over-stated by the presenters. The view presented to the media, and in the presentation that they gave in Canberra, was that this was a critical threat allowing the modification to all votes prior to the removal of the vulnerability. ScytI's analysis was that the Piwik threat was present, but a difficult to exploit Man-in-the-Middle (MITM) attack that will allow the remote control of the voter's terminal (Internet browser), meaning that in order to exploit the vulnerability the attacker must also get into the communication path between the voter and the voting server. Whilst the first threat was present, the second threat was based on speculations about probabilities that communication infrastructure components could be compromised.

This is akin to a hostile postman taking a letter and varying its content, in other words it affects only the vote attacked, and not the wider population of votes collected. As the election is open for postal voting this is an inherent existing risk, and broadly understood by the teams operating the environment.

In any case, it is important to note that the iVote system was designed to consider the possibility of an attacker taking control of the voter terminal. A mechanism is implemented to allow voters to detect any attack in the voter's computer that affects the integrity of their votes. This is implemented in the iVote system by a voter verification mechanism that allows voters to check if their votes are stored in the ballot box, and further that the stored vote contains exactly the same selections made by the voter. More concretely the system allowed:

- Voters to validate the contents of his/her cast vote
- Election managers to cancel voter credentials and allow voters to re-cast his/her vote.

This mechanism will allow a voter to detect any manipulation of his/her vote, notify this information to election officials, cancel their credentials and cast a new vote.

## 5 Other matters

### *Council elections.*

ScytI believes that the take-up in use of the iVote system reflects people's desire for convenience and ease of use when interacting with Government. ScytI recognises and acknowledges the cultural activities associated with Election Day, however this should also be balanced by the competing need for Government to make services available to citizens, especially those who have difficulty using the services as they stand such as travellers and the visually impaired.

When reviewing the process around Council Elections in NSW, and other areas of Australia, the ballot is held largely by postal vote. The postal ballot system, being intrinsically linked to the future of Australia Post, is an area that is worthy of investigation, and the continuing reliance of the NSW Electoral system on the postal system appears likely to come to a head in the not too distant future. A recommendation by ScytI to the Victorian Local Government Electoral Review was based on statements by the Australia Post Chief Executive reported in an article where it is stated that "Australia Post will introduce a second-class delivery system as it grapples with a worsening slump in volumes and raises its rhetoric seeking government help to maintain regular services<sup>1</sup>", and we believe that position remains valid.

Further, based on strong support from disability groups in the past, and feedback gleaned from feedback in this election, ScytI is of the view that to leave iVote out of the Council elections will reduce the available palatable options for that sector of the community.

The iVote system is perfectly placed to assist the NSW Government in supporting the running of the polls in upcoming Local Government elections.

### *The cost of running elections.*

Elections are intrinsically expensive events to stage, and have been reported by the AEC in the Commissioners review of 2013 as "... described as Australia's largest peacetime event, an election covers a vast array of complex and interdependent activities...<sup>2</sup>". The scale of an AEC election exceeds that of the NSWEC, however the underlying principles are very similar. There are numerous logistical hurdles to overcome, and those hurdles are linked to collecting the electoral intention from specific individual voters, whilst maintaining a voters right to privacy and to freely choose.

For those voters who cannot, for whatever reason, attend a ballot box present a situation to an electoral commission where the votes are difficult to collect and become expensive in the context of the rest of the election. Appropriate use of scalable technology to assist in these particularly difficult

---

<sup>1</sup> <http://www.smh.com.au/business/australia-post-says-letters-business-failing-20140509-38109.html>

<sup>2</sup> <http://annualreport.aec.gov.au/2013/contents/files/1-review.pdf>



areas, can be used to address these cost concerns – and a key criteria is usage – the return on investment for a system is usually improved significantly when the use of that system is extended. By increasing the number of votes collected by the iVote system to in excess of 280,000 ScytI expects that the state of NSW has returned increased value from their investment – an investment in a system that can be re-used for future elections.

