

Hon Andrew Little

Minister Responsible for the GCSB

Minister Responsible for the NZSIS

Proactive release – Strategic Capability and Resourcing Review Report Back

Date of issue: 28 May 2019

The following documents have been proactively released in accordance with Cabinet Office Circular CS (18) 4.

The Cabinet paper is being released with redactions, information has been withheld on the basis that it would not, if requested under the Official Information Act 1982 (OIA), be released. The table below sets out the relevant section of the OIA.

No.	Document	Comments
1	<p>Strategic Capability and Resourcing Review Report Back <i>Cabinet paper</i> Office of the Minister Responsible for the GCSB and NZSIS</p>	<p>A redacted version of the Cabinet paper is being released.</p> <p>Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.</p> <p>Key redaction codes: Section 6(a) of the OIA, as releasing the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand.</p> <p>Section 9(2)(f)(iv) of the OIA, maintaining the confidentiality of advice tendered to Ministers of the Crown and officials</p>

Strategic Capability and Resourcing Review Report Back

Proposal

1. This paper details the progress made by the New Zealand Intelligence Community (NZIC) in building capabilities and strengthening its capacity following an investment of \$178.7 million, spread over four years from 2016 [NSC-16-MIN-0002 refers]. It outlines changes in the strategic environment and threatscape that the NZIC is now working in. The NZIC comprises the Government Communications Security Bureau (GCSB), the New Zealand Security Intelligence Service (NZSIS) and the National Security Group (NSG) of the Department of the Prime Minister and Cabinet (DPMC).
2. This paper also sets the direction for a future report back to External Relations and Security (ERS) committee on options for further risk mitigation and investment options.

Executive Summary

3. NZIC capabilities are crucial to how New Zealand makes sense of the world and manages national security threats, and in doing so contribute to the wellbeing of the nation and its citizens. NZIC's intelligence and protective security activities help New Zealand protect its most valuable infrastructure and intellectual property. Intelligence provided by the NZIC helps to preserve the independence of New Zealand's foreign policy, [REDACTED] 6(a) [REDACTED] 6(a) [REDACTED]
4. In 2014 and 2015 a number of reviews were undertaken into the NZIC. These identified significant capability and organisational weaknesses across the agencies. In 2016, the NZIC received an investment of \$178.7 million, over four years, [REDACTED] 6(a) [REDACTED] 6(a). The investment would also help the Government mitigate its most critical (non-natural hazard) national security risks and stabilise the NZIC in the face of significant cost pressures.
5. The investment built a foundation for the NZIC to prioritise operational effort to keep New Zealanders safe, to protect and grow the economy, and provide foreign intelligence and assessment about issues that matter most to New Zealand.
6. The investment followed a comprehensive capability-by-capability cost-benefit analysis of NZIC's national security contributions. This body of work, known as the Strategic Capability and Resourcing Review (SCRR), provided Ministers and central agencies with confidence that the NZIC was investment ready and had a firm grasp of what it could deliver, and at what cost.
7. The NZIC is now three years into the four year investment programme and has lifted capacity and capability across all core functions [REDACTED] 6(a) [REDACTED] 6(a). These lifts and their impact on New Zealand's national security are detailed in Annex One.
8. As NZIC's capability and capacity have grown, the three agencies continue to develop a more sophisticated understanding of national security threats facing New Zealand. [REDACTED] 6(a) [REDACTED] 6(a). The agencies' understanding of the technological capabilities required to keep pace with national security threats has also improved; in part spurred by NZIC's own experience in building cyber defence and intelligence capabilities like CORTEX, Malware Free Networks, [REDACTED] 6(a) [REDACTED]

