Submission to the Federal

Joint Standing Committee on Electoral Matters

INQUIRY INTO AND REPORT ON ALL ASPECTS OF THE CONDUCT OF THE 2016 FEDERAL ELECTION AND MATTERS RELATED THERETO

Authors:

Ian Brightwell
Consultant

Richard Buckland
Associate Professor
Computer Security, Cybercrime, and Cyberterror,
UNSW

Dr Roland Wen
Visiting Research Fellow
UNSW

Clancy Rye
Student
UNSW

Ian Brightwell

Date: 30 October 2016

Joint Standing Committee on Electoral Matters

INQUIRY INTO AND REPORT ON ALL ASPECTS OF THE CONDUCT OF THE 2016 FEDERAL ELECTION AND MATTERS RELATED THERETO

Table of Contents

Authors:

Ian Brightwell
Consultant

Richard Buckland
Associate Professor
Computer Security, Cybercrime, and Cyberterror,
UNSW

Dr Roland Wen
Visiting Research Fellow
UNSW

Clancy Rye
Student
UNSW

Executive Summary

This submission considers the new electronic preference capture system deployed in the 2016 federal election and identifies security and reliability risks in the design and operation of that system, primarily in relation to *scrutiny* and *transparency.* These risks affect the ability of the system to detect and prevent both accidental and malicious errors which could have a significant impact on an election outcome.

A new system for the electronic capture of handwritten Senate preference data was used in the 2016 Federal Election arising from the recent changes to above the line preference voting. The authors acknowledge that the Australian Electoral Commission (AEC) and their partners only had a very short timeframe to implement this system. However, the authors have significant concerns that the reliability of the results from the new system depends on all procedures being followed perfectly and the system operate without error or malicious activity.

This **submission identifies several significant errors in the reported results** which were not detected by the scrutiny process used at the election. The presence of these errors is compelling evidence of the need for improved openness and more effective scrutiny of count processes. Appropriate new methods of scrutiny and a commitment to openness are both essential to ensure the same quality of scrutiny is achieved for technological processes as are currently achieved with current manual processes[1].

The Submission suggests ways that these and other errors can be detected at future elections. This submission also deals with the inadequacies in the transparency and scrutiny of the new Senate preference capture process. It identifies that special skills and additional information is required to adequately assess the effectiveness of the new computerised preference capture processes at a given election event.

It also highlights issues surrounding the AEC's inability under current electoral legislation to provide adequate information to scrutineers and the public regarding the testing and operation of the system. Indeed, the AEC has also advised that the provision of such information is also not supported under current FOI legislation.

The submission makes two recommendations to address the above concerns and improve the scrutiny and security of technology used directly in the management of votes.

1 "2016 Federal Election Service Plan", AEC, June 2016

Recommendations

The authors commend the following recommendations for the Committee's consideration.

Recommendation 1 (see section 6.1)

The Commonwealth Electoral Act be amended to provide for the creation of a specialist Election Technology Review Board, to scrutinise technology used to capture and count votes. The Board should have access to sufficient information about the design, implementation, configuration and operation of electronic vote management systems to allow it to effectively assure that the systems are operated in accordance with legislation. The Board should report before and during the election only to the Electoral Commissioner, then post-election provides a publicly available assurance report to the Joint Standing Committee on Electoral Matters.

Recommendation 2 (see section 6.2)

The Commonwealth Electoral Act be amended require an audit of a sample of voters' actual paper ballots cast against the electronic data used in the count process. The audit sample size should be chosen to ensure that the cross-check process provides adequate statistical confidence in the electoral outcome.

1 Introduction

This submission responds to the following sections in the terms of reference provided to the Committee.

1. *All aspects of the 2016 Federal election and matters related thereto, and without limiting the scope of the committee's inquiry, with particular reference to:*

   (d) *The potential **application of new technology** to voting, **scrutiny** and counting, with particular reference to its application to remote voting, ADF personnel on deployment and supporting vision-impaired voters.*

The submission is focused on the implementation of the new Senate scan system for capturing Senate ballot preferences. The submission focuses on scrutiny issues and the challenges new technology creates for electoral transparency and integrity.

2 Background of Authors

The authors of this submission are computer scientists and cyber security experts with extensive experience and expertise in computer security, system integrity, failure critical engineering and the application of computers to electoral processes.

- Ian Brightwell has some 17 years' experience in the management of technology in the election process and has worked in the information technology area for over 30 years, with an emphasis on the use of technology within government agencies.

- Richard Buckland is Associate Professor in Computer Security, Cybercrime, and Cyberterror at UNSW, and a Director of the Australian Computer Society (ACS) and the Australian Centre for Cyber Security (ACCS). Associate Professor Buckland has been involved in election technology and related areas for over 10 years and has made several submissions to electoral matters committees around Australia.

- Dr Roland Wen is a Visiting Fellow at the UNSW and completed his Ph.D. in the area of election technology with a particular focus on upper house counting and the management of election technology. Dr Wen is also active in submissions to electoral matters committees around Australia and attends international conferences on e-voting and election technology.

- Clancy Rye is a senior undergraduate at UNSW studying Computer Science and Security Engineering and was also a scrutineer for a political party at the 2016 election. He has had an interest in politics and election process security for several years.

3 Electronic Scanning of Senate Votes

The 2016 election was the first time an electronic means to scan and capture all Senate vote preferences has been used for every Senate election in Australia. This change in process was a direct result of amendments to Senate voting legislation.