### ***Outcomes.***

ScytI was pleased to observe analysis by NSWEC that showed comparisons of the iVote system and its usage against the more traditional vote collection mechanisms. A satisfaction rate of 97% for a public service is extremely satisfying for those on the project who worked to make it successful.

### ***Data Analysis.***

Analysis of data has also shown a high level of correlation between data on the traditional voting channels, and the data related to the iVote system. Where there is a deviation this can lead to discussion to understand why this variation is seen, and secondly to indicate whether there are any issues with the iVote system itself.

Analysis by Antony Green (Australian Broadcasting Commission) found a detectable bias<sup>3</sup> that is based on screen layout of the large NSW ballot paper. This sort of detailed analysis brings strength to the iVote system as it provides data upon which to tune the system and enhance it for future operation.

In a similar vein, such analysis may uncover nefarious activity within the system – and such activity has not been detected to our knowledge.

### ***Responsible disclosure***

'Outage 2 – Piwik' was a security related matter that was discovered during the running of the election. This matter was known initially to the presenters who discovered the vulnerability, and those with whom they shared it. As mentioned earlier the presenters at no stage communicated directly with ScytI or the NSWEC.

In keeping NSWEC and its providers (Piwik and ScytI) away from the knowledge of the potential security issue that could affect the iVote system, and at the same time making this information available to others, the presenters withheld the ability to mitigate or solve the issue in the quickest possible time. This action by the presenters is contrary to the usual approach followed by academics when discovering computer related vulnerabilities, which consists of contacting the owners of the vulnerable systems prior to disclosure to others. [REDACTED]

[REDACTED]

---

<sup>3</sup> <http://blogs.abc.net.au/antonygreen/2015/04/does-electronic-voting-increase-the-donkey-vote.html>

### ***Academics, Researchers and Activists.***

ScytI is a company open to careful and educated review of its systems by others. ScytI participates actively in the academic research on security mechanisms for electronic voting and have several publications about their cryptographic protocols and security mechanisms implemented in its solutions.

How the systems are made available for review is determined on a case by case basis in conjunction with our Customers. ScytI believes that responsible disclosure, and the active support of that activity, is a necessary part of building strong, resilient, secure software. Researchers at ScytI carefully follow this principal when detecting security issues on non-ScytI systems.

ScytI employs a number of active Researchers in its R&D department based in Barcelona, Spain. Amongst their number are the authors of many published works related to cryptography and its use when related to online elections, as well as extensive research into electronic voting protocols as well as application in other areas of the electoral process. ScytI also supports academic researchers who join with the company in a partnership to extend knowledge in this area. We meet with those with differing views and encourage robust academic debate.

During the running of the 2015 NSW state general election two presenters, one from the University of Melbourne and one from the University of Michigan, gave presentations in Canberra and Melbourne. Their presentations indicated that they would be investigating the NSW iVote system. As far as we are aware there was no attempt by the presenters to advise ScytI that they were interested in formally reviewing the system, even though one of the presenters had previously performed a high level review of the ScytI system in use in Victoria. The two presenters are associated with a group named 'Verified Voting' and have previously been involved with media based activity during electoral events.

ScytI would like to encourage research done into Internet and Electronic Voting as this is a dynamic environment where the technology is under constant improvement.

## **6 Conclusion**

ScytI is proud to have worked with the NSW Electoral Commission and its partners for the delivery of the iVote system. ScytI believe that the close working relationship formed between the Commission and its suppliers assisted in bringing the project to the successful culmination that we have seen. Based on ScytI knowledge of elections conducted over the internet, ScytI have stated that the NSW State General Election in 2015 is the world's largest binding government election to date. This allowed the collection of votes from electors who would otherwise have struggled to meet their legislated requirement of casting a ballot in a secure manner. ScytI looks forward to its ongoing relationship with the NSW Electoral Commission and looks forward to seeing how this technology investment by the NSW Government can be leveraged by others.