- 6(a) and providing assessments of the security risk of 5G technology.
9. A 2018 follow up Performance Improvement Framework (PIF) review of NZIC agencies confirmed the positive progress from the SCRR investment. The NZIC is now delivering fundamentally better advice, services and products that connect directly to the Government's National Security and Intelligence Priorities (NSIPs).
10. The 2018 PIF stated that the NZIC was on the right path, and had addressed weaknesses identified in the 2014 PIF review. Despite significant progress, 6(a) The 2018 PIF identified that the future performance challenge for the NZIC is to fully embed the changes that have been made and use that as a platform 6(a) 6(a)
11. 6(a)
12. The unprecedented terrorist attacks in Christchurch on 15 March 2019 represent a significant change in New Zealand's threatscape. Many of the long term implications are still unknown and will be shaped by the Royal Commission of Inquiry into the Christchurch terrorist attack (the Royal Commission), however they will likely require policy work and capability development in areas such as intelligence and information sharing.
13. In Budget 2019, the NZIC received an investment of \$50 million over four years. 6(a) 6(a) 6(a) The funding will also contribute to some unavoidable cost pressures, for the next two years.
14. I have approved a programme of work to develop an NZIC four year investment plan for Budget 2020 and beyond. This investment plan will develop options for managing the changing threat environment and will respond to recommendations, if any, from the Royal Commission.

2016 Investment in the New Zealand Intelligence Community

15. In 2014 and 2015, GCSB, NZSIS and DPMC were subject to several major reviews, including the 2014 State Services Commission-led PIF Review, and the 2015 Independent Review of Intelligence and Security in New Zealand.
16. Across all PIF areas, 6(a) 6(a) 6(a)

6(a)

- [REDACTED] 6(a)
- The organisational health of both GCSB and NZSIS was under significant strain with [REDACTED] 6(a) and isolation from the wider State Sector.
- Public confidence in the agencies was at a low ebb following allegations of potentially illegal surveillance, which led to the Review of Compliance at the GCSB.

[REDACTED] 6(a)

17. These challenges were exacerbated by rapidly evolving technological and societal changes and an increasingly complex threat environment.
18. In response to these reviews, and the changing strategic environment facing New Zealand, the Government of the day commissioned a capability-by-capability cost-benefit analysis of NZIC's current and future national security contributions. A variety of key customers, including New Zealand Defence Force (NZDF), Ministry of Defence (MoD), Ministry of Foreign Affairs and Trade (MFAT) and central agencies were involved in developing this body of work, known as the Strategic Capability and Resourcing Review (SCRR).
19. SCRR generated a robust understanding of NZIC's cost drivers; what it could achieve and at what cost. Strong support from central agencies and customer agencies was an important factor in its success.

20. [REDACTED] 6(a)

21. [REDACTED] 6(a)

22. [REDACTED] 6(a)

23. In November 2015, Ministers approved [REDACTED] 6(a) [REDACTED] 6(a) \$178.7million over four years. Ministers would decide which funding track would be taken into out years after February 2019. Ministers also set an expectation that the core NZIC would not seek any further funding until at least February 2019 [NSC-15-MIN-0010].

24. As a condition of the funding increase, an efficiency target was built in. No allowance for remuneration or inflationary increases was given to the community. By the end of the four year SCRR programme, the NZIC

6(a)
6(a)

25. The investment was supported by agency-specific modernisation projects, which have ensured that the agencies' internal leadership, structure, systems and processes become increasingly fit-for-purpose over time, to enable delivery of agreed outcomes.

26. Demonstrating that the NZIC could absorb additional investment in a sustainable and safe way was a priority for the Government of the day. As a result, the NZIC developed a sequential implementation plan. This was particularly important given:

6(a)

- The skills necessary to perform many intelligence functions take years to build, and are not readily found in the open job market; and
- The high operational tempo of the agencies.

27. This approach resulted in considerable focus on foundational areas such as capacity building and addressing organisational health, as well as service improvement.

6(a)
6(a)

Impact of investment after three years

28. SCRR was developed to contribute to nine intelligence priorities:

6(a)
6(a)

By focusing on these priorities the NZIC has improved service delivery and performance across all core functions.