This submission is only concerned with the transparency and integrity of the Senate preference capture process as implemented for the 2016 election. The submission does not consider the suitability of the process design or the specific technology used to capture Senate preferences from an efficiency perspective. It also does not consider any issues with the downstream process of distributing preferences done by the EasyCount system.

It should be noted that the scrutiny and integrity issues raised in this submission are also applicable to the use of election technology in general, and in particular to systems for electronic voting. Therefore, this submission has broader implications, should there be a need to return ballots electronically in the future.

4 Electoral Transparency and Scrutiny

4.1 Required Scrutiny Standards

It has been a long accepted principle that electoral processes require a higher standard of transparency and scrutiny than other processes conducted by public authorities. The reason for this high level of transparency and scrutiny is that the outcome of elections must be trusted by the community at large if they are to be an effective means of transferring power.

The AEC has stated very clearly the standard it aims for to achieve trust in their 2016 Federal Election Service Plan[1]. The plan said;

> *The Australian Electoral Commission (AEC) is committed to delivering **trusted**, reliable, high quality and **high integrity** electoral events and services.*
>
> *The public and stakeholders have confidence that the electoral process is well managed - The AEC is **committed to delivering processes that uphold electoral integrity** and **engender voter and stakeholder trust** in the result and to ensuring the security and sanctity of the ballot paper at all times.*

The main method of achieving scrutiny for paper ballot handling is the use of scrutineers to inspect physical artefacts and processes. The role of scrutineers is defined in the Commonwealth Electoral Act (CEA) legislation; the act allows scrutineers to be present to witness many aspects of the electoral process. The Scrutineers Handbook 2016[2] defines scrutineers as:

> *People appointed by candidates to be their representatives at polling places, or at any place at which the scrutiny of votes is being conducted. scrutineers have the right to be present when the ballot boxes are sealed and opened and when the votes are sorted and counted so that **they may check any possible irregularities**, but they may not touch any ballot paper. – page 69*

[2] "Scrutineers Handbook 2016", Version 03, 30 June 2016, AEC
http://www.aec.gov.au/elections/candidates/files/scrutineers-handbook.pdf

Very few processes undertaken by public bodies allow this level of overview by the public. It is because elections are unique and can largely only be validated by independent review that this level of oversight is allowed and indeed required.

4.2 Challenges Scrutinising Technology

The current paper based election scrutiny is focused on the scrutiny of individual ballot papers to ensure that the election officials interpret the preference marks correctly. The checking of vote tallying is not specifically mentioned as a role for scrutineers but the legislation does allow scrutineers to query vote tallies and request that they check their tallies are correct. In a paper based environment this is generally simple and done without complaint, because the recheck process only involves retrieving the ballots in question from a secure store and counting them again in the presence of a scrutineer.

However, the scrutiny of electronic elections is not simple. The skills needed for the scrutiny of votes which are electronically captured and managed are obviously quite different to those needed in previous entirely paper based elections. The main reason being that information flow is not tangible and so inherently non-transparent because neither the AEC and the scrutineer can be certain that the computer has faithfully captured and held the electronic ballot preferences and passed them uncorrupted to the count process. The new system only provides scrutineers with “snapshots” of individual ballots on a screen at different stages of the process. These “snapshots” identify which preference marks the computer uses in the final count. However, it is all but impossible for a scrutineer to confirm that the preference marks they saw in a “snapshot” are accurately reflected in the final preference file used for the distribution of preferences process. Given this situation new approaches to transparency are necessary to enable the combination of electronic systems and physical processes to be scrutinised effectively.

An important first step in software system assurance is that the software and associated processes and technology be made available for independent audit and review. However, it is unlikely that traditional scrutineers will have the expertise or available time to effectively undertake this.

Furthermore, audits of the technology, although prudent, are not sufficient to give certainty that the process is working as expected. As convincingly demonstrated in the 2016 Census. The only real means by which individual scrutineers can have confidence that the final captured preference data is correct is to compare the preferences used in the final count with earlier physical preference information and to undertake random checks of the data.

To improve confidence in the technology based vote capture to the level desired by the service plan, expert and independent reports about the effectiveness and reliability of the process need to be made available for independent analysis. Also, there needs to be a report on the discrepancies between initial manual count results with final count results and ballots counted when different contests are run at the same election event. These reports need to be clear enough for non-specialist observers to confidently identify that sufficiently low levels of error have occurred in the capture of preferences from ballot papers and that the election outcome is correct.

4.3 Scrutiny in the 2016 Election

The Scrutineers Handbook 2016[2] also states:

> *The actual scrutiny of Senate ballot papers is done by the AEO at the CSS centre in the weeks following election night. scrutineers have the same rights and responsibilities at the CSS as they have at a HoR scrutiny undertaken by the DRO. - Page 56*

It is difficult for a scrutineer to achieve the same level of scrutiny with the new Central Senate Scrutiny (CSS) scan system as with manual counting because computers do not have the same properties as paper for scrutineers observing the tallying and secure handling of ballots.

For example, the CSS only allowed Senate ballots to be processed through the system end to end in *batches* with the CSS first preference tally only becoming available on the Internet several days (or in some cases weeks) later. This meant any discrepancies between a scrutineer's tally and published results could only be identified at a much later date, and then only if the scrutineer is able to consolidate tallies of all batches making up a polling place (a very challenging task which we understand is not supported well by the current system) and retain that information until the results are published.

In contrast, when a count is done manually at a count centre using paper ballots the tally for a polling place is known immediately after the count is finished and the scrutineer can record that tally and check their tally against the final result published. They can also observe that the ballots were handled securely and make an assessment whether the ballots have been tampered with by examining questionable ballots.

