Submission to the Victorian Inquiry into Electronic Voting

Roland Wen[1] Richard Buckland[1,2]

[1]School of Computer Science and Engineering
The University of New South Wales

[2]Australian Centre for Cyber Security

Executive Summary

E-voting systems used in large-scale public elections in Victoria, other Australian jurisdictions and overseas have all suffered from critical failings and unacceptable risk, especially in terms of quality and security. Moreover none of these systems provides verifiability, which is a key security requirement. The Victorian vVote project was a commendable attempt at designing a system to address this shortcoming in verifiability, but it was unsuccessful.

Numerous alternative designs have been proposed for e-voting systems, including designs that aim to provide verifiability. But adapting an existing design to satisfy the requirements of Victorian or Australian elections is highly challenging, and in many instances is simply infeasible (for instance it is impractical to adapt many designs to preferential voting). The vVote project, which adapted an existing design, highlights the risks of introducing a range of shortcomings and significantly weakening the security of an existing design. These are in large part consequences of the original design being unable to account for many practical and context-specific requirements from the outset.

Regardless of whether an existing e-voting system can be adapted to Victorian requirements or a completely new e-voting system needs to be developed, the key issue is to ensure that the system will maintain the high quality and security of the electoral process. Achieving this demands best engineering and management practices for developing and operating an e-voting system of high quality and security, and for providing strong assurance of this level of quality and security so that the system is trustworthy. The current shortcomings in these engineering and management practices are the root causes of the problems in existing e-voting systems. These shortcomings have been compounded by failings in scrutiny, transparency and risk management.

This submission covers the four issues of failure-critical engineering, scrutiny, transparency and risk. We make recommendations on how to address the failings relating to these four issues.

1 Introduction

E-voting has the potential to offer a range of significant benefits, and electoral bodies worldwide have strong incentives to harness these benefits. However e-voting remains highly controversial. Many jurisdictions around the world have abandoned or prohibited e-voting due to concerns over the quality and security of e-voting systems.

The universal problem with adopting e-voting has been addressing failings in the quality, security and trustworthiness of e-voting systems, and the consequent risks to the electoral process. We have written extensively on the topic of these problems, their root causes and the steps needed to address the root causes [BTW11; BW12; CORE12; WB15; CORE11].

This submission summarises the four key issues we have previously identified: failure-critical engineering, scrutiny, transparency and risk. For each issue in turn we discuss the common e-voting failings, and we make recommendations to address these failings.

2 Failure-Critical Engineering

E-voting systems are critical national infrastructure. Failures in these systems can have catastrophic, far-reaching consequences. Developing and operating e-voting systems according to failure-critical engineering practices is essential to ensuring and assuring the quality and security of elections.

2.1 Current Problems

At present e-voting systems used in large-scale public elections in Victoria and worldwide are developed and operated according to standard commercial practices or worse. This has resulted in serious failings in the quality and security of e-voting systems, and thus placed elections at high risk.

In particular these e-voting systems do not provide cryptographic verifiability, which is an essential security feature that acts as a "last line of defence" by helping to detect certain integrity failures, thereby facilitating the scrutiny of particular aspects of e-voting systems.

Failures in e-voting systems can have more serious consequences than failures in manual voting methods. For example failures in manual procedures in the 2013 WA Senate Election caused immense controversy but at least the problems were able to be detected, identified and rectified, and the election was then re-run. In contrast, failures in an e-voting system may not be detectable. Moreover even if the failures were detected, it would not be appropriate to use a "patched" version of the e-voting system when re-running the election because such failures typically stem from underlying failings in the engineering processes. These engineering failings are difficult and time-consuming to rectify, and until they have been rectified there cannot be any trust that the problems have been correctly identified and rectified, that no new problems have been introduced in doing so, and that no other problems remain.

An underlying cause of these quality and security shortcomings is that electoral commissions do not currently have the engineering and management capabilities to develop and operate e-voting systems according to failure-critical engineering practices. In particular there is no engineering expertise in critical disciplines such as failure-critical systems, security and risk.

