Preface

This is a submission to the Joint Investigatory Committee with regard to Electronic Voting in Victoria. I make reference specifically to the second term of reference: alternatives that are available that if implemented would ensure the continued integrity and security of the system. This submission aims to outline the risks of electronic voting if implemented as the primary means of casting a ballot. This submission will ignore the social impacts of electronic voting, and focus exclusively on the security risks inherent in electronic voting.

Part 1: Introduction

1.1 Paper-based voting has been used for centuries as the primary means of voting. In 1856, Victoria becomes the first democracy in the world to employ a secret ballot[1] to ensure that electors are anonymous and can vote without fear of retribution on the basis of their political preferences.

1.2 It goes without saying that anonymity is a key part of the election process to ensure a fair and balanced outcome. However, another key aspect of free and fair election is trust which exists on two levels.

- 1.2.1 There must be sufficient checks and balances in place during the administration and counting of the election because it is not permissible to trust any one person.
- 1.2.2 The general public must be able to trust that the result is correct.

1.3 The paper-based system achieves the goals of anonymity and trust, due to the ability for it to be open to scrutiny. Part of this submission will outline the impracticality of scrutinising an electronic platform.

1.4 In this submission, I will be outlining flaws with the two most prevalent forms of electronic voting available today: DRE voting systems and web- based voting systems.

- 1.4.1 A DRE voting system is a physical computer network established at a designated polling place.
- 1.4.2 A web-based voting system is a secure website established to allow electors to vote from home on their own electronic devices.

Part 2: Security Concerns (Overview)

2.1 There are many threats to an electronic voting system if the attacker merely seeks to disrupt the election process.

[1] Victorian Electoral Commission, *Electoral Events* (26 May 2014) <https://www.vec.vic.gov.au/Results/results-historical-vicevents.html>

2.2 Students in a graduate computer science course at Rice University in Texas examined ways to subtly affect the outcome of an electronic polling system.[2] There were 4 main methods the students used to compromise the integrity of the units.

2.2.1 Result manipulation[3] – elements of the code were altered to skew the results in favour of a particular outcome.

2.2.2 Broken authentication[4] – the system employed by the software had a mechanism by which a voter would identify themselves using a unique PIN number which would only be valid for a limited time. These hacks allowed certain PIN numbers to vote multiple times without alerting the administrator's terminal.

2.2.3 Violating anonymity[5] – this hack involved either attaching an identifying feature to a ballot, or removing the randomisation of ballots (so the time the vote was cast could be determined) to ensure that the person who cast the ballot could be identified.

2.2.4 Denial of service[6] – these bugs were designed merely to disrupt the voting process, but could still have real world implications if affecting electorates known to vote a certain way. These hacks sought mainly to crash the terminal, or allow any user to finalise the election results at any time.

2.3 Another part of the *Hack-a-Vote* project by the students of Rice University was to then audit another group's work. Every auditing group missed at least one flaw in the system. This was based on students given one week to analyse software with 2,000 lines of code. Estimates for real-world software would consist of approximately 50,000 lines of code.

Part 3: Security Concerns – Voting Software

3.1 Regardless of whether the software is implemented on a website for electors to vote at home, or onto a voting machine at a polling place, there are several concerns.

3.2 One concern is in the writing of the software. If the software is made by one team, this reduces the prevalence of errors but increases the risk of bribery, threats or corruption as only a small group has to be targeted. Alternatively, if it is created by multiple teams and firms, the source code can no longer be classified as secret and the lack of communication between the writers would greatly increase the risk of errors in the code.

3.3 Another concern is the verification of the software. As listed at *1.2.1* of this submission, the public is entitled to hold no absolute trust in the process, thus the election process must be open to facilitate trust.

[2] Jonathan Bannet et al, *Hack-a-Vote: Demonstrating Security Issues with Electronic Voting Systems* (2003) < https://www.cs.rice.edu/~dwallach/pub/hackavote2003tr.pdf>
[3] Ibid at [4.1]
[4] Ibid at [4.2]
[5] Ibid at [4.3]
[6] Ibid at [4.4]

3.3.1 The software can then consist of being either open-source, where everybody can look at it (including potential attackers), or proprietary and secret, where only selected people can examine the software and the public at large just has to trust that what they input on the screen is what the machine records.

3.3.2 The Federal Constitutional Court in Germany ruled in 2009 that the result of the election must be verifiable without any specialist knowledge in the subject.

3.4 How do we enable verification of the correct ballot? How does a voter know that what they've voted for is the final result? We have already established that it is not good enough to merely 'trust' the process, but in order for a voter to check their e-vote, an identifying feature would have to be included, removing the concept of anonymity from the process.

3.5 How is the software tested? Technology progresses at an alarming rate, meaning that it is likely new software would need to be implemented at every election (every 4 years). A full-scale implementation only occurs during an election due to the sheer volume of end users. It is not possible to run a full scale test which simulates election conditions prior, meaning any flaws in the software will only be detected after a problem has occurred.

3.6 The final issue here is the auditing of the software. How do we know that the software that was implemented in the solution is the one still there at the end of voting? When do we check the software? And if a discrepancy is found, is all polling data taken using the compromised software discarded or is it still counted?

