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

A11667985

30 October 2020

Connor Miller
fyi-request-13895-d391d54b@requests.fyi.org.nz

Dear Connor,

Official information request regarding cyber attacks against NZX

I refer to your Official Information Act 1982 (OIA) request dated 1 October 2020 for all information the Government Communications Security Bureau (GCSB) holds on the recent cyber attacks on the New Zealand Stock Exchange (NZX). After subsequent communication with my office on Monday 5 October, you agreed to refine the scope of this request to all information provided to the Minister Responsible for the GCSB regarding the cyber attacks on the NZX.

You also requested "a copy of the statement regarding the privacy and security of New Zealand before and after the attacks occurred and a statement with information recommending what the NZX does in future to better protect itself."

Information provided to the Minister of the GCSB regarding the NZX cyber attacks

Between 28 August and 18 September 2020, the GCSB provided Minister Andrew Little with five briefing notes and an aide memoire about the Denial of Service (DoS) cyber attacks against the NZX. The Minister also received verbal briefings from GCSB staff, as well as written talking points to assist with media engagement.

I have chosen to make this information available by giving a summary of the contents of the original documents in accordance with sections 16(1)(e) and 16(2)(c) rather than providing copies of those documents to you in full.

This is because some of the information contained in those documents has been withheld on the following grounds:

- 6(a), where 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;
- 6(b)(i), where the making available of the information would be likely to prejudice the entrusting of information to the New Zealand government by the government of any other country or any agency of such government;
- 9(2)(b)(ii) – release of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information;
- 9(2)(ba)(i) – 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.

Please find a summary of the information provided to the Minister Responsible for the GCSB regarding the NZX cyber attacks attached.

Statements regarding privacy and security of New Zealand and NZX protection

I must refuse your request for "a copy of the statement regarding the privacy and security of New Zealand before and after the attacks occurred and a statement with information recommending what the NZX does in future to better protect itself." This request is refused under s18(e) of the OIA, as the documents requested do not exist.

The National Cyber Security Centre (NCSC) did produce some general security advice for New Zealand organisations about protecting against ongoing DoS campaigns. If you are interested, you can read more here: https://www.ncsc.govt.nz/newsroom/general-security-advisory-ongoing-campaign-of-dos-attacks-affecting-new-zealand-entities/.

If you are interested in learning more about the cyber threats impacting New Zealand, you can find the NCSC Cyber Threat Report online at https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2018-2019.pdf.

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.

Yours sincerely

Andrew Hampton
Te Tumu Whakarae mō Te Tira Tiaki
Director-General, Government Communications Security Bureau

Information provided to the Minister for the GCSB about NZX Cyber Attacks

Denial of Service attacks against NZX

- The NZX were subject to Denial of Service (DoS) attacks on multiple days between 25 August and 16 September.
- A DoS attack is designed to overwhelm websites by generating excessive volumes of otherwise seemingly legitimate web requests for the purpose of stopping, or limiting, any genuine web browser requests for the website.
- This activity impacted the NZX's public website (NZX.com) which resulted in trading being halted on the 25th, 26th, 27th, and 28th August.
- The nature of DoS attacks means that internet service and external security providers are best placed to provide and implement technical mitigations.
- While DoS attacks are common, those targeting NZX were large and within the top 10% of DoS attacks globally.
- NCSC assessed it was likely the perpetrator of the cyber activity was a financially motivated cyber-crime actor.

GCSB involvement in the response

- New Zealand's national security system was activated to coordinate the all of government response to this incident, with the GCSB's National Cyber Security Centre (NCSC) acting as the Government's lead.
- Other government agencies involved in the response were CERT NZ, New Zealand Police, the Department of Prime Minister and Cabinet, Financial Markets Authority and the Ministry of Business, Innovation and Employment.
- NCSC engaged with NZX to understand the controls that NZX were putting in place to mitigate the ongoing DoS attacks and to provide cyber security advice.
- NCSC also engaged with a range of other organisation in both the public and private sectors to source information and provide coordination regarding the DoS attacks.
- NCSC issued cyber security advisories on DoS activity to a variety of organisations, as well as issuing general advice through its website.