IT has traditionally been outside the domain of expertise of electoral commissions, even though IT systems now pervade most of their activities. As a result electoral commissions have become heavily dependent on outsourcing to contractors (both short and longer term), consultants and vendors. This dependency on outsourcing compromises quality and security in a range of ways, for instance:

- Knowledge and skills are continually lost as temporary staff leave and also as "skeleton" permanent staff leave (possibly poached by outsourcing partners).
- Outsourcing partners typically follow commercial practices as they do not have the highly specialised skills and knowledge required for failure-critical engineering, especially since outsourcing tends to be driven by cost.
- Claims made by vendors over their capabilities and the quality and security of their e-voting systems cannot be properly assessed. This is especially the case for properties such as privacy and verifiability, which are technically complex and are highly susceptible to inaccurate and misleading claims that the requirements are satisfied.
- Conflicts of interest and corruption, which are common risks of outsourcing [ICAC13], can result in other interests displacing efforts to ensure high quality and security.

In the case of the vVote project, the entire team was outsourced but the team was still under-resourced. The design and the bulk of the implementation was carried out by academics who had a wealth of research expertise in verifiable e-voting systems, but who had limited to no practical engineering expertise and experience. Thus despite the best of intentions, the quality and security of the vVote system was severely compromised, to the extent that the project failed to deliver a system that provided verifiability, which was a primary objective of this project. Such failings are a common pattern in e-voting projects.

Building up and maintaining engineering capabilities is a challenge faced by electoral commissions and the public sector in general, due to factors such as limited funding, the often project-based nature of IT, tight schedules, and the worldwide IT skill shortage, particularly for high-calibre staff with specialised skills in areas such as security. However until this challenge is addressed, the quality and security of e-voting systems will continue to be at high risk.

2.2 Recommendations

Recommendation 1. *E-voting systems must be treated as failure-critical systems, not as commercial-grade best-effort systems.*

E-voting systems are critical national infrastructure, and must be developed and operated according to failure-critical engineering practices. This is essential to ensuring both the reality and community perception of the quality, security and trustworthiness of the electoral process and in the outcomes it reports. Elections are high-stakes, non-repeatable events and can result in outcomes that are unpopular for a significant proportion of the public. They are increasingly tempting targets for foreign powers, terrorists, criminal organisations and well-funded special interest groups. It is vital for the democratic stability of the nation that there is trust in the reported outcomes of these intangible systems and that this trust is well-deserved and demonstrable.

Recommendation 2. *Electoral commissions need to ensure that they have the capability to ensure technical oversight and governance of e-voting systems.*

As critical national infrastructure, e-voting systems require the highest level of oversight, control and governance. Electoral commissions require permanent, in-house engineering and management expertise and resources to ensure quality, security and compliance, and to specify, ensure and provide oversight of failure-critical engineering practices. Accordingly electoral commissions must be provided with adequate funding to build up and maintain these capabilities.

Outsourcing should be used only to complement core capabilities, rather than providing core capabilities. For quality and security reasons, critical dependence on external providers should be minimised. In particular it is inappropriate for national security to outsource governance or oversight to external commercial organisations.

Recommendation 3. *A single national approach to e-voting should be considered.*

The quality and security of e-voting systems is paramount as failure-critical national infrastructure. Establishing an e-voting system of appropriately high quality and security will require considerable resources. It would be far preferable to pool resources and produce a single quality system, rather than duplicating efforts and producing a number of lower quality systems. In addition a system that is used more regularly and is more regularly exposed to scrutiny is more likely to be secure than one that is used less frequently.

Closer engineering collaboration across electoral commissions should also be considered, to avoid duplicated effort and repeated mistakes, and to allow experience and expertise to be shared.

