DEPARTMENT OF THE
PRIME MINISTER AND **CABINET**
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

2 August 2021

[redacted]

Reference: OIA-2020/21-0644
And OIA-2020/21-0645

Dear [redacted]

Official Information Act requests relating to cyber security

I refer to your queries, received by the Department of the Prime Minister and Cabinet (DPMC) as requests made under the Official Information Act 1982 (the Act) on 4 June 2021. As noted in my response to you dated 5 July 2021, I decided to combine my response to your requests as below. You requested:

> *"…under the OIA pls provide the two latest NCPO's advisories or similar to the Minister for the Digital Economy and Communications that contain information cyber security policy that pertains to the health sector, and the two latest advisories or similar that contain information specific to the health sector (DHBs, PHOs etc)…"*
>
> And
>
> *"…The NZ cyber security strategy 2019 says "An annual work programme" will be produced.*
> *1. Pls provide these annual work programmes (as many as there are, as far back as they go), dated.*
>
> *It also says the responsible Minister will release a public annual report on progress in each priority area.*
> *2. Pls provide these annual reports (as many as there are, as far back as they go), dated*
>
> *NCPO oversees the implementation of the strategy*
> *3. Pls detail its obligations outlined under that strategy*
> *4. Has NCPO fulfilled each obligation outlined under that strategy, and on time, since 2015?*
>
> *NCPO provides cyber security advice to the responsible Minister…*
> *5. Pls provide its latest substantive advice regards DHBs/the public health sector generally (PHOs etc)*
>
> *Re the NSCS (pls transfer this request if need be)*
> *6. Pls list those critical national infrastructure organisations the NSCS has engaged with*
>
> *7. Pls describe the outcome of that engagement*

Executive Wing, Parliament Buildings, Wellington, New Zealand 6011
☎ 64 4 817 9698 www.dpmc.govt.nz

8. Pls list those govt agencies the NSCS has engaged with to share best practice, since start of 2019

Re the annual reports on system-wide capability and maturity in privacy and protective security of government agencies, to the Public Service Minister

9. Pls list what contributions to these reports (first done in 2016) or their subsequent iterations, have come from the agencies the DPMC and NZIC oversee…"

I note my previous response to you advised that advice provided by the National Cyber Policy Office (NCPO) is at a strategic level, rather than operational, and that tailored advice specifically regarding the health sector has therefore not been provided to the Minister for the Digital Economy and Communications by NCPO. My response advised, however, that more general advice regarding cyber ransoms has been provided by NCPO.

My previous response also advised that, although New Zealand's Cyber Security Strategy 2019 states an annual report will be prepared by the responsible Minister, an annual report has not been produced as some of the initiatives under the Cyber Security Strategy were slowed or deferred. An annual report will be produced for 2021/22.

I noted that it would have been necessary to transfer parts 6 – 9 of your request, relating to the National Cyber Security Centre (NCSC), to the NCSC by way of the Government Communications Security Bureau (GCSB), had you not already requested this information directly from the relevant party. Further, I advised that the timeframe for responding to the remainder of your request (parts numbered 1, 3, 4 and 9, in so far as it relates to DPMC), were extended under section 15A of the Act to allow for further consultation to be undertaken. Following this, I am now in a position to respond.

With regard to part one 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.

The Cyber Security Strategy Work Programme 2019/20 is outlined in a Cabinet Paper of the same name. Please find a copy of this document enclosed. Some information has been withheld under the following sections of the Act:

- Section 6(a), as the making available of that information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand,
- 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)(i), 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.

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 listed below 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 three and four of your request, NCPO is responsible for coordinating the Cyber Security Strategy's implementation. The NCPO has a governance reporting and coordination role for the Cyber Security Strategy work programme, as well as leading several projects. NCPO also chairs an interagency cyber working group. This is alongside the NCPO's role of leading the development of cyber security policy advice and providing advice to the government on investing in cyber security activities.

The NCPO's general delivery against obligations is reported within DPMC's annual reports. Outstanding initiatives in the work programme have been rolled over for completion in the 2021/22 financial year.