Protective Security

29. The NZIC is now much better connected to the private and public sectors.

6(a)

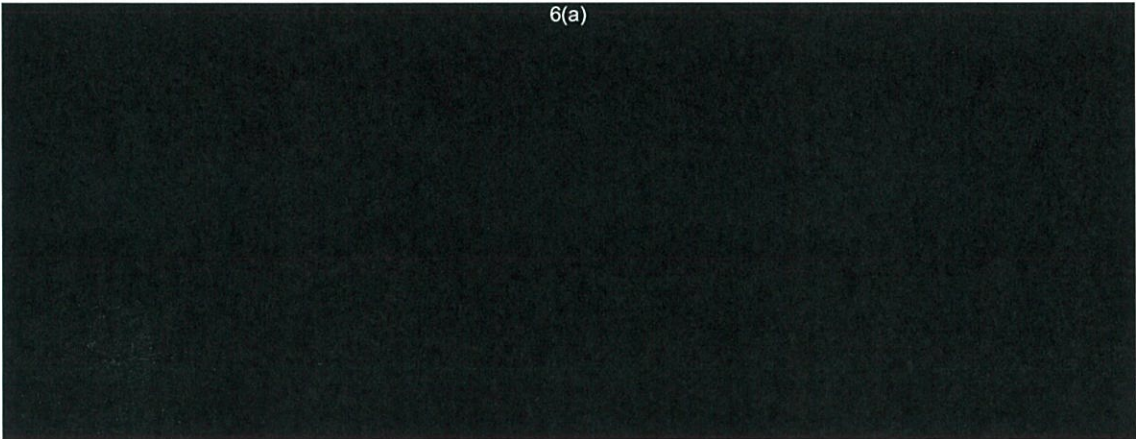
GCSB and NZSIS's protective security functions are highly regarded and their advice is grounded in the real world. Specific achievements include:

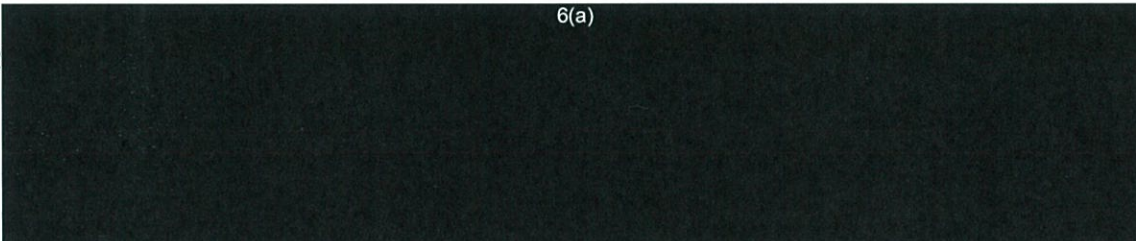
- In 2014, the Protective Security Requirements (PSR) were approved by Cabinet and since then there has been a significant lift in capability across the State Sector. This has materially reduced the probability of security breaches. NZSIS has engaged with nearly 6(a) on the PSR.

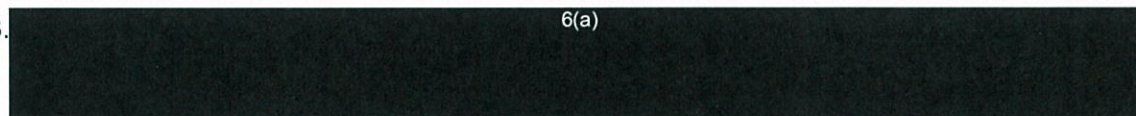
6(a)