3 Culture of Scrutiny

A strong culture of election scrutiny is a core principle of traditional paper-based elections in Australia. Robust scrutiny and the expectation of this level of scrutiny, especially external and public scrutiny, has been fundamental to motivating and driving the high quality of elections in Australia, to fostering trust in this quality, and to ensuring the continuous improvement of our elections.

Similarly, a strong culture of technical scrutiny is a core principle of failure-critical engineering. Rigorous, ongoing reviews and audits are fundamental to ensuring high quality and security by identifying and rectifying defects and vulnerabilities as early as possible, to providing high assurance of this quality and security, and to continuously improving the engineering and management processes.

3.1 Current Problems

At present the strong cultures of election scrutiny and technical scrutiny are not extended to e-voting systems, or to election technology more generally. The absence of such scrutiny has created a high risk that serious quality, security, engineering and management failings in e-voting systems will be undetected and unaddressed. This has also created a high risk that these systems and the outcomes they produce will not be trusted, especially by losing candidates and their supporters.

Election technology has remained largely outside election scrutiny processes, despite the fact that elections have become heavily dependent on these systems, which have been used extensively for behind-the-scenes election administration tasks in Australia for decades. To date there has been minimal scrutiny of election technology by party-appointed scrutineers and by regular parliamentary inquiries into elections, even when critical failures have occurred. As a result there has been a lack of opportunity to understand and discuss the issues, including the very issue of how to scrutinise these systems. Greater attention has been drawn to these scrutiny shortcomings only recently as e-voting systems have begun to be used in Australia, and the high visibility and risk of these systems have raised questions over quality, security and trustworthiness.

Technical scrutiny of election technology has also been inadequate or non-existent, and this problem has continued with e-voting systems. Reviews and audits are currently considered as optional, standalone activities. In many instances independent reviews and audits are not performed at all because either they were not planned or they were abandoned due to cost and/or time constraints. Typically when reviews or audits are carried out, they are held too late to address serious issues, they are too brief and narrow in scope to identify many of the issues, and the engineering and management processes are not examined.

In the case of the vVote project, the vVote system has received minimal election scrutiny despite the significance of the project. With the exception of our submission to the Inquiry into the Conduct of the 2014 Victorian State Election [WB15], there has been little commentary on the problems and the lessons that should be learned. Likewise the vVote project lacked technical scrutiny, and this resulted in serious problems and risks not being identified. Although during the project a number of us raised serious concerns over the failure to carry out engineering reviews [BJRW13], these concerns were never addressed. Instead independent audits were deemed unnecessary, and only a single engineering review was conducted, which lasted merely a week and was carried out when the development was almost completed.

3.2 Recommendations

Recommendation 4. *Election scrutiny of e-voting systems needs to be integrated into the broader election scrutiny process.*

Multiple forms and layers of election scrutiny are imperative to the electoral process. These include internal reviews and analysis by electoral commissions, external assessments by government auditors (such as ANAO) and independent experts, election observation by party-appointed scrutineers, and regular public inquiries by parliaments. Such thorough scrutiny and the broad participation in this scrutiny have served to build and improve the high quality and trustworthiness of elections in Australia, even when the outcome is extremely close.

The same strong culture of election scrutiny needs to be extended to e-voting systems to maintain the current quality and trust in our elections. Clear expectations for rigorous scrutiny need be established from the outset, and these need to be followed through. Setting a strong mandate for scrutiny would act as a powerful incentive to develop and operate e-voting systems as failure-critical national infrastructure. The current parliamentary inquiry into electronic voting is a rare opportunity to openly discuss what is necessary to develop strong election scrutiny of e-voting systems.

Recommendation 5. *Technical scrutiny of e-voting systems needs to be integrated into engineering and management processes.*

Multiple forms and layers of ongoing internal and external reviews and audits are imperative to failure-critical engineering for e-voting systems. These include reviews and audits of requirements, design, implementation, tests, deployment, and the engineering and management practices. Quality and security of e-voting systems rely heavily on reviews and audits to continuously improve the systems, as well as the processes for their development and operation. As such technical scrutiny needs to be incorporated throughout the entire engineering and management processes from the outset, to avoid the common risk of cost and time pressures leading to reduced scrutiny, and thus reduced quality and security.