In regard to previous strategies, one report was released against the Cyber Security Strategy 2015, which is available on DPMC's website at:

New Zealand's Cyber Security Strategy Action Plan Annual Report 2016 | Department of the Prime Minister and Cabinet (DPMC)

With regard to the part of your request in part nine, for DPMC to "*list what contributions to these reports (first done in 2016) or their subsequent iterations, have come from the agencies the DPMC and NZIC oversee*", for the "*annual reports on system-wide capability and maturity in privacy and protective security of government agencies, to the Public Service Minister",* DPMC does not oversee any agencies that have made contributions to these reports. I am accordingly refusing this part of your request under section 18(e) of the Act, as "the document alleged to contain the information requested does not exist". DPMC has, however, undertaken completed privacy and protective security self-assessments as noted in the public reports found on the Public Service Commission website.

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

~~RESTRICTED~~
~~BUDGET SENSITIVE~~

Office of the Minister of Broadcasting, Communications and Digital Media

Chair, Cabinet Governance Administration and Expenditure Review Committee

CYBER SECURITY STRATEGY WORK PROGRAMME 2019/20

Proposal

1. This paper reports back with the 2019/20 work programme to deliver the Cyber Security Strategy 2019.

Background

2. Cabinet approved a refreshed Cyber Security Strategy in November 2018 [CAB-18-MIN-0562]. The strategy has five priority areas:

   2.1. Cyber security aware and active citizens

   2.2. Strong and capable cyber security workforce and ecosystem

   2.3. Internationally active

   2.4. Resilient and responsive New Zealand

   2.5. Proactively tackle cybercrime

3. The Cabinet Economic Development Committee invited the Minister of Broadcasting, Communications and Digital Media to report back to Cabinet in 2019 with a work programme to deliver the strategy, including a range of further actions to advance the priorities above [DEV-18-MIN-0256].

4. The strategy was released publicly in July 2019, following Budget decisions. The strategy outcomes, priorities and key areas of focus are listed at Annex A.

Delivery of priority actions is underway

5. The 2018 Cabinet paper included seven priority actions to deliver the strategy. Of these, three funded actions are underway and initiatives to enable the sector to work together more effectively have progressed, as described below.

Enhancing New Zealand's capacity building activities in the Pacific

6 In September 2019, the Deputy Prime Minister and I announced a programme providing $10 million over five years to support Pacific countries to develop national cyber security strategies, secure infrastructure and data, enhance online safety, and implement robust cybercrime laws across the Pacific. Planning for delivery of this programme is under way. As part of this work, a Pacific Partnerships Coordinator role has been established within CERT NZ.

Strengthening New Zealand's posture in response to malicious cyber incidents

7. The release of a strengthened narrative in the Cyber Security Strategy 2019 provided an important signal of New Zealand's policy to international partners. Ministers and officials have reiterated this message in our related international engagements.

8. The Director-General of GCSB, alongside international partners, released a statement in December 2018, publicly linking the Chinese Ministry of State Security to a global campaign of cyber-enabled commercial intellectual property theft.

Improving the security of our most important national assets

9. The GCSB's National Cyber Security Centre (NCSC) has continued work to scale the benefits of its cyber defence capabilities through the provision of the new Malware Free Networks (MFN) service to an expanded range of nationally significant organisations.

10. In the past 12 months, the NCSC has used its cyber defence capabilities, and its international relationships to respond to a range of significant, potentially high impact cyber security incidents, and to help develop proactive guidance which has reduced the impact in New Zealand of known global cyber campaigns.

11. The NCSC is also building on its baseline assessment of nationally significant organisations' cyber security resilience levels (published in 2018), through the production of guidance for business leaders and practitioners, to assist them to more effectively plan, implement and monitor cyber security initiatives across the organisations for which they are responsible.

12. Through the GCSB Director-General's role as Government Chief Information Security Officer, there is a more strategic approach to identifying security risk, and working across agencies to ensure effective responses to that risk from a Government perspective. This includes identifying technical responses, and making sure we have effective policy settings across government.