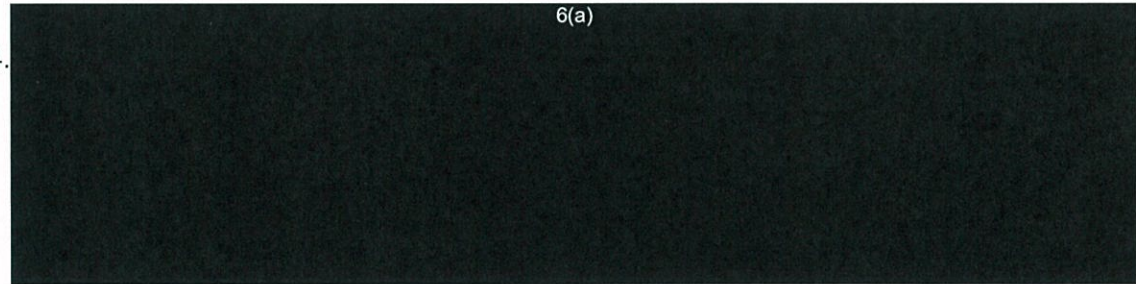
- The GCSB, through its National Cyber Security Centre, has worked with 250 organisations of national significance to develop an understanding of their cyber security resilience and provide guidance on how resilience can be increased in four key areas: governance, investment, readiness and supply chain security.

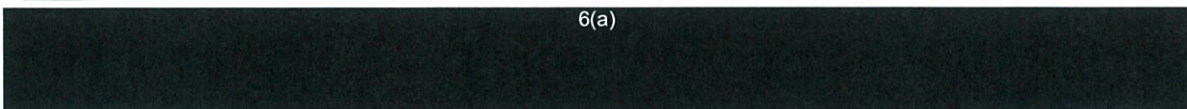
30. Although funded separately from SCRR, GCSB provides advanced protection from cyber threats to organisations of national significance, through its CORTEX capabilities. CORTEX allows for the detection of advanced cyber threats that a number of companies and institutions would not be able to detect or mitigate themselves. GCSB estimates that in the 2017/18 financial year, the operation of CORTEX cyber defence capabilities reduced harm from advanced cyber threats to New Zealand's organisations of national significance by nearly \$27 million. This comes to a total of nearly \$67m over the past two financial years.

31.  6(a)

32.  6(a)

33.  6(a)

34.  6(a)

 6(a)

Organisational health

- 35. A major lift in organisational health has occurred across NZIC agencies. New legislation, the Intelligence and Security Act 2017, is now well embedded, compliance practices are significantly more mature and the NZSIS and GCSB have demonstrated higher levels of employee engagement in climate survey results. NZIC agencies have made concerted efforts to work better as a community to improve collaboration, including a Joint Leadership Team⁴ responsible for high level strategic planning and oversight of significant investments, and the development of a shared workforce plan.
- 36. A 2018 follow up PIF review of NZIC agencies confirmed the positive progress over the course of the SCRR investment. The NZIC is now delivering fundamentally better advice, services and products that connect directly to the Government's National Security and Intelligence Priorities (NSIPs) as a result of investment to date.
- 37. A more detailed summary of progress is outlined in Annex One.

Changes in the strategic environment and threatscape

- 38. [REDACTED] 6(a)
- 39. The unprecedented terrorist attacks in Christchurch on 15 March 2019 represent a significant change in New Zealand's threatscape. Many of the long term implications are still unknown and will be shaped by the Royal Commission, however they will likely require policy work [REDACTED] 6(a)
[REDACTED] 6(a)
- 40. [REDACTED] 6(a)
- 41. [REDACTED] 6(a)
New Zealand's open, internationally-connected economy, and its democratic institutions and values are assets worth protecting. They provide significant benefits and opportunities, which New Zealand must continue to pursue to grow our national wellbeing and prosperity. There are, however, risks associated with foreign state involvement in our economy and democracy. If foreign interference risks are not effectively understood and managed, New Zealand could see some of the economic returns it expects from being "open for business" lost, its international reputation significantly damaged or its fundamental values and institutions undermined.
- 42. [REDACTED] 6(a)

⁴ The Joint Leadership Team is made up of senior staff from DPMC, GCSB and NZSIS and governs NZIC wide initiatives of the SCRR investment programme.

