Te Tira Tiaki
Government Communications Security Bureau

Te Pā Whakamarumaru
New Zealand Security Intelligence Service

14 June 2024

Scott
fyi-request_26349_84f309ad@requests.fyi.org.nz

Tēnā koe Scott

Official Information Act request

Thank you for your Official Information Act 1982 (OIA) request of 7 April 2024 to the New Zealand Security Intelligence Service (NZSIS). As the document you requested relates to both the NZSIS and the Government Communications Security Bureau (GCSB), and our agencies share some joint functions relevant to your request, we have prepared a joint response. Your request asked for the following:

> *"...I would like to request a copy of the 2011 NZSIS briefing to the incoming minster/Prime Minister (which I understand was a joint briefing with the GCSB).*
>
> *In terms of Section 16(2) of the OIA my preference is to receive a copy of this document, rather than an excerpt or summary..."*

We note you were advised on 6 May 2024 that the time limit for responding to your request was extended to 18 June 2024, to allow the consultations necessary to make a decision on your request to conclude, and due to the volume of information searched in responding to your request. In considering this, it may be helpful to note that our systems have changed since this document was prepared, and that it was drafted by multiple agencies.

Response

Please find a copy of Briefing Note *Advice for Incoming Prime Minister on the New Zealand Intelligence Community,* dated 9 December 2011, enclosed. As you may be aware, the core New Zealand Intelligence Community (NZIC) is comprised of the GCSB, NZSIS, and National Assessments Bureau within the National Security Group at the Department of the Prime Minister and Cabinet (DPMC). Some further information about the NZIC can be found online at: https://www.nzic.govt.nz.

The NZIC prepared this briefing for Rt Hon John Key, who in addition to retaining responsibility for all national security aspects of the Prime Minister portfolio following the 2011 General Election, also continued to hold Ministerial responsibility for the GCSB and NZSIS. This combined briefing accordingly incorporated material from the GCSB, NZSIS, and the DPMC unit then known as the Intelligence Co ordination Group.

Some information has been withheld in this briefing as marked under the following section 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.

In assessing this document for release, we were interested to note how our approach to briefings for incoming Ministers has evolved over the years. If of interest to you, the most recent Briefing to the Incoming Minister Responsible for the GCSB and NZSIS can be found online through the following links:

- https://www.gcsb.govt.nz/information-releases/proactive-information-releases
- https://www.nzsis.govt.nz/information-releases/proactive-information-releases

Given the GCSB and NZSIS's shared functions include Financial Services, and a combined policy team, we continue to provide a combined briefing for incoming Ministers on behalf of both our agencies. However, our agencies also continue to collaborate with DPMC to provide advice as appropriate. We understand DPMC's Briefing to the Incoming for National Security and Intelligence is available through the following link:

- https://www.dpmc.govt.nz/sites/default/files/2024-02/bim-2023-national-security-intelligence.pdf

Review

If you would like to discuss this response with us, please feel free to contact information@gcsb.govt.nz or oia.privacy@nzsis.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.

Please note that the GCSB and NZSIS proactively publish OIA responses in accordance with the expectations of Te Kawa Mataaho/the Public Service Commission. We may to publish this response (with your personal information removed) on our websites. Publication of such responses is done on a quarterly basis.

Ngā mihi

Andrew Clark
Te Tumu Whakarae mō Te Tira Tiaki
Director-General of the GCSB

Andrew Hampton
Te Tumu Whakarae mō Te Pā Whakamarumaru
Director-General of Security

Briefing Note

To: Prime Minister

Cc: Maarten Wevers

From: Director, ICG

Date: 09 December 2011

Subject: ADVICE FOR INCOMING PRIME MINISTER ON THE NEW ZEALAND INTELLIGENCE COMMUNITY

New Zealand's National Security Environment

The national security environment for New Zealand is changing (new threats, new targets, new risks and new intelligence methods). New challenges faced by the intelligence community include:

- The rise of cyber threats – evidence of serious intrusions into government networks and those of key private sector companies;
- Support to military – Afghanistan has demonstrated the power of intelligence in a conflict situation;
- Support for law enforcement – transnational crime s6(a) [redacted] s6(a) [redacted] are growing threats.

