A16888332

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

19 January 2023

Scott
fyi-request-21401-d9173ec7@requests.fyi.org.nz

Tēnā koe Scott

Official Information Act request

Thank you for your Official Information Act 1982 (OIA) request of 12 December 2022 to the Government Communications Security Bureau (GCSB) seeking a report provided to InPhySec on the Waikato DHB ransomware incident.

Response

As allowed under section 16(1)(e) of the OIA, I am enclosing a summary of the *Incident Analysis Report (IAR-2021-2589) Redacted Version*, to protect the interests covered in the following sections of the OIA:

- section 6(a), as the making available of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; and
- section 9(2)(ba)(i), as the withholding of the information is necessary to protect information, which is subject to an obligation of confidence or which any person has been, or could be, compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied.

Under sections 11 and 12 of the Intelligence and Security Act 2017 (ISA), the GCSB may provide, to certain entities, protective security services, advice and assistance relating to the protection, security and integrity of communications and information infrastructures of importance to the New Zealand Government.

The National Cyber Security Centre (NCSC), within the GCSB, has a function to respond to cyber security incidents of potential national significance. The release of this report in full would hinder the NCSC's ability to carry out this function as other entities would likely not be as forthcoming with necessary information. It is therefore within the public interest for this report to be withheld and a summary to be provided.

Furthermore, hindering the NCSC's ability to carry out their functions would be likely to prejudice New Zealand's national security. Information within this report could reveal our operational methods and capabilities.

Review

If you wish to discuss this response with us, please feel free to contact information@gcsb.govt.nz.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Ngā mihi

Lisa Fong
Te Tumu Whakarae Rangitahi mō Te Tira Tiaki
Acting Director-General, GCSB

Summary: Incident Analysis Report (IAR-2021-2589) Redacted Version

Summary prepared under section 16(1)(e) of the OIA in order to protect the interests of sections 6(a) and 9(2)(b)(i).

On 18 May 2021, the Waikato District Health Board (WDHB) contacted the National Cyber Security Centre (NCSC) to report a ransomware incident impacting WDHB IT systems. The NCSC provided incident management, digital forensics and communications support to WDHB to support the following key objectives:

- Determine the initial vector of compromise used by the malicious actor to gain access to the WDHB network.
- Determine the scope of the incident to assess the period of compromise and which WDHB systems may have been accessed.
- Determine the impact to WDHB data assets and identify signs of data exfiltration from the WDHB network.
- Provide cyber security advice and guidance to support WDHB in recovering from the ransomware incident.
- Help inform the assessment of risk to the wider domestic health sector.

Among other things, forensic analysis of WDHB systems determined:

- the system was compromised by a legitimate WDHB user account and used this access to connect to WDHB infrastructure on 10 May 2021,
- a number of actions across the WDHB network were affected, and
- WDHB data had been exfiltrated.

The NCSC assessed information at a forensic level and provided findings to WDHB as they became available.