The level of scrutiny allowed at the CSS for the 2016 Senate count was identified in the Frequently Asked Questions[3] document provided to scrutineers by the AEC. This document defined the limits of scrutiny as:

> *As prescribed in the Commonwealth Electoral Act 1918, scrutineers may oversee the count process including the first preference counts, ballot paper scanning, data verification of preferences from the digital images and, should they require, inspection of the physical ballot papers. - Question 17*

The effect of the above interpretation of legislation on the Senate capture process was to only allow scrutineers to view the processing of isolated ballots at different parts of the process at the count centres. This meant scrutineers could only witness:

- some manual processes related to scanning the ballots,
- operators fixing the interpretation of scanned images with uncertain computer interpretation and
- data entry operators keying from scanned images.

[3] Federal election 2016, Central Senate Scrutiny, frequently asked questions, AEC http://www.aec.gov.au/elections/candidates/files/counting/css-faqs.pdf

The above scrutiny processes are useful in providing scrutineers a view of how individual ballots are interpreted but is not sufficient for scrutineers to be confident that the preferences for all ballots in a given polling place are correctly captured. It is not possible for a scrutineer to follow a ballot from scanning through to the commencement of counting in the current CSS system, which was a feature of the manual paper based system. Also, it was **not possible for a scrutineer to verify that the ballot preferences captured by the system and used in the count for any given ballot matched those shown on the ballot paper.**

The Scrutineers Handbook 2016[2] suggested that audit information about the processing of ballots would be made available:

> *This system provides full accountability and an audit trail, including reports for inspection by scrutineers. - page 23*

However the experience of the fourth author, a scrutineer for the Renewable Energy Party in NSW, showed that in practice this was not the case. The response to a written request to the NSW Senate Returning Officer for audit reports was that they would not be provided. The following text is from the emailed request:

> *Whilst at the CSS I would like to scrutinise the process in the manner defined in the attached senate count process document. Additionally, whilst at the CSS, I would also like to review the documents outlined in the FAQ. This would include:*
>
> 1. *IBM's independent third party quality assurance test completion report.*
> 2. *Certification report by the National Association of Testing Authorities for the count program.*
> 3. *The test completion report for penetration testing by an independent, accredited Australian Information Security Registered Assessors (IRAP) Program auditor for the systems and networks.*
>
> *I would also like to know the following statistics for the CSS process:*
>
> 1. *Number of ballots yet to be scanned.*
> 2. *Number of ballots scanned.*
> 3. *The number of ballots scanned which are subsequently sent to "Data entry #1 validate and correct" process as a percentage of ballots scanned.*
> 4. *The number of ballots which "Compare data entry" identifies as Mismatched as a percentage of ballots scanned.*
> 5. *Number of ballots fully processed through the CSS.*

The following is the emailed response from the NSW Senate Returning Officer:

> *The purpose of scrutiny, role of scrutineers and the process to be followed is set out in section 265 and 273 of the Commonwealth Electoral Act (CEA) and the AEC produces a handbook to assist scrutineers which may be found at* http://www.aec.gov.au/Elections/candidates/scrutineers.htm *. Matters which fall outside of the relevant section of the CEA, such as your request for review of documents, are not considered part of scrutiny and are therefore not available.*

Concerningly the scrutineer did NOT receive any of the requested information. The response from the NSW Senate Returning Officer clearly stated that the AEC did not believe they were obliged under the CEA to provide such reports. This response is at odds with the Scrutineers Handbook and, the authors believe, with the public assurance principles and intent of the scrutiny process. The effect of this situation was that scrutineers were unable to determine the overall effectiveness of the CSS system in processing ballot preferences.

At the time of the election the AEC only provided high level documentation about how the count centre was to operate and final count results. No audit trail reports or other operational reports were provided, showing how effectively the CSS did operate. This means scrutineers were unable to identify how effective the new CSS system was in processing ballot preferences and where potential failures may have occurred or their significance on the overall result.

A subsequent Freedom of Information (FOI) request for the three audit reports referenced above was made by one of the authors and was accepted by the AEC on the 16/8/16. A response denying the request was received on the 18/10/16 and has been attached as Appendix A. The response from the AEC denied the request on the following grounds:

- Documents disclosing trade secrets or commercially valuable information; and
- Public interest conditional exemptions—certain operations of agencies - providing access would be contrary to the public interest.

It should be noted that the reasons for denying the FOI request were substantially based upon the response revealing proprietary information about the AEC's EasyCount system. It was not the intention of the requestor to request information about EasyCount, in fact the requestor was surprised any EasyCount information was contained in these reports. The requestor has asked for an internal review of this decision, requesting the FOI be satisfied by redacting any information about EasyCount, and only provide information about the scanning system used at the Fuji Xerox facility. Should this not be possible then it suggests these test reports are mainly related to the EasyCount system testing and not scanning systems at the CSS which is significantly different the impression given in the documentation provided by the AEC.

Concerningly the response to the FOI request also states that the system tested contains security vulnerabilities that "could affect the outcome" of the election, that it is possible to make "an unauthorised alteration of the data" put into the system and "affect the outcome of [the] election" (appendix A highlighted clauses 1.3, 2.4, 3.2, and 4.2). This approach is contrary to current cyber security thinking which believes that such weaknesses and flaws increase the need for review and scrutiny, rather than reducing it.

The authors believe the above denial is a further clear demonstration that the current legislation is not appropriate for providing information to support the required electoral transparency of systems used to directly handle votes. Also, there appears to be a legislative barrier for the AEC to provide information which would permit adequate scrutiny of electronic systems. It is therefore recommended amendments are made to legislation to ensure information required by scrutineer can be provided by the AEC.