2. In addition there are the more "traditional" intelligence functions:

- Counter-terrorism – s6(a) [redacted]
- Counter-espionage
- Foreign and economic intelligence to aid decision-makers

3. New Zealand's full access to intelligence from our Five-Eyes partners (Australia, Canada, the UK and US) is a significant enabler in assisting the New Zealand Intelligence Community (NZIC) to meet the above challenges eg on cyber threats. s6(a) [redacted] s6(a) [redacted] s6(a) [redacted]

Organisation of the NZIC

4. Good progress has been made in implementing the reforms approved by Cabinet following the Wintringham and Murdoch Reviews in 2009-10, specifically in ensuring that intelligence is ***serving New Zealand's national security interests*** and helping identify key

risks (the National Security System document spelled out the importance of these linkages and the mechanisms to achieve them):

- ***strengthening central coordination*** of the intelligence community by removing silos and fostering a "whole-of-government" approach. The Intelligence Coordination Group in DPMC was established for this purpose and a new subcommittee of ODESC, known as ODESC(G), established to take responsibility for governance of the NZIC.

- ***efficiencies in the NZIC***. The NZIC has started a process of 'clustering' and has already created a number of efficiencies and savings. One example is the proposed move of NZSIS into Pipitea House, which will help create and sustain greater efficiencies and effectiveness in the NZIC.

- a useful start, through mechanisms such as a joint Statement of Intent for GCSB, NZSIS and NAB, has been made to ***setting priorities*** for the NZIC. Further work is underway on this particularly seeking to link priorities to resources.

- ***resource allocation***. A common Budget Alignment Proposal was submitted by GCSB, NZSIS and NAB in 2011 and a common Four Year Budget Plan has been prepared in draft by those agencies for the next budget. They appreciate the need for an agreed set of resourcing priorities.

The Next Three Years

Co-location in Pipitea House

5. A detailed business case will be presented to Cabinet in February on the proposal to collocate NZSIS with the other agencies in Pipitea House. There are good economic grounds for co-location, which should release savings s6(a) [redacted] s6(a) [redacted] s6(a) [redacted] But even more important is the opportunity to achieve alignment between our two largest intelligence organisations that, while carefully respecting their legal mandates, can improve effectiveness in the future.

Cyber

6. Cyber intrusions are the new espionage. In addition to compromising national security and other sensitive government information, the threats to New Zealand's economic well-being and intellectual property are very real. Public awareness of such attacks would likely impact adversely on public confidence and weaken New Zealand's international reputation.

7. To deal effectively with this challenge will require the NZIC, primarily through the new National Cyber Security Centre (NCSC) in GCSB, to work in new ways with new partners, both in government and the private sector. This effort needs to be ramped up given the intrusions into both government and private sector networks uncovered in the last year. We s6(a) [redacted] have some advantages of size s6(a) [redacted] on which we need to capitalise.

8. The implementation of New Zealand's cyber security strategy, approved by Cabinet in May 2011, requires the development and implementation of policy relating to cyber security standards, engagement with international partners (especially in the Five-Eyes community), the two-way sharing of threat and mitigation information between government and the private sector, and awareness-raising across government, the private sector and the general public. It also requires the development of New Zealand's regulatory environment for telecommunications and cyber systems and its harmonisation, to the maximum extent possible, with those of close partners s6(a) [redacted]. The strategy itself needs to be kept under regular review as our understanding of the threat environment and the necessary responses to it evolve. This policy framework guides the direction of New Zealand's operational response, led by the NCSC and with the involvement of other national security agencies, and is in turn informed by it.

9. It is proposed that this policy work should be coordinated and led by a new cyber security policy unit created within DPMC and located in Pipitea House, where it would sit alongside the NCSC and the intelligence-related business units of DPMC. The unit would be staffed, at least initially, by secondees from other agencies with interests in the cyber area. This proposal will be discussed further with you at an early opportunity and if agreement in principle is reached, a Cabinet paper will be drawn up for consideration in February as part of the budget process.

s6(a) [redacted]

s6(a) [redacted]

Legislation in a Changing Environment

11. Given the changing environment in which the NZIC is operating, it is likely that adjustments to the legal framework will be required in order to enable the NZIC to continue to operate effectively.

NZSIS Act

12. In 2011 the NZSIS enabling legislation was amended to update NZSIS' powers to reflect technological changes. A more fundamental revision of the NZSIS Act is required to bring it into line with today's expectations for controlling intelligence activities. In particular, there is a pressing need to redefine the role and the functions of the NZSIS, to update oversight arrangements as well as other measures.

s6(a) [redacted]

s6(a) [redacted]

s6(a) [redacted]

Telecommunications interception capability

14. The NZSIS, NZ Police and GCSB have commenced collaborative work to modernise lawful domestic interception capability across the New Zealand surveillance agency community. A paper proposing a strategy for modernising domestic interception capability should be available for consideration by Cabinet during March 2012. This work has linkages to the review of the Telecommunications (Interception Capability) Act and to the ultrafast broadband project.