4 Transparency

Strong transparency has long been a key feature of paper-based elections. It promotes understanding of the electoral process, and lays the foundation for the strong culture of election scrutiny. In this way strong transparency supports and enhances the quality, security and trustworthiness of elections. However the introduction of election technology has reduced transparency. These systems are inherently non-transparent due to their virtual and highly complex nature. The challenges involved in providing transparency to support electoral processes and technical processes have yet to be addressed for election technology and e-voting systems.

4.1 Current Problems

At present e-voting systems do not have transparency requirements. Little consideration has been given to the transparency needs of the range of participants in the electoral process, and what information and material needs to be created and released to meet these diverse needs. For example:

- Failure-critical engineering and management practices require transparency for effective collaboration, communication and knowledge sharing.
- Technical scrutiny requires transparency to understand and assess the complex technical details of e-voting systems and the engineering and management processes.
- Election scrutiny has different transparency requirements to provide higher-level scrutiny based on less technical material such as detailed reports by electoral commissions, auditors and independent experts.
- Voters using e-voting systems, election staff supervising the systems, and the broader public have different transparency requirements again, as they need to understand and trust these systems at a different level and for different purposes.

In the absence of transparency requirements, e-voting systems have not been developed with these transparency needs in mind. The material needed to support transparency is either not released or not even created. In particular there is currently no onus to provide evidence of quality and security of e-voting systems. This places elections at high risk because quality and security are frequently compromised due to cost and time constraints, but these trade-offs may appear invisible until a publicly evident failure occurs (and many failures may not be publicly or even internally evident).

In addition conflicts of interest have created strong incentives to reduce transparency. For example there are natural reputational incentives to avoid revealing shortcomings in quality and security. Furthermore there are commercial incentives to conceal system details to protect intellectual property. This is most prevalent when a system has been developed by a vendor but can also occur when the systems are developed in-house, as demonstrated by the Australian Electoral Commission's refusal to release the source code for its EasyCount Senate counting software on the basis of commercial reasons [Cor13]. There are also financial incentives for outsourcing partners to increase the dependency on outsourcing by reducing transparency.

Failing to prevent these other interests from overriding the public interest in transparency also risks damaging trust in the electoral process, especially given the broader public expectation of transparency arising from the current movement towards open, transparent and accountable government.

In the case of the vVote project, the original intention was to make all aspects of the project publicly transparent. This did not eventuate as transparency requirements were never specified. Although source code and several research papers were published, most

engineering and project material was not released (including documentation of the practices adopted and evidence that these were followed). Critical engineering specifications were not created, largely due to time constraints. The subsequent low transparency contributed to the failure to provide verifiability, as voters and independent verifiers were unable to understand and perform their complex verification tasks.

4.2 Recommendations

Recommendation 6. *E-voting systems need upfront transparency requirements that support election scrutiny and technical scrutiny.*

Transparency is fundamental to both election scrutiny and technical scrutiny in failure-critical engineering practices. Both of these types of scrutiny demand that transparency needs are well-defined in advance. Otherwise barriers to transparency will naturally and inevitably emerge in e-voting systems, and these barriers can be infeasible to later overcome. In particular the quality and security of e-voting systems can be made transparent only if the necessary evidence is produced from the outset.

Other barriers to transparency are more explicit. Notably, commercial e-voting systems are typically encumbered by intellectual property issues that preclude or at least restrict transparency and scrutiny.

Recommendation 7. *E-voting systems need upfront transparency requirements that support understanding by voters, election officials, and the broader public.*

Non-technical participants in the electoral process, such as voters and election officials, have unique transparency needs to understand e-voting systems so that they can effectively use and trust these systems. Transparency requirements for these non-technical audiences need to be well-defined in advance. Only then can technical requirements and designs for the systems be developed from the outset to meet these transparency needs, for instance by simplifying procedures and maximising usability. Furthermore substantial effort must be invested in developing non-technical material (for instance instructional documents and videos) to support these transparency needs.