5 Electoral Integrity

The AEC developed a new technology based process to capture vote preferences. However, the reliance on technology to carry out this process will always put in doubt the integrity of the process unless the public has confidence that the system is adequately tested and the results can be and are independently scrutinised and verified.

Apparently, some system testing was conducted by the AEC but the results of these tests have not been made available despite requests by a scrutineer and through FOI. Furthermore, there has been no public indication that the AEC has undertaken an appropriate auditing cross check of the written preferences on paper ballots against the scanned versions of the preferences used to determine the candidates elected.

The table below (Table 1) shows there are several unexplained discrepancies in the official election results data currently published on the results website. Some of these discrepancies are significant and should be subject to further investigation and explanation. Furthermore the discrepancies identified are only for NSW, so further investigations of results for other states should be conducted and the findings publicly reported.

Notwithstanding, these discrepancies the authors are not suggesting that candidates were incorrectly elected at the 2016 election, but rather there is evidence that unexplained discrepancies exist within the results data that could, under certain circumstances, have an impact on electoral outcomes, and **yet they appear not to have been found by scrutineers prior to the declaration of the poll**. This information should have been readily accessible for scrutiny prior to the declaration of results, and if necessary rechecked before the final result was declared.

Table 1 – Ballots counted in the HOR compared to the Senate at venue level

		HOR	Senate			Difference	
Division – Polling Place or PPVC	Votes Issued	Final	As @ 10/7	As @ 24/7	Final	Senate & HOR	%
Kingsford Smith - Randwick KINGSFORD SMITH PPVC		9762		9958	10754	992	9%
Werriwa - Fairfield WERRIWA PPVC	970*	964	132	132	175	-789	-451%
Wentworth - Waverley WENTWORTH PPVC		10509		10152	10901	392	4%
North Sydney - Chatswood NORTH SYDNEY PPVC		5363	4630	5038	5038	-325	-6%
Berowra - West Ryde BEROWRA PPVC	320**	318			0	-318	
Barton - Rockdale BARTON PPVC		6876	6478	6478	7173	297	4%
Robertson - Divisional Office (PREPOLL)	417^	0		288	308	308	
Fowler - Fairfield FOWLER PPVC	11284	11308		9830	11201	-107	-1%
Parramatta - Westmead Central		543	542	597	630	87	14%

* estimated votes issued on the 1/7/16, ** estimated votes issued on the 1/7/16 & 30/6/16, ^ includes declaration votes
Note: Highlighted cells identify the value which is most likely to be in error.

The significance of Table 1 is that there should be a similar number of HOR and Senate ballots counted at any given venue. The table above shows that for some venues this was not the case. In fact, for some venues (Parramatta - Westmead Central, Barton - Rockdale BARTON PPVC) the

number of ballots counted on election night was similar for both the HOR and Senate, but was then changed markedly during the subsequent post-election night counting processes. In other cases, either HOR or Senate ballot papers for the whole venue appear to be missing (Berowra - West Ryde BEROWRA PPVC, Robertson - Divisional Office (PREPOLL)). The addition of 992 Senate ballots at Kingsford Smith - Randwick KINGSFORD SMITH PPVC is also a concern and is in itself sufficient to have an impact on a close HOR seat, if the error were to be with the HOR count.

The only way to determine the valid count of ballots for these venues is to examine the mark-off statistics for each venue. This information is not available to the public but the authors suggest it should be made available with the final results at future elections.

Without scrutiny, public confidence in the results depends entirely on confidence in the officials and systems carrying out the processes. Without scrutiny, any process errors are less likely to be found, but if they do exist and are found serendipitously they have the potential to significantly impact public confidence in the process. Again, the 2016 census provides a graphic demonstration of this. In this case the level of internal checking and audit carried out appears to have been be insufficient to ensure that evident handling or counting errors were resolved prior to the final declaration of the poll.

Given the additional risks arising from the use of technology in the vote handling process the above discrepancies indicate an even greater concern as additional types of hard to observe failure are possible with all electronic systems. Given the lack of scrutiny and the consequent difficulty of identifying the above errors it is suggested the Committee request the AEC to routinely provide post-election a report which identifies discrepancies which are over acceptable tolerance and explain why these discrepancies have occurred and why they will not affect the electoral outcome.

All electronic voting processes, of which the Senate preference capture process is one, need an independent verification process which allows a validation of a voter's intent without revealing their identity. Currently the AEC is not required under legislation to undertake such an audit validation for the Senate capture and as such did not do so. Consequently, we strongly advise that the legislation be amended to require that in future elections a publicly available validation be conducted to ensure that the electronic data used in the counting, accurately reflects the actual physical data recorded on ballot papers by voters.

6 Recommendations

The authors recommend the following changes be made to legislation to improve transparency, scrutiny and integrity of elections which use technology to directly manage ballots.

6.1 Election Technology Review Board

To overcome the issues identified above the authors recommend the committee consider the creation of an Election Technology Review Board to scrutinise technology and systems used to capture and count votes. This board should be selected before an election is called and comprise suitably qualified people i.e. people with a security engineering and/or technology management and/or election background. These appointments should be made by an organisation at arm's length from the AEC. A suitable entity may be the Australian National Audit Office in conjunction with the

electoral matters committee. Additionally, there are professional bodies that have members skilled in these areas who would be willing to assist in the process by nominating suitable people to serve on such a board.

