Hon Andrew Little

Minister of Health
Minister Responsible for the GCSB
Minister Responsible for the NZSIS
Minister for Treaty of Waitangi Negotiations
Minister Responsible for Pike River Re-entry
Lead Coordination Minister for the Government's Response to the Royal Commission's Report into the Terrorist Attack on the Christchurch Mosques

5 July 2022

Scott

By email: fyi-request-19608-e7a064af@requests.fyi.org.nz
Ref: ALOIA216

Dear Scott

Response to your request for official information

Thank you for your request under the Official Information Act 1982 (the Act) on 7 June 2022. You asked:

> *"…I would like to make a request for the following information relating to the inquiry into the Waikato DHB ransomware attack commissioned by your office.*
> *ONE: A copy of the inquiry terms of reference*
> *TWO: The identity of the reviewer (if not included in the terms of reference)*
> *THREE: Copies of all briefings the minister has received on the topic of the inquiry"*

Please find a copy of the terms of reference attached to this letter. This has been released to you in full. The review was undertaken by InPhySec Security. Regarding part three of your request for all briefings I have received on this topic, this is refused under section 18(d) of the Act as information requested will soon be publicly available following the release of the independent report.

Under section 28(3) of the Act, you have the right to ask the Ombudsman to review any decisions made under this request. The Ombudsman may be contacted by email at: info@ombudsman.parliament.nz or by calling 0800 802 602.

Yours sincerely

Hon Andrew Little
Minister of Health

Private Bag 18041, Parliament Buildings, Wellington 6160, New Zealand
+64 4 817 8707 | a.little@ministers.govt.nz | beehive.govt.nz

Independent Review Terms of Reference: Health response to the Waikato DHB ransomware incident

1. Purpose

This review will provide advice to the Minister of Health, the Chief Executive of Waikato DHB, and the Ministry on what can be learnt from the Waikato DHB ransomware attack, vulnerabilities in the IT services and planning, and recommended actions that will minimise future risk and strengthen the cyber resilience of New Zealand's health and disability system.

2. Context

On the 18 May 2021, Waikato DHB suffered a ransomware attack which compromised IT services. The cyber-attack impacted many areas of the health services that the Waikato DHB provide to the community. The Waikato DHB stood up an incident response and the Ministry of Health provided national leadership to the incident, with input from other key agencies including the National Cyber Security Centre. The incident response focused on:

- Managing health service delivery.
- IT service restoration.
- Assessing privacy impacts and notifying impacted individuals as appropriate.
- Cyber security incident investigation and response

3. Scope

The scope of the review is on two areas to be assessed, evaluated and reported on. In addition, outcomes are provided to detail the purpose and objectives for each topic within the review.

The topics, details of what will be reviewed, and their outcomes are as follows:

1. Waikato DHB risk assessment and controls prior to the breach

a. Capability and level of resource: including experienced security staff performing security related governance, risk and compliance (GRC) tasks and operational security related tasks.
b. Information management: Including the policies and procedures for classifying information assets, understanding the business service impact of data loss or service disruption, preventative and detective measures to detect data loss of high-risk information assets, information governance frameworks and polices in place, and staff awareness and training.
c. Information security controls: implementation of industry standard security controls including such things as logical access controls, monitoring controls, change control, software update and vulnerability management, and platform resilience.
d. Technical architecture: how the technical environment was designed and deployed to mitigate and manage security risks, including what stops a security event affecting other systems such as an entire DHB or the wider health sector. The review should include how future system changes are implemented as not to introduce new security risks or undo existing security controls.
e. Governance: IT services risk management and reporting and KPIs, roles and responsibilities, budgeting and funding, governance, strategy and roadmap development, on-going security assurance, reporting scope and regularity to the DHB's senior leadership team and governors.

Outcome: Identification of any cyber resilience vulnerabilities DHB had prior to the breach that can be mitigated in other DHB health and disability systems to strengthen the resilience of the sector.

2. WDHB IT service restoration

a. Governance and decision making: The governance and decision making that determined the process for prioritisation of IT services to be restored.
b. Timeliness: The timeliness of the IT service restoration process was appropriate.
c. Restoration: Evaluate supporting documentation relating to the planned safe restoration of servers.
d. Awareness of risk: The level of awareness of the potential risk exposure and guidelines including staff working practices and operational security monitoring.
e. Expert assistance: The use of experienced experts to help ensure the restoration of services occurs quickly and without creating any further risk of another security breach.

Outcome: Strengthen the process and mechanisms of IT service restoration within the health and disability system.

Out of scope

The scope of this review does not include:

- The criminal investigation of the cyber-attack.
- Attribution of any contributing factors to specific individuals involved in the incident.
- Non-IT impacts of the breach, including how privacy was managed and or health service delivery impacts.
- The overall response model, communications and engagement approach used to support response efforts
- Concurrent incident responses (eg, NICU outbreak, COVID-19)

4. Stakeholders to be interviewed

The following organisations will be consulted as part of this review:

a) Minister of Health
b) Ministry of Health
c) Waikato District Health Board
d) Local Member of Parliament
e) National Cyber Security Centre
f) NZ Police
g) Office of the Privacy Commissioner
h) HealthShare
i) Ernst and Young
j) Clyde and Co
k) Regional DHBs affected by the incident

Where the stakeholder's area of expertise is deemed out of scope of the review their interview will focus only on those items in scope as outlined in section 3.

5. Accountability

Group members are responsible for reporting back to (Minister of Health or other as required).

6. Review

The group review is to start the review post the recovery activities (estimate date February 2022 as confirmed) and complete by April 2022.

The review will be completed by an experienced member of the Department of Internal Affairs Security and Related Services panel.