Cyber

15. Separate legislative change is needed to enable agencies, principally the GCSB, to undertake a broader and more proactive range of interventions to help maintain New Zealand's cyber security. This also has implications for the amendment of the Telecommunications (Interception Capability) Act.

Connectivity

16. In order to fully benefit from the Five-Eyes relationships, New Zealand agencies, especially s6(a) [redacted] agencies need enhanced s6(a) [redacted] connectivity. s6(a) [redacted] s6(a) [redacted] s6(a) [redacted] We need to push ahead with connectivity with our close partners, s6(a) [redacted] s6(a) [redacted] A coordinated approach will maximise the efficiency and effectiveness of the NZIC effort and being benefits to a wide range of intelligence and national security agencies across government.

The Intelligence Community and Public Perception

17. When the National Security System document was approved by Cabinet it was also agreed that the Prime Minister might periodically make a statement to the House on the Government's national security objectives. If the Government chooses to deliver such a statement early in the new Parliament, it would provide an opportunity to set out the changing priorities in the intelligence community and the close links between their work and New Zealand's national security challenges broadly defined.

Competing Priorities

18. The NZIC is experiencing a rising tempo of demand from a wide range of New Zealand National Security customers s6(a) [redacted] on the following issues:

- Security
- Cyber
- Foreign intelligence
- Support for law enforcement
- Support for Military Operations

19. The NZIC is being asked to deliver more on traditional outputs, as well as new outputs. In a more tightly fiscally-restrained environment, it may be that the NZIC has to slim down or abandon some lines of services. This will have consequences, but we will work on a better process for making decisions on competing priorities and will inform you of these areas and their consequences ahead of time.

s6(a) [redacted]

The Statutory Intelligence and Security Committee of Parliament

21. The Intelligence and Security Committee Act requires the Prime Minister to take the lead in nominating MPs for the Committee in consultation with other party leaders and the Leader of the Opposition. The Prime Minister is then required, as soon as practicable after the commencement of the Parliament, to submit to the House of Representatives, for endorsement, the nominated Members to serve on the Committee. We will provide you with further advice about this process separately. You should note, however, that the membership of the Committee needs to receive parliamentary approval in time for a first meeting to be held to approve the NZSIS and GCSB's annual reports and to carry out their financial reviews for reporting back to Parliament by probably the end of March.

Ministerial Access to Intelligence

22. The distribution of intelligence material to other Ministers s6(a) [redacted] s6(a) [redacted] Separately we have put a submission to you with some detailed recommendations. It would be our intention to recommend that all Ministers who are s6(a) [redacted] be briefed to enable them to receive intelligence material.

Decisions Required by March 2012

Decision required	Date by which decision must be made	Consequences of deferral
Approval of project funding for the NZSIS move to Pipitea House: s6(a) [redacted]	March 2012 (as part of the 4-year budget process)	Deferral will delay the relocation of NZSIS to Pipitea House and consequently the relocation of NZDF staff s6(a) [redacted] to Defence House.
Approval for transfer of accumulated depreciation funding from GCSB to NZSIS to fund its recapitalisation in Budget 2013 as set out in the Joint Four-Year Budget Plan	February/March 2012	NZSIS will be unable to renew assets as they reach the end of their useful life, resulting in reduced capability. The joint plan suggests using GCSB's accumulated depreciation for this purpose.
Approval for GCSB to carry forward s6(a) [redacted] for funding of the National Cyber Security Centre (NCSC)	March 2012	Would impact the operational effectiveness of the newly established NCSC
Approval of funding for cyber security policy unit in DPMC and full resourcing of Phase 1 of the NCSC	March 2012 (as part of the 4-year budget process)	Would impact the implementation of the Cabinet-approved national cyber security strategy across both government and the private sector
New Zealand Security Intelligence Service Act: Second Phase Review – Agreement to process and timing proposals	March 2012	Delay to policy development process – putting pressure on timing the passage of an NZSIS Bill during the term of the new government
Agreement to legislative measures to address s6(a) [redacted] s6(a) [redacted]	March 2012	s6(a) [redacted]
Agreement to a strategy that will seek to modernise interception capability arrangements across NZSIS, Police and other agencies	March 2012	Would delay the current review of the Telecommunications (Interception Capability) Act and impact on the ultrafast broadband project
Statutory Intelligence and Security Committee of Parliament to approve Annual Reports and financial statements of GCSB and NZSIS	End of March 2012	Under legislation the financial statements must be approved by the ISC before the end of March.