In addition verifiable e-voting systems have particular transparency requirements that are necessary to satisfy verifiability. Voters must be able to understand and perform their verification tasks, and election officials must be able to assist voters with the verification tasks. Also independent verifiers must be able to understand and perform their verification tasks, namely assessing the system's verifiability claims and implementing verifier software to check the system's verification artefacts.

5 Risk

E-voting systems pose numerous complex risks. Many of these are new risks that fundamentally change the risk profile of elections, in terms of how election integrity can be compromised and how election security can be violated. For example large-scale Internet voting makes it trivial to buy votes undetectably. Identifying, analysing and managing

these risks are at the heart of failure-critical engineering, where the practices are designed to mitigate risks, especially those relating to quality and security.

5.1 Current Problems

At present the risks of e-voting systems are poorly understood. Risks to quality and security are frequently overlooked or underestimated, and even well-known IT risks are often badly managed. It appears likely that the actual risks of current e-voting systems are well in excess of the risk appetites of electoral commissions.

Inadequate understanding, communication and management of the risks is a major factor in catastrophic failures of failure-critical systems. For example an underlying cause of the Space Shuttle Challenger disaster was a severe underestimation of the risk of failures by NASA management, who faced significant pressures to meet flight schedules and maintain confidence in the organisation. The night before the launch, engineers warned against launching at low temperatures due to the high risk of the O-ring seals failing in these conditions [Fey86; Fey88]. Subsequently the failure of the seals caused the destruction of the shuttle. Although this particular failure was later rectified, the failures in the risk management processes were not addressed. Known problems and high risks continued to be disregarded on the basis that these had not caused catastrophic failures, and this poor risk management culture caused the Space Shuttle Columbia disaster 17 years later [CAIB03].

Electoral commissions face similar pressures and risks with e-voting systems. Despite last-minute development and operational problems, to date the final decision has always been made in favour of launching an e-voting system for an election, rather than reconsidering using the system due to high risks. Subsequently live failures have occurred and serious vulnerabilities have been discovered. Although most of these particular problems were later fixed, the underlying risk management failures still persist, and so it would seem to be only a matter of time before a catastrophic failure occurs.

An underlying cause of the current risk failures is that electoral commissions do not have the necessary expertise in risk assessment and risk management for such complex and critical systems. Currently there are no risk experts to implement and follow rigorous risk assessment and management processes. Also there is inadequate technical expertise to assess the risks and to propose and decide on appropriate treatments and trade-offs.

In the case of vVote, technical risks to the quality and security of vVote were overlooked, and high-risk decisions and trade-offs were made as the risks were not properly considered. Risk assessment and risk management were ad hoc, did not follow a clear methodology, and were overly simplified. For example the VEC used software provided by the Victorian Managed Insurance Authority (VMIA) to assess and manage risks, and this software was "designed as a simple solution for risk managers to record and report on risks. The product is targeted specifically at organisations that do not have risk management software, require an easy to use application, and would be unlikely to to obtain funding for an off-the-shelf solution... The software is not targeted at organisations that require sophisticated integrated Governance, Risk and Compliance (GRC) or incident management systems" [VMIA11].

5.2 Recommendations

Recommendation 8. *E-voting systems need to explicitly focus on risk in their development and operation.*

As complex failure-critical systems, e-voting systems need to have risk, quality and security addressed and monitored continuously from the outset. This requires comprehensive and continuous risk assessment according to a rigorous, systematic methodology, and in broad consultation with technical experts in areas including risk, failure-critical systems and security. It also requires risk management to be systematically integrated into all engineering and management processes, and in particular all decision-making processes.