Part 4: Security Concerns – Web Based Voting Systems

4.1 This model implies that the electoral commission charged with collecting voting data implements a secure website where electors cast their ballots from their own devices.

4.2 The only feasible way for the data to be transmitted to the final count using this method is via the internet.

4.3 The most common attack vector would be a *man-in-the-middle* (MitM) attack. This involves a hacker altering the connection between the voter's device and the electoral commission's server to first pass through their system. From here, the hacker can relay only the information they want seen through to the electoral commission.

4.3.1 While it may seem like a lot of effort to intercept one machine, consider if such an attack was implemented at an internet café, public WiFi hotspot or even the connection between an Internet Service Provider who is relaying all the votes from their customers to the electoral commission. One attack may impact many votes.

4.4 Another way by which web-based voting is vulnerable is that any code uploaded to a website is open-source; a possible attacker can see the 'blueprint' for what they are trying to compromise. This makes a prospective hacker's job easier in planning an attack to the system.

4.5 In allowing people to use their own devices, the ability to verify the integrity of the device is lost. A highly conservative estimate by internet security company *Kaspersky*

puts the number of infected devices at 1 in 20.[7] Some estimates go as high as 48% (almost 1 in 2).

4.6 Another issue with web-based voting is that it opens the door to attacks to come from outside Australia. The only method we have to prevent this is IP Address logging, which firstly damages the anonymity of the vote, and secondly, can be easily defeated through the use of a Virtual Private Network (VPN) or Proxy Server.

Part 5: Security Concerns – Direct Recording Electronic (DRE) Voting Systems

5.1 This model implies a custom built electronic voting network, implemented at polling places.

5.2 Notwithstanding the concerns raised in *Part 3* of this submission, there are several concerns which apply to the use of DRE voting systems.

5.3 How can we be sure that the software developed for the DRE machines is the software actually loaded onto it? If the machine is a sealed unit, the software cannot be verified throughout the day, meaning the voter must simply trust the software. If the machine has accessible ports to allow maintenance and verification during polling, the software may be compromised by an attacker installing their own software using that point of ingress.

5.3.1 Using encryption techniques, hashes or checksums as a form of 'electronic seal' does not greatly mitigate this risk, as we merely move the issue from the voting software being legitimate to the verification software being legitimate.

5.4 How are the votes stored and returned to the central count? The following outlines the different methods and their flaws:

5.4.1 A sealed unit has a storage device built inside which has saved all the voting data to it. The machine is sealed in plastic and transported to the final count.
FLAW: Notwithstanding the machine verification and trust issues, the logistics of transporting all of these machines from their respective voting centres would be costly and complex.

5.4.2 Download the voting data onto a portable storage device (such as a USB stick or SD card) and transport that to the count.
FLAW: By having an external port on the voting machine, we have provided a means of ingress for an attacker to compromise the software on the machine (see *5.3*). Furthermore, if that device is damaged during transport, the voting data is lost and these votes cannot be counted.

5.4.2.1 Redundancy mechanisms to ensure damaged storage devices do not compromise the vote (such as RAID arrays) amplify the cost and increase the complexity of verifying the count.

5.4.3 At the closing of the polls, the machines are instructed to upload the voting data and transmit them over the internet.

[7] Eugine Kaspersky, *One in twenty is the sad truth* (25 March 2013) < https://eugene.kaspersky.com/2013/03/25/one-in-twenty-is-the-sad-truth/>

FLAW: Notwithstanding MitM attacks (see *4.3*), there is no modern standard of encryption that theoretically cannot be breached. Furthermore, by networking a machine to the internet at large, the possibility of Denial of Service (DoS) attacks has arisen.

5.4.3.1 As the government does not own or operate a state-wide telecommunications network, any data transmitted has to pass through a 3rd party Internet Service Provider (ISP), which breaks the custody of the data from the electoral commission to the corporation which may have its own political interests.

5.4.4 After every vote, a paper copy is generated via a printer built into the machine with details of the vote.

FLAW: Firstly, this damages anonymity of the vote as we have an order of votes cast and details of how the vote was cast. Not to mention that using this solution, we have now returned to a paper-based system as is currently in place now. Also, compromised software may alter what is printed on the paper.

5.5 Assume the current process of phoning the Returning Officer with the count before transmitting the votes via one of the methods above is still enabled. The physical count will only be rendered to the polling place administrator as a variable stored by the software, which may have been altered by compromised software.

Part 6: Central Returns Server

6.1 This device is the server which will invariably receive the details of the count from all polling places and possibly verify that the votes have not been compromised (if verification is possible).

6.2 If this server receives the information from internet based uploads, it may be susceptible to a Denial of Service attack.

6.3 This server faces the same verification issues outlined in *Part 3* of this submission.

Part 7: Summary and Conclusion

7.1 By implementing electronic voting as a primary means of voting, the essential elements of democratic voting are lost. Trust and anonymity are both at stake. This system asks the general public to trust that the machine is coded correctly, trust that it is audited frequently and expertly and trust that human error does not occur.

7.2 Paper-based voting, as it currently stands, has numerous checks and balances to ensure that human error on the part of one person cannot affect any part of the election. For the reasons listed above, electronic voting cannot provide these safeguards.