ELECTORAL COMMISSION
TE KAITIAKI TAKE KŌWHIRI

23 November 2022

[redacted]
By email to: [redacted]

Dear [redacted]

OFFICIAL INFORMATION ACT REQUEST 2022/35

On 26/10/22 you made a request under the Official Information Act 1982 (the OIA) for the following information:

1. *...in relation to the 2017 and 2020 General Election.*
   A detailed list of any and all cyber-attack attempts on the Commission's election management systems.
   With specifics:
   Location
   Attempt type and success
   Action taken by EC
   Dated between 2017 and 2022

2. *Any and all assessments and reports relating to cyber-attack attempts on the Commission's election management systems.*

3. *A detailed list of any and all interference attempts (foreign or otherwise) on the Commission's election management systems.*
   With specifics:
   Location
   Attempt type and success
   Action taken by EC
   Dated between 2017 and 2022

4. *Any and all assessments and reports relating to interference attempts (foreign or otherwise) on the Commission's election management systems.*

5. *A summary of spending of the budgeted $8 million provided specifically for the additional security and resilience measures for the 2020 election.*

6. *A copy of any and all advice prepared by the Electoral Commission in relation to security for the elections described above.*

Responses to each part of your request are provided below:

Items 1, 2 and 3

Like all organisations, attempts are regularly made to find vulnerabilities in the Electoral Commission's systems, for example, phishing, credential sign-ons, and automated scanning by bots. We always need to be prepared for the possibility of interference or cyber threats.

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.

The Electoral Commission works with other government agencies to prepare for elections including the Ministry of Justice, the Department of Prime Minister and Cabinet, Government Communications Security Bureau and the New Zealand Security Intelligence Service. As outlined below, before the 2020 General Election detailed protocols were developed setting out how agencies would work together in the event of a disruption to the 2020 General Election.

As has been widely reported, we can confirm that there were no successful attacks on the Electoral Commission's systems during the election period and the interagency election protocols were not triggered.

We are unable to provide further details of attempts and reports into this work as to do so might disclose aspects of our capabilities which could be of benefit to malicious actors. Under sections 9(2)(k), 6(a) and 6(c) of the Act, copies of additional documentation 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. The withholding of the information is also 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 or in the public interest to make that information available

Items 5

A summary of spending of the budgeted $8 million provided specifically for the additional security and resilience measures for the 2020 election follows.

There was approximately ($7.9m) additional spending on security and resilience measures made up of:

- ($2.5m) on IT security including certification, accreditation and penetration testing; cyber security specialist advice; denial of service protection; and additional personnel cost.
- ($5.4m) additional physical security measures, including security guards; specialist security advice and site evaluations; site security measures and remedial work; staff training, personnel and equipment; and security of materials.

Items 4 and 6

Some of the information that falls within your request is already available in the public domain and can be found at:

- April 2018: Report of the Electoral Commission on the 2017 General Election
- 30 August 2018: Electoral Commission - Submission on the Inquiry into the 2017 General Election and 2016 Local Elections
- 6 May 2019: Advice on the security of online voting
- May 2021: Report of the Electoral Commission on the 2020 General Election and referendums
- June 2021: NZSIS - Director-General remarks: Justice Committee Inquiry into the 2020 General Election and Referendums

I have also attached the following:

- Paper for the Minister on Electoral Commission Plans for managing an emergency affecting the 2017 election (Appendix 1)
- Advice for parties on cyber-security 2017 (Appendix 2)
- copies of relevant documents regarding advice to political parties in 2020. (See Appendix 3). In the emails entitled 'Cyber security information for political party secretaries', the names and email addresses of some persons have been withheld under section 6(a) of the Act because the making available of the information would be likely to prejudice the security or defence of New Zealand.

The Electoral Commission worked on interagency protocols on the management and response to election disruptions and communications related to the 2020 General Election process. These protocols were made between the Electoral Commission and the Department of the Prime Minister and Cabinet and the Ministry of Justice in close consultation with an inter-agency 2020 General Election Senior Officials Committee. This Committee, chaired by the Chief Electoral Officer as Chief Executive of the Electoral Commission, included representatives from the Ministry of Justice, Department of the Prime Minister and Cabinet (including the National Emergency Management Agency and Cabinet Office), Government Communications Security Bureau, New Zealand Security Intelligence Service, Department of Internal Affairs, Te Puni Kōkiri, Ministry of Foreign Affairs and Trade, Crown Law, and New Zealand Police.

These protocols include information relevant to your request. Copies of these protocols are available here.

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

J.A. Willcocks

James Willcocks
Chief Information Officer
Electoral Commission