The committee should consider appropriate amendments to legislation and/or regulation to support the establishment of an independent board to scrutinise technology used to manage votes and the effectiveness of the associated business processes.

The Board would need the following information as a minimum to conduct effective scrutiny of technology used in critical election processes.

- The Board should be able to request and be provided sufficient information about the underlying technology and processes to be able to assess information regarding the adequacy of the system's design, implementation, configuration and testing.
- The Board should be permitted to scrutinise the operation of the system to allow them to determine with appropriate confidence that the system is performing as planned.
- The Board should be able to investigate and witness verification of a cross check process demonstrating that the intent of the voter has been processed in accordance with the legislation and the accuracy of the process is sufficient to be confident the correct candidates have been elected.
- The Board should report on the adequacy of technological processes and digital information produced.
- The Board should provide a publicly available report to the electoral matters committee after each election.
- The Board should have appropriate investigative powers and access to enable it to carry out its functions.

The use of specialist Boards to deal with technology issues in election processes has been implemented in other jurisdictions. In particular, Norway implemented an Internet Election Committee (IEC) for their internet voting election trials in 2013 which had oversight of the trials with a particular focus on security. More information about the committee's work can be found in The Carter Centre's report[4] Also it should be noted that Canada has a completely independent body to oversee elections. Some aspects of this entity's structure and function[5] may also be applicable in the Australian environment to address the increased complexity of the electoral processes.

See Recommendation 1 in the Recommendations section of this document.

6.2 End to end audit and scrutiny

An "end to end" audit allows the checking and scrutiny of each link in the chain from the voter casting their vote on the ballot paper through to the final tally. Auditing and permitting scrutiny of

4 Expert Study Mission Report, TheCarter Center, Internet Voting Pilot: Norway's 2013 Parliamentary Elections, 19 March 2011 https://www.cartercenter.org/resources/pdfs/peace/democracy/carter-center-norway-2013-study-mission-report2.pdf

5 Commissioner of Canada Elections Annual Report 2014-2015, About Us https://www.cef-cce.gc.ca/content.asp?section=rep&dir=rep3&document=abo&lang=e

only some steps, but not others, means there can not be full public confidence that the final result is correct.

No audit or verification was conducted of ballot paper markings against the data produced by the Senate scan system. Two separate groups of academics[6,7] have examined the Senate scan process and each group found there was a need for a random sample cross check of input paper ballots to the output file, as an integrity check of the scanning process. The authors of this submission further believe that similar public scrutiny and verification of this nature is required of each step in the election process to ensure confidence in the overall electoral result.

The reason given for not allowing such an end to end validation was because it was not required by legislation. Therefore, the authors recommend that legislation be amended to require a cross check audit of a randomly selected sample of paper ballot papers against the output file from the Senate capture process.

For example, this check could be conducted by cross calling the preference marks on a random sample of the ballot papers to another person who is reading from a report prepared from the output file used to perform the distribution of preferences. This should be done in the presence of scrutineers and the board. The size and nature of the sample can be determined by well-known statistical methods. For example, a paper entitled "Auditing Australian Senate Ballots"[8] outlines an approach to determining the sample size for a given election.

See Recommendation 2 in the Recommendations section of this document.

6 Is the new Senate vote capture system as risky as electronic voting?, Roland Wen UNSW, Richard Buckland UNSW, July 19, 2016, The Conversation Australia.
https://theconversation.com/is-the-new-senate-vote-capture-system-as-risky-as-electronic-voting-62436

7 Paper audits crucial for automated counting, Dr Vanessa Teague, Department of Computing and Information Systems, University of Melbourne, Pursuit, University of Melbourne, July 2016.
https://pursuit.unimelb.edu.au/articles/paper-audits-crucial-for-automated-counting

8 "Auditing Australian Senate Ballots", Berj Chilingirian, Zara Perumal, Ronald L. Rivest, Grahame Bowland, Andrew Conway, Philip B. Stark, Michelle Blom, Chris Culnane and Vanessa Teague, October 4, 2016
https://arxiv.org/pdf/1610.00127v1.pdf

LS5721 ~ file 16/693.

Mr Ian Brightwell
By email to

Dear Mr Ian Brightwell

Your Freedom of information request no. LS5721

I refer to your email dated 15 August 2016 7:24 AM in which you request ('your FOI Request] to the Australian Electoral Commission ('AEC') under the *Freedom of Information Act 1982* for access to documents relating to the Senate count.

2 I am writing today to give you a decision about access to documents that you requested in your FOI Request.

Summary

3 I, Paul Pirani, Chief Legal Officer of the AEC, am an officer authorised under section 23(1) of the FOI Act to make decisions in relation to FOI requests.

4 Specifically you sought access to:

1. IBM's independent third party quality assurance test completion report.
2. Certification report by the National Association of Testing Authorities for the count program.
3. The test completion report for penetration testing by an independent, accredited Australian Information Security Registered Assessors (IRAP) Program auditor for the systems and networks.

5 I identified 4 documents that fell within the scope of your request.

6 I did this by directing inquiries to:

(a) the AEC's Election Planning Systems and Services Branch which is the AEC's business owner of the EasyCount software; and

(b) the AEC's Information Technology Branch which oversees the operation of the EasyCount software.

7 The schedule of retrieved documents in Attachment A provides a description of each document that falls within the scope of your request and observations supporting the access decision for each of those documents.

8 With regard to the documents you requested (set out in Attachment A), I have decided to refuse access to the 4 retrieved documents.

9 I also decided not to offer in lieu access to edited copies of those documents from which exempt material was redacted.

