

23 November 2023

By email to: [REDACTED]

Dear [REDACTED]

OFFICIAL INFORMATION ACT REQUEST 2023/89

On Friday 27 October 2023 you made a request under the Official Information Act 1982 (the Act) for the following information:

How many votes were there doubles for in the previous 3 elections. How many were investigated. How many were found to be by two different people and how many by the same. How many were referred to police and what was the outcome of there investigations. A copy of the security testing and penetration testing reports of all election sytems. Electoral roll management system. Electronic roll scrutiny sytem. And UVP. For the previous 3 elections. Are the comapnies making the software and doing testing checked for foreign or possible malicious intent. Such as Qual IT Solutions Limited, Planit Software Testing Limited, Lateral Security (IT) Services Limited and Aura Information Security. Also catalyst. Or any other comapny involved in election software. Who is able to access the election sytems and is it conected to the internet. Does the new zealand security intelligemce service play any part in elections or reccomendations around elections. Or security. What agency is resposnible for making security requirments around elections. Can i get a copy of the master and supplematry role from this most recent ellection and the one before. Has there ever been any breaches in the elections system. Either internally or external security breaches in the previous 3 elections. Has there been any reports of attempted or successful hacking of the sytem by foreign or domestic entities in the past.

- 1. How many votes were there doubles for in the previous 3 elections. How many were investigated. How many were found to be by two different people and how many by the same. How many were referred to police and what was the outcome of their investigations.*

Following the 2020 general election, 637 cases of potential dual votes were investigated. Of those, 48 cases were referred to the New Zealand Police. Of those 48 cases referred to the Police, two were prosecuted and convicted.

Following the 2017 general election, 576 cases of potential dual votes were investigated. Of those, 37 cases were referred to the New Zealand Police. Of those 37 cases referred to the Police, two were prosecuted and convicted.

Following the 2014 general election, approximately 597 cases of potential dual votes were investigated. Of those, 126 cases were referred to the New Zealand Police. We are not aware of any of these cases being prosecuted by the Police.

2. *A copy of the security testing and penetration testing reports of all election systems. Electoral roll management system. Electronic roll scrutiny system. And UVP. For the previous 3 elections.*

Disclosure of this information would prejudice the Electoral Commission's ability to prevent and detect cyber security threats and may also result in exposure of the information to those who may use this information for improper gain. This gain or advantage could damage trust and confidence in the electoral system.

Therefore, this part of your request is declined under section 6(c) of the Act on the ground that making this information available would be likely to prejudice the maintenance of the law, and under section 9(2)(k) of the Act on the ground that withholding this information is necessary to prevent the disclosure or use of official information for improper gain or improper advantage.

3. *Are the companies making the software and doing testing checked for foreign or possible malicious intent. Such as Qual IT Solutions Limited, Planit Software Testing Limited, Lateral Security (IT) Services Limited and Aura Information Security. Also catalyst. Or any other company involved in election software.*

All of the companies listed above have been engaged by the Electoral Commission as Department of Internal Affairs (DIA) approved vendors from the 'Consultancy and Professional Services' government channel.

The Consultancy and Professional Services channel covers services delivered by a professionally qualified individual or business. This includes architecture, building, engineering and ICT.

Further information about the Consultancy and Professional Services channel can be found at this link <https://marketplace.govt.nz/about-marketplace/whats-open-on-marketplace/consultancy-and-professional-services/>.

4. *Who is able to access the election systems and is it connected to the internet.*

There are a number of electoral systems that, by design, are connected to the internet and available for use by members of the public. These are as follows:

URL	Used by members of the public to:
https://vote.nz/	<ul style="list-style-type: none">• enrol, check or update their enrolment details using a New Zealand driver licence, New Zealand passport or RealMe verified identity• access other ways to enrol without a New Zealand driver licence, New Zealand passport or RealMe verified identity• download voting papers for qualifying overseas and remote voters

	<ul style="list-style-type: none"> upload voting papers for qualifying overseas and remote voters
https://www.electionresults.govt.nz/	<ul style="list-style-type: none"> view the results of electoral events
https://elections.nz/	<ul style="list-style-type: none"> seek information and access resources regarding elections apply to work at the Electoral Commission

Systems used by political parties to access election resources, provide nominations for individual electoral candidates and submit party lists to the Electoral Commission are connected to the public internet but access is restricted to authorised users only.

Other electoral systems used by the Electoral Commission are not accessible via the public internet and access is restricted to authorised users only.

5. Does the new zealand security intelligence service play any part in elections or recommendations around elections. Or security.

The NZSIS does not have any input into or make any recommendations regarding elections. Representatives from the NZSIS contribute to all-of-government risk and threat assessments. These assessments help inform the Electoral Commission's approach to security.

6. What agency is responsible for making security requirements around elections.

The Electoral Commission is responsible for the security of the voting process during an election. This includes the security of materials, staff, and voters in a voting place. If there is an incident that reaches the threshold for criminal activity or threatens public safety, this will be referred to Police.

7. Can I get a copy of the master and supplementary roll from this most recent election and the one before.

Master rolls, showing the name of voters for each electoral district, including special voters, are compiled for each election. A master roll for an electoral district can only be inspected by a registered elector of the district in the office of the Electoral Commission for the district until the next general election.

The master rolls for the 2023 General Election can be inspected at our offices in accordance with section 187(5) of the Electoral Act 1993.

The master rolls for the 2020 General Election are no longer available, in accordance with section 187(4) of the Electoral Act 1993.

The Commission produces printed electoral rolls each year, with the names and addresses of registered electors in each district, in accordance with section 104 of the Electoral Act 1993.

Printed copies of the 2023 General and Māori electoral rolls can be inspected at our offices and public libraries. In accordance with section 110 of the Electoral Act the 2023 rolls are also available for sale. The cost of an electoral roll is \$30.20 incl. GST (or \$10.90 incl. GST if it is for an electoral purpose). Please email rolls@elections.govt.nz if you want to purchase 2023 printed rolls.

8. *Has there ever been any breaches in the elections system. Either internally or external security breaches in the previous 3 elections.*

There have been no successful hacking attempts or data breaches of Electoral Commission systems. We do not disclose information regarding attempted hacking as this would prejudice the Electoral Commission's ability to prevent and detect cyber security threats and may also result in exposure of the information to those who may use this information for improper gain. This gain or advantage could damage trust and confidence in the electoral system.

Therefore, this part of your request is declined under section 6(c) of the Act on the ground that making this information available would be likely to prejudice the maintenance of the law, and under section 9(2)(k) of the Act on the ground that withholding this information is necessary to prevent the disclosure or use of official information for improper gain or improper advantage.

9. *Has there been any reports of attempted or successful hacking of the system by foreign or domestic entities in the past.*

Please see above answer.

In the interests of transparency, we release responses to Official Information Act requests every 3 months. We will publish this response with your personal details redacted.

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 request. Information about how to do this is available at www.ombudsman.parliament.nz or by phoning 0800 802 602.

Yours sincerely



Kristina Temel
Manager, Legal and Policy