Risk assessment and risk management are a particular issue when systems start at a small scale, where an informal treatment of risk might appear adequate, but then the system grows gradually in scope and scale over time and repeated use. Unless risk is centrally incorporated from the outset, such systems inevitably evolve into dangerously complex and insecure infrastructure. A similar problem exists when early components or iterations of system components are designed or developed by developers with commercial experience and capability, rather than expertise in failure-critical systems.

References

[BJRW13] Richard Buckland, Rui Joaquim, Peter Y. A. Ryan and Roland Wen. "Concerns and Recommendations for Transparency and Review". Private communication to the VEC. 6th May 2013.

[BTW11] Richard Buckland, Vanessa Teague and Roland Wen. "Towards Best Practice for E-election Systems - Lessons from Trial and Error in Australian Elections". In: *E-Voting and Identity - Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers*. Ed. by Aggelos Kiayias and Helger Lipmaa. Vol. 7187. Lecture Notes in Computer Science. Springer, 2011, pp. 224–241.
URL: http://dx.doi.org/10.1007/978-3-642-32747-6_14.

[BW12] Richard Buckland and Roland Wen. "The Future of E-voting in Australia". In: *IEEE Security & Privacy* 10.5 (2012), pp. 25–32.
URL: http://dx.doi.org/10.1109/MSP.2012.59.

[CAIB03] Columbia Accident Investigation Board. *Columbia Accident Investigation Board Report*. Vol. 1. 2003.
URL: http://history.nasa.gov/columbia/CAIB_reportindex.html.

[Cor13] Michael Cordover. *Freedom of Information Request to the Australian Electoral Commission: Software by which Senate counts are counted*. 2013.
URL: https://www.righttoknow.org.au/request/software_by_which_senate_counts.

[CORE11] Roland Wen, Vanessa Teague and Richard Buckland. *Best Practices for E-election Systems. Computing Research and Education Association of Australasia (CORE) Supplementary Submission to the Inquiry into the 2010 Federal Election*. Submission 101.1, Inquiry into the 2010 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia, 2011.
URL: https://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=em/elect10/subs/sub101.1.pdf.

[CORE12] Vanessa Teague and Roland Wen. *Problems with the iVote Internet Voting System. Computing Research and Education Association of Australasia (CORE) Submission to the Inquiry into the Administration of the 2011 NSW Election and Related Matters*. Submission 7, Inquiry into the Administration of the 2011 NSW election and related matters. Joint Standing Committee on Electoral Matters, Parliament of NSW, 2012.
URL: http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/BA09355EDE5E3859CA2579AD0001D53C.

[Fey86] Richard P. Feynman. "Appendix F - Personal observations on the reliability of the Shuttle". In: *Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident*. Vol. 2. 1986.
URL: http://history.nasa.gov/rogersrep/v2appf.htm.

[Fey88] Richard P. Feynman. *What Do You Care What Other People Think? - Further Adventures of a Curious Character*. Ed. by Ralph Leighton. W. W. Norton & Co., 1988.

[ICAC13] NSW Independent Commission Against Corruption. *Managing IT contractors, improving IT outcomes*. Discussion paper. 2013.
URL: http://www.icac.nsw.gov.au/component/docman/doc_download/4191-managing-it-contractors-improving-it-outcomes-august-2013.

[VMIA11] Victorian Managed Insurance Authority. *VMIA Risk Register Software User Guide*. Release version 1.2.6. Victorian Managed Insurance Authority. Sept. 2011.
URL: https://www.vmia.vic.gov.au/~/media/internet/content-documents/risk/risk-tools/risk-register-software/instructions/risk-register-software-user-guide.pdf.

[WB15] Roland Wen and Richard Buckland. *Problems with E-Voting in the 2014 Victorian State Election and Recommendations for Future Elections*. Submission 12, Inquiry into the Conduct of the 2014 Victorian State Election. Electoral Matters Comittee, Parliament of Victoria, 2015.
URL: http://www.parliament.vic.gov.au/images/stories/committees/emc/2014_Election/Submissions/No_12_Dr_Roland_Wen_and_Associate_Professor_Richard_Buckland.pdf.