10 More information, including my reasons for my decision, is set out below.

11 A decision was due on your FOI Request on 14 October 2016. I apologise for the delay in finalising your FOI Request.

Decision and reasons for decision

Decision

12 With regard to the documents identified in Attachment A, I have decided:

(a) to refuse access to Document Nos 1, 2 and 3 under section 47C (*Documents disclosing trade secrets or commercially valuable information*); and

(b) to refuse access to Document Nos 1 - 4 under section 47E of the FOI Act (*Public interest conditional exemptions—certain operations of agencies*) as providing access would be contrary to the public interest.

Material taken into account

13 I have taken the following material into account in making my decision:

(a) the content of the documents that fall within the scope of the FOI Request;

(b) the FOI Act, specifically the long title and sections 3, 3A, 11A, 11B, 22 47C and 47E;

(c) the guidelines ('FOI Guidelines') issued by the Australian Information Commissioner under section 93A of the FOI Act, specifically paragraphs 3.85 – 3.90, 5.19 and 5.20, 5.33, 5.34, and 5.181 – 5.191, 6.11 – 6.33 and 6.86 - 6.112; and

(d) the views of a third party consulted by the AEC under section 27 of the FOI Act.

Reasons

14 Attachment A indicates each document to which access is refused. My reasons for refusing access are given below.

Exemption – Documents disclosing trade secrets or commercially valuable information

15 With respect to Document Nos 1, 2 and 3, I found that:

(a) each document contained information that would lead to the disclosure of a trade secret, namely the source code of the EasyCount software owned by the Commonwealth of Australia in right of the AEC;

(b) each document contained information that would lead to the destruction or diminution of the commercial value of the EasyCount software; and

in the alternative, I found that

(c) each document contained information that of itself may not be exempt would when combined with other information available form a mosaic that would lead to the disclosure of a trade secret, namely the source code of the EasyCount software; and

(d) each document contained information that of itself may not be exempt would when combined with other information available form a mosaic that would lead to the destruction or diminution of the commercial value of the EasyCount software

16 Under paragraph 47(1)(a) of the FOI Act, a document is an exempt document if it its disclosure under this Act would disclose trade secrets.

17 The application of paragraph 47(1)(a) of the FOI Act to the EasyCount software was established in proceedings in the Administrative Appeals Tribunal in 2015: see *Cordover and Australian Electoral Commission (Freedom of information)* [2015] AATA 956 ('Cordover's Case').

18 Under paragraph 47(1)(b) of the FOI Act a document or a copy of that document is an exempt document if its disclosure under this Act would disclose information having a commercial value that would be, or could reasonably be, expected to be, destroyed or diminished if the information were disclosed.

19 The application of paragraph 47(1)(b) of the FOI Act to the EasyCount software was established in proceedings in the Administrative Appeals Tribunal in 2015: see the Cordover Case.

20 Section 47 of the FOI Act provides:

47 Documents disclosing trade secrets or commercially valuable information

(1) A document is an exempt document if its disclosure under this Act would disclose:

(a) trade secrets; or

(b) any other information having a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if the information were disclosed.

(2) Subsection (1) does not have effect in relation to a request by a person for access to a document:

(a) by reason only of the inclusion in the document of information concerning that person in respect of his or her business or professional affairs; or

(b) by reason only of the inclusion in the document of information concerning the business, commercial or financial affairs of an undertaking where the person making the request is the proprietor of the undertaking or a person acting on behalf of the proprietor; or

(c) by reason only of the inclusion in the document of information concerning the business, commercial or financial affairs of an organisation where the person making the request is the organisation or a person acting on behalf of the organisation.

(3) A reference in this section to an undertaking includes a reference to an undertaking that is carried on by:

(a) the Commonwealth or a State; or

(b) an authority of the Commonwealth or of a State; or

(c) a Norfolk Island authority; or

(d) a local government authority.

21 I made my findings in paragraph 15 of this letter after I had had regard to paragraph 5.33, 5.34, and 5.181 – 5.191 of the FOI Guidelines.

22 Accordingly I am satisfied that the document is exempt under paragraph 47(1)(a) and paragraph 47(1)(b) of the FOI Act.

Public interest conditional exemptions—certain operations of agencies

23 With respect to Document Nos 1 - 4, I found that:

(a) each document contains information that could be used to enable unauthorised access to and alteration of the EasyCount software or the data put into that software for the purpose of its operation; and

(b) unauthorised access to and alteration of the EasyCount software or the data put into that software for the purpose of its operation would prejudice the operations of the AEC.

24 Paragraph 47E(d) of the FOI Act conditionally exempts a document if its disclosure under the FOI Act would or could reasonably be expected to have a substantial adverse effect on the proper and efficient conduct of the operations of the AEC.

25 Subsection 47E of the FOI Act provides:

47E Public interest conditional exemptions—certain operations of agencies

A document is conditionally exempt if its disclosure under this Act would, or could reasonably be expected to, do any of the following:

(a) prejudice the effectiveness of procedures or methods for the conduct of tests, examinations or audits by an agency;

(b) prejudice the attainment of the objects of particular tests, examinations or audits conducted or to be conducted by an agency;

(c) have a substantial adverse effect on the management or assessment of personnel by the Commonwealth or by an agency;

(d) have a substantial adverse effect on the proper and efficient conduct of the operations of an agency.

Note: Access must generally be given to a conditionally exempt document unless it would be contrary to the public interest (see section 11A).

26 The relevant operations of the AEC are the use of the EasyCount software to electronically conduct the count of ballots cast in an election including the allocation and counting of preference votes expressed in the ballot papers.