Working together more effectively

13. A new cross agency Cyber Security Strategy Coordination Committee has been established to plan, govern and monitor the annual work programme.

14. Budget 2019 also established a joint appropriation under Vote DPMC to deliver the strategy.

Reprioritisation to reflect funding constraints

15. The remaining four priority actions require funding. Budget 2019 delivered $2 million per annum over four years for strategy implementation. 9(2)(f)(iv), 9(2)(g)(i) 9(2)(f)(iv) and led to a reprioritisation exercise. This exercise took into account resource constraints, and environmental factors 6(a)

Work programme for 2019/20

16. The work programme for 2019/20 is a result of the reprioritisation exercise. It consists of seven initiatives to be funded through the joint appropriation. These are detailed at Annex B. The work programme focuses on initiatives that are relatively easy to

implement (quick wins) in the next six months and will set up the sector for future delivery against the strategy.

17. The initiatives are:

    17.1. identification of optimal targeting for future awareness campaigns;

    17.2. a joint workforce initiative with industry partners focused on schools;

    17.3. a refreshed international engagement plan;

    17.4. a fund to support civil society attendance at international meetings on cyber security issues;

    17.5. progress towards accession to the Council of Europe Convention on Cybercrime (the Budapest Convention);

    17.6. establishment of a cyber security coordinator; and

    17.7. advice on establishment of a collaboration forum (with private sector, civil society and government representation).

18. Key milestones for these initiatives are detailed at Annex C.

19. The total cost of the work programme is estimated at around 9(2)(f)(iv) . 9(2)(f)(iv) Officials are currently developing a detailed plan for the 2020/21 financial year.

Other initiatives that contribute towards strategy implementation

20. The initiatives above will be funded through the joint appropriation for strategy implementation. However, there is a significant amount of work underway or planned in other work streams and within individual portfolios that will contribute to strategy outcomes. This work is listed at Annex D, to provide Ministers with clarity on work underway across the sector, and upcoming decision points.

Consultation

21. This paper was drafted by the Department of the Prime Minister and Cabinet. The Department of Internal Affairs, Government Communications Security Bureau, Ministry of Business, Innovation and Employment, Ministry of Defence, Ministry of Foreign Affairs and Trade, Ministry of Justice, New Zealand Defence Force, New Zealand Police, and State Services Commission have been consulted.

Financial, Legislative, Human Rights, Gender Implications, and Disability Perspective

22. There are no implications.

Publicity

23. I will release a public annual report on progress under each of the strategy's priority areas, including against the 2019/20 work programme, by December 2020.

Proactive Release

24. This paper will be publicly released, with some redactions (including of Budget sensitive matters) within 30 business days of a final decision being taken by Cabinet.

Recommendations

25. I recommend that the Committee:

1. note that on 7 November 2018, the Cabinet Economic Development Committee invited the Minister of Broadcasting, Communications and Digital Media to report back to Cabinet in 2019 with a work programme to deliver the five priorities in the Cyber Security Strategy [DEV-18-MIN-0256];

2. note that work is underway to deliver priority actions under the strategy;

3. note that some actions have been reprioritised to reflect resource constraints, and events since the strategy was approved in 2018;

4. note that the Cyber Security Strategy work programme for 2019/20 will consist of:

    4.1. identification of optimal targeting for future awareness campaigns;

    4.2. a joint workforce initiative with industry partners focused on schools;

    4.3. a refreshed international engagement plan;

    4.4. a fund to support civil society attendance at international meetings on cyber security issues;

    4.5. progress towards accession to the Council of Europe Convention on Cybercrime (the Budapest Convention);

    4.6. establishment of a cyber security coordinator; and

    4.7. advice on establishment of a collaboration forum.

5. note that significant additional work is underway across government that will also contribute to strategy outcomes; and

6. note that I will provide a public report at the end of the financial year on progress under each of the strategy's priority areas, including against the work programme for 2019/20.

Authorised for lodgement
Hon Kris Faafoi
Minister of Broadcasting, Communications and Digital Media