ELECTORAL COMMISSION
TE KAITIAKI TAKE KŌWHIRI

15 February 2021

Bonnie McGregor
fyi-request-14420-71ab5cd3@requests.fyi.org.nz

Dear Bonnie,

OFFICIAL INFORMATION ACT REQUEST 2021/03

On 8 January 2021 you made a request under the Official Information Act 1982 (the Act). Specifically, you have asked:

> *"I understand that we manually count votes in NZ by hand.*
> *Once the count is complete for each voting place during the official count, the totals are recorded on a certificate of results which is signed by the returning officer and a Justice of the Peace. The results are entered into our Election Management System which records the results.*
>
> *I was wondering where I can find the signed certificates for the manual count please, as the ones on the election website are the certificates printed from the software.*
> *My understanding is the manual count is signed off then entered into the system.*
> *If my understanding is not correct can you please explain the vote counting process in detail, step by step including any step that includes checkers.*
>
> *I also have a question about the software that is used, are they required to inform you what open source code they integrate into their software? for example election guard is free and integrates into any voting system, how would the public find out if this had been integrated?*
> *can you point me towards the accreditations and certifications that the election management system is required to go through?*
> *I understand catalyst makes the software, on their website they say "We also built a mechanism for electronic scanning and reading of votes, and logic into the Commission's existing system to decide the winner and act as a tiebreaker if needed."*
> *is this logic turned on for manual counts?*
> *have we ever needed to use it? why is it built in when we count manually?*
>
> *regarding the computers with the software on it, I understand they are all connected to the internet when data is entered. can you confirm if any other software is on these computers? are they built specifically for the election?*
> *do any of them have remote access software on them?"*

Answers to your questions are set out below.

Question 1 - Signed certificates & Vote Count Process

Once the results have been finalised following the completion of the official count and the Writ has been returned, Returning Officers must pack all materials away to be sent to the Office of the Clerk of the House. There they are stored securely for 6 months and can only be opened by court order. After 6 months the materials must be destroyed. You are correct that the manual count sheets are signed off but these records are with the materials now stored with the Office of the Clerk. Therefore the only certificates available are those on our website. Accordingly, this aspect of your request is refused under s 18(g) of the Act as it is not held by the Electoral Commission.

Questions 2 Open source software, Certification & Accreditation

Yes, our suppliers advise us what Open Source software is used. Our software does not integrate with the ElectionGuard software.

From time to time we receive queries from the public including OIA requests, we provide such information to the public via these channels as appropriate.

Question 3 - **Certification & Accreditation**
Our systems undergo certification and accreditation in line with NZ government guidance. The certification and accreditation process is described under section 4 of the New Zealand Information Security Manual (https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/).

This includes penetration testing of systems to ensure that data cannot be tampered with or manipulated. We adhere to best practice and industry standards to protect our systems and to ensure that we are managing our information security risks with suitable controls in place including:

- Denial of Service protection
- Firewalls
- Physical security
- Transport layer security
- Intrusion detection systems
- Incident response procedures.

Under sections 9(2)(k) and section 6(c) of the Act, copies of additional process documentation and penetration testing results are withheld as the release would increase the likelihood of compromise of the integrity of the security arrangements for elections and that this would be likely to prejudice the maintenance of the law, and the withholding of the information is necessary to prevent the disclosure or use of official information for improper gain or improper advantage and this is not outweighed by other considerations which render it desirable, in the public interest to make that information available.

While we cannot release the documents, I would be happy to discuss any questions you have on this if you would like to phone me phone (04) 495 0030.

Questions 4 -Statement on Catalyst website and Flag referendums

On the website of Catalyst IT Limited they state, "*We also built a mechanism for electronic scanning and reading of votes, and logic into the Commission's existing system to decide the winner and act as a tiebreaker if needed.*"

This statement relates to the 2015 an -2016-referendums on the New Zealand flag, specifically a referendum management system used for postal referendums, not for elections and referendums via the ballot box.

The logic referred to relates preferential voting, as used for the first flag referendum. Further information on these referendums is available via https://elections.nz/democracy-in-nz/historical-events/2015-and-2016-referendums-on-the-new-zealand-flag

Scanning and optical mark recognition (OMR) for counting has been used on postal referendums since the 2013 "Asset Sales" referendum. OMR was enhanced for the first flag referendum to allow for optical character recognition (OCR) of numeric preferential votes.

Voting papers were placed into batches of 50. The batches were then scanned and uploaded into the referendum management system. Each voter had a unique referendum ID which was recorded on their voting paper in a QR code. The referendum ID was used to mark each person off the roll as having voted. RMS used Optical Character Recognition (OCR) for the first referendum and Optical Mark Recognition (OMR) for the second referendum to capture the vote on each voting paper. Any mark on a voting paper that could not be read went to an operator for primary consideration and was escalated for review, including secondary checking and auditing as appropriate.

Questions 5 – Computers and software used

Laptops used at Electorate Headquarters are purpose-built for the election. As an Independent Crown Entity running a complex nation-wide event, several software applications are used in the day-to-day running of our organisation. Many of these are general and used throughout the public service and in private enterprise such as the Office suite of products and Outlook email. We use anti-virus, anti-malware, device management and encryption software on these laptops. Connectivity to the election management System is via direct network connection or VPN. All our systems undergo security testing and certification as described in Question 3 above.

You have the right under section 28(3) of the Act to make a complaint to the Ombudsman if you are not satisfied with the response to your requests. Information about how to do this is available at www.ombudsman.parliament.nz or by phoning 0800 802 602.

Yours sincerely

J.A. Willcocks

James Willcocks
Chief Information Officer
Electoral Commission