27 The EasyCount software is used by the counting of votes in Senate and industrial and fee for service elections.

28 In making my decision I had regard to:

(a) the following parts of the FOI Guidelines:

(i) Part 5 (Exemptions), specifically paragraphs 5.19 and 5.20; and

(ii) Part 6 (Conditional Exemptions), specifically paragraphs 6.86 -6.112; and

(b) the following matters that I considered relevant:

(i) particular matters in relation to each document noted in the entry about it in the schedule in Attachment A;

(ii) an unauthorised alteration to the EasyCount software or an unauthorised alteration of the data put into that software for the purpose of its operation could affect the outcome of a particular election and thereby causing an irregularity into the election;

(iii) any irregularity in an election could involve the Commonwealth in litigation:

(A) in the Court of Disputed Returns or, if remitted to it, the Federal Court of Australia in respect of a Senate election;

(B) in the Federal Court of Australia in respect of an inquiry into the election under section 201 of the *Fair Work (Registered Organisations) Act 2009*; and

(C) in a state or territory court or tribunal in respect of a fee for service election.

29 Accordingly, I am satisfied that the document falls within the scope of the conditional exemption for deliberative matter provided by paragraph 47E(d) of the FOI.

Weighing of public interest factors

30 Under subsection 11A(5) of the FOI Act, access to a document covered by a conditional exemption must be given unless it would be contrary to the public interest.

31 My weighing of public interest factors follows.

(a) I identified the following harm that would affect the Commonwealth of Australia, namely the harm identified in paragraph 23 of this letter.

32 I considered the following factors favouring disclosure:

(i) The objects of the FOI Act expressed in its long title and sections 3 and 3A of the FOI Act; and

(ii) the public interest in being assured that the computer systems and programs used by the AEC to count ballot papers operate effectively to produce accurate counts and distribution of preferences expressed by voters in their respective ballot papers;

(b) I considered the following factors that militate against disclosure:

(i) The harm identified in paragraph 23 of this letter;

(ii) The public interest in being assured that the computer systems and programs used by the AEC to count ballot papers operate free from unauthorised access and tampering with the data that they process in the course of producing counts and distribution of preferences expressed by voters in their respective ballot papers.

33 In accordance with subsection 11B(4) of the FOI Act I excluded from my consideration the following matters:

(a) access to each document could result in embarrassment to the Commonwealth Government, or cause a loss of confidence in the Commonwealth Government;

(b) access to each document could result in any person misinterpreting or misunderstanding the document;

(c) the author of each document was (or is) of high seniority in the agency to which the request for access to the document was made;

(d) access to each document could result in confusion or unnecessary debate.

34 In considering the weighing of public interest factors I had regard to the FOI Guidelines at paragraphs 6.11 – 6.33.

35 In my view, the factors against disclosure of each document outweigh the factors in favour of disclosure for the following reasons:

(a) the public interest in knowing that the computer systems and programs used by the AEC to count ballot papers have operated without interference to produce an accurate outcome of the voting has greater weight than the interest of the public in being assured that the computer systems and programs used by the AEC to count ballot papers operate effectively to produce accurate counts and distribution of preferences expressed by voters in their respective ballot papers;

(b) the costs of conducting a second election in the event that the result of the initial election was set aside because of doubts flowing from an attack on the computer systems and programs used by the AEC are significant in as much as depending on the scope of an attack may range from $32,000,000 to $232,350,000.

36 Accordingly, I am satisfied that the Document Nos 1 - 4 are conditionally exempt under paragraph 47(d) of the FOI Act and because disclosure would be contrary to

the public interest and that the documents should be treated as exempt from disclosure under the FOI Act.

Preparation of an edited copy

37 In accordance with section 22 of the FOI Act I next considered whether it is both possible and practicable to prepare an edited copy of from which material that could lead to the disclosure of the EasyCount software source code or other information that would make it vulnerable to attack is redacted.

38 Section 22 of the FOI Act provides:

> **22 Access to edited copies with exempt or irrelevant matter deleted**
>
> *Scope*
>
> (1) This section applies if:
>
> (a) an agency or Minister decides:
>
> (i) to refuse to give access to an exempt document; or
>
> (ii) that to give access to a document would disclose information that would reasonably be regarded as irrelevant to the request for access; and
>
> (b) it is possible for the agency or Minister to prepare a copy (an ***edited copy***) of the document, modified by deletions, ensuring that:
>
> (i) access to the edited copy would be required to be given under section 11A (access to documents on request); and
>
> (ii) the edited copy would not disclose any information that would reasonably be regarded as irrelevant to the request; and
>
> (c) it is reasonably practicable for the agency or Minister to prepare the edited copy, having regard to:
>
> (i) the nature and extent of the modification; and
>
> (ii) the resources available to modify the document; and
>
> (d) it is not apparent (from the request or from consultation with the applicant) that the applicant would decline access to the edited copy.
>
> *Access to edited copy*
>
> (2) The agency or Minister must:
>
> (a) prepare the edited copy as mentioned in paragraph (1)(b); and
>
> (b) give the applicant access to the edited copy.
>
> *Notice to applicant*
>
> (3) The agency or Minister must give the applicant notice in writing:
>
> (a) that the edited copy has been prepared; and
>
> (b) of the grounds for the deletions; and
>
> (c) if any matter deleted is exempt matter—that the matter deleted is exempt matter because of a specified provision of this Act.

(4) Section 26 (reasons for decision) does not apply to the decision to refuse access to the whole document unless the applicant requests the agency or Minister to give the applicant a notice in writing in accordance with that section.

