



16 August 2021

Scott

By email: fyi-request-15848-b83b2a3d@requests.fyi.org.nz

Reference: OIA-2020/21-0696

Dear Scott

Official Information Act request relating to cyber security

I refer to your request made under the Official Information Act 1982 (the Act), received by the Department of the Prime Minister and Cabinet (DPMC) on 21 June 2021. You requested:

“...ONE: I request a copy of the evaluation report and corrective action plan for the DPMC-led cyber security incident response exercise ACTUATOR, conducted November 2018 through the National Exercise Programme.

TWO: The Cyber Security Strategy Action Plan 2016 mandates “twice yearly inter-agency exercises, including with the private sector and international partners.”

I request the following information for every inter-agency cyber security exercise conducted since the beginning of 2019:

- *The name of the exercise*
- *The date it was conducted (month and year)*
- *The identity of every participating agency or organisation*
- *A description of the scenario covered*

THREE: The Cyber Security Strategy 2019 mandates the production of an annual Cyber Security Strategy work programme. I request a copy of the latest work programme.

FOUR: I request a copy of the Cyber Security Emergency Response Plan...

I note the timeframe for responding to your request was extended by 20 working days, to allow for further consultation to take place. Following this, I am now in a position to respond.

With regard to part one of your request, for a copy of the evaluation report and corrective action plan relating to Exercise ACTUATOR, I have decided to withhold the evaluation report under the following sections of the Act:

- Section 9(2)(f)(iv), to “maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials”, and
- Section 9(2)(g)(iv), to “maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any public service agency or organisation in the course of their duty”.

I can however advise that the four key points arising from the exercise were:

- Transfer responsibility of exercise planning and execution to a response agency;
- Amend the Cyber Security Emergency Response Plan (CSERP) to better acknowledge the role of the private sector;
- Release a public version of the CSERP; and
- Explore options for enhanced interagency engagement and coordination.

With regard to the part of your request for the Exercise ACTUATOR Corrective Action Plan, I must refuse this part of your request under section 18(e) of the Act, as this document does not exist. Although there were intentions to prepare a Corrective Action Plan, it was ultimately overtaken by national security events, including the events of 15 March 2019. However, the key points noted above, and lessons learnt from subsequent incidents and events, continue to be incorporated into agency processes. These are reflected in the Cyber Security Emergency Response Plan (CSERP).

With regard to part two of your request, no DPMC-led cyber security exercises have taken place as part of the National Exercise Programme since 2019, due to the number of real-life incidents and events, including the response to the COVID-19 pandemic and subsequent cyber considerations. The next exercise on the National Exercise Programme is planned for November 2021.

With regard to part three of your request, work programmes were produced for the 2019/20 and 2020/21 years. The work programmes focus on additional activities to business as usual and ongoing functions of agencies supporting New Zealand's cyber security.

A prioritised Cyber Security Strategy implementation work programme for 2020/21 was considered by the Security and Intelligence Board in late 2020, as recommended by the inter-agency Cyber Security Strategy Coordination Committee. The initiatives were agreed to be immediately progressed (following a costed project plan, including people resourcing/contractor requirements where necessary). The 2020/21 work programme is outlined below:

Awareness

- Translate CERT NZ resources into commonly spoken languages in New Zealand.
- Procure research on how to best target cyber security awareness campaigns.
- Additional funding for awareness campaigns (funding of \$200,000 has already been allocated to continue MBIE's Trade Smart campaign in response to risks around COVID-19).

Workforce

- Funding for a cyber security trades training industry liaison role.
- Including cyber security in current digital career outreach events.

Resilience

- Funding for a National Cyber Security Exercise.

Cyber crime

- Budapest Convention policy work (ongoing funding).
- Procure research on the cyber crime risk landscape.

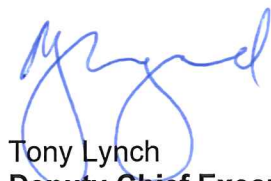
With regard to part four of your request, for a copy of the Cyber Security Emergency Response Plan (CSERP), the Security and Intelligence Board approved the most recent version of this document in July 2021. This version can be found on DPMC's website at the following address: <https://dpmc.govt.nz/publications/new-zealands-cyber-security-emergency-response-plan>. Accordingly, I am refusing this part of your request under section 18(d) of the Act, as the information requested is publicly available.

In making my decision, I have taken the public interest considerations in section 9(1) of the Act into account.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on DPMC's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely



Tony Lynch
Deputy Chief Executive
National Security Group