39 I had regard to paragraphs 3.85 – 3.90 of the FOI Guidelines.

40 I found that it is both impossible and impracticable to prepare an edited copy of Document Nos 1 - 4 from which material that could lead to the disclosure of the EasyCount software source code or other information that would make it vulnerable to attack is redacted.

41 My reasons for the finding in paragraph 40 are that:

(a) it is difficult to make a judgment as to how significant any information is that may contribute a mosaic piece to uncovering the exempt information; and

(b) the resulting edited copy from which exempt material was redacted was unlikely to be acceptable to the applicant in lieu of access in full to Document Nos 1, - 4 given that each would be meaningless.

42 Accordingly, I decided not to offer access to an edited copy of Document Nos 1 - 4 from which material that could lead to the disclosure of the EasyCount software source code or other information that would make it vulnerable to attack is redacted.

YOUR REVIEW RIGHTS

43 If you are dissatisfied with my decision, you may apply for internal review or Information Commissioner review of the decision. We encourage you to seek internal review as a first step as it may provide a more rapid resolution of your concerns.

Internal review

44 Under section 54 of the FOI Act, you may apply in writing to the AEC for an internal review of my decision. The internal review application must be made within 30 days of the date of this letter.

45 Where possible please attach reasons why you believe review of the decision is necessary. The internal review will be carried out by another officer within 30 days.

Information Commissioner review

46 Under section 54L of the FOI Act, you may apply to the Australian Information Commissioner to review my decision. An application for review by the Information Commissioner must be made in writing within 60 days of the date of this letter, and be lodged in one of the following ways:

online:	https://forms.business.gov.au/aba/oaic/foi-review-/
email:	enquiries@oaic.gov.au
post:	GPO Box 52189, Sydney NSW 2001
in person:	Level 3, 175 Pitt Street, Sydney NSW

47 More information about Information Commissioner review is available on the Office of the Australian Information Commissioner website. Go to www.oaic.gov.au/freedom-of-information/foi-reviews.

QUESTIONS ABOUT THIS DECISION

48 If you wish to discuss this decision, please contact Owen Jones at:

post: Locked bag 4007, Canberra ACT 2601
telephone: 02 6271 4528

Yours sincerely

Paul Pirani
Chief Legal Officer

17 October 2016

Attachments

Attachment A (Schedule of documents);

Attachment A

LS5721 FOI REQUEST BY IAN BRIGHTWELL

Request for copy of:

1. IBM's independent third party quality assurance test completion report.
2. Certification report by the National Association of Testing Authorities for the count program.
3. The test completion report for penetration testing by an independent, accredited Australian Information Security Registered Assessors (IRAP) Program auditor for the systems and networks.

SCHEDULE OF RETRIEVED DOCUMENTS

Document No.	Description	Date	Observations
1	Test Summary Report for the EasyCount Senate Reform Project	6/06/2016	
	1.1 Document No. 1 reports on the type of tests applied and the outcome of those tests to the Count and Data Entry functionality of the AEC's EasyCount software. ***Trade Secret*** 1.2 The description of the tests in Document No. 1 are capable of contributing to a mosaic of information that may lead to the unmasking of the source code in the AEC's EasyCount software which is a trade secret. ***Operations of the AEC.*** 1.3 Document No. 1 contains information about the Count and Data Entry functionality of the AEC's EasyCount software that can be used to facilitate an electronic attack on that software or the data that it processes in the course of counting ballot papers.		

Document No.	Description	Date	Observations
2	Test Summary Report for the EasyCount Senate Reform Project (Scan Import)	17/6/2016	2

2.1 Document No. 2 reports the outcome of a second series of formal NATA test that were conducted to cover the following:

(a) Import of XML files into EasyCount;

(b) Count regression testing to ensure that the generated reports are identical to those that were generated during the original Count formal testing.

Trade Secret

2.2 The description of the tests in Document No. 2 are capable of contributing to a mosaic of information that may lead to the unmasking of the source code in the AEC's EasyCount software which is a trade secret.

Operations of the AEC

2.3 XML is an acronym for the Extensible Markup Language used in computing as a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

2.4 Document No. 2 contains information about the import of XML files AEC's EasyCount software that can be used to facilitate an electronic attack on that software or the data that it processes in the course of counting ballot papers.

3	Power point presentation *Scanning Quality Assurance Service – Detailed Report*	19/06/2016	3

	Trade Secret 3.1 The description of the tests in Document No. 2 are capable of contributing to a mosaic of information that may lead to the unmasking of the source code in the AEC's EasyCount software which is a trade secret. ***Operations of the AEC*** 3.2 Document No. 3 contains naming conventions used by the AEC to process scanned Senate ballot papers that provide information that could be used to make an unauthorised alteration of the data put into the EasyCount software for the purpose of its operation could affect the outcome of a particular election and thereby causing an irregularity into the election.		
4	Email from Ryan Catterall, Penetration Tester, Ionize Pty Ltd to Professor Mark Looi, Information Technology Security Adviser, AEC and another re *Activity Summary - EasyCount Pentesting*	29/06/2016 3:34 PM	
	Operations of the AEC 4.1 Document No. 4 reports the outcome of penetration testing undertaken in respect of the EasyCount software. 4.2 Document No. 4 contains information about vulnerabilities of the EasyCount software to external attack that could be to make an unauthorised alteration of the data put into the EasyCount software for the purpose of its operation could affect the outcome of a particular election and thereby causing an irregularity into the election.		

End.