6(a)

43. A crucial part of any country's national security system is its ability to make sense of the global and domestic environment. High quality intelligence and assessment is a critical input to this process and the Government establishes policy and National Security and Intelligence Priorities (NSIPs) to direct this work

6(a)

44. As awareness grows of the variety of threats the public and private sectors are facing the demand for protective security services increases. The Directors-General of the GCSB and NZSIS have recently been appointed as Government functional leads for government information security (GCISO) and protective security (GPSL) respectively. These are system level roles for the agencies that provide better support for New Zealand Government agencies to deal with protective security issues. These functions are currently funded out of baseline.

45. The GCSB has seen a year on year increase of cyber security incidents effecting New Zealand, with links to state actors. The New Zealand Cyber Security Strategy 2018 has been developed to support cyber security improvement, and the NZIC will play a key role in this work.

46. Improving cyber security is a fundamental enabler for New Zealand to thrive in the digital age. As New Zealand becomes more connected to the world, there are a greater number of technological vulnerabilities. Technology is now exploited in a range of new spheres, including democratic processes (For example, the recent compromise of Australian Federal Parliament and the 2016 compromise of US Democratic National Committee systems) and large scale exhortative action (WannaCry disruptions to UK NHS). Without adequate cyber security, New Zealand will be unable to protect its intellectual property, maintain its reputation as a stable and secure place to do business, and ensure governmental and democratic processes remain free from interference. The ability to adapt to technological change is the key challenge to sustaining existing capabilities such as CORTEX.

47.

6(a)

48. Demand for, and complexity of, regulatory services is also increasing. This is especially relevant for the Telecommunications (Interception Capability and Security) Act 2013 in relation to 5G, and the Outer Space and High-altitude Activities Act 2017, in relation to Rocket Lab.

49. [REDACTED] 6(a) as part of the original SCRR project, are not well aligned with New Zealand's current strategic environment or Government priorities. [REDACTED] 6(a)

50. In Budget 2019 the GCSB and NZSIS received an investment of \$50 million over four years. [REDACTED] 6(a)

51. The Budget 2019 investment represents a foundational year for capabilities that will respond to the changing strategic and threat environment. The next steps for those capabilities will be laid out in a four year investment plan for Budget 2020 and beyond.

Budget 2020 and beyond

52. The NZIC will need to develop new capabilities and capacity to respond to the changing environment. I have approved a programme of work to develop an NZIC investment plan for Budget 2020 and beyond. The investment plan will respond to New Zealand's strategic and threat environment and deliver against Government policy and the NSIPs. [REDACTED] 6(a)

53. The Royal Commission is due to report in December 2019 and may make recommendations that the investment plan will need to respond to. Any changes to Government policy, in response to the events in Christchurch, that require additional resource, will also be addressed in the investment plan.

54. Based on the work undertaken to date in developing the investment plan [REDACTED] 9(2)(f)(iv) Any investment will be carefully phased to ensure that the NZIC will continue to build its capability safely and sustainably.

55. There are cross-overs between the work of NZIC and a number of other agencies across the wider security sector. [REDACTED] 9(2)(f)(iv)

Other NZIC business cases in 2019

56. [REDACTED] 6(a)

Proactive release

57. Due to the substantive redactions required to declassify this Cabinet paper I propose to release this paper in summary form.

Human rights

58. This paper presents no inconsistencies with the Human Rights Act 1993 and the New Zealand Bill of Rights Act 1990.

Legislative implications

59. This paper has no legislative implications.

Financial implications

60. There are no financial implications for this paper.

Regulatory impact analysis

61. This paper does not require a regulatory impact analysis.

Gender implications

62. This paper does not require a gender implications statement.

Recommendations

63. The Minister Responsible for the Government Communications Security Bureau and New Zealand Security Intelligence Service recommends that the Committee:

1. **Note** the 2016 investment in the New Zealand Intelligence Community was designed to stabilise the community in the face of significant cost pressures. Funding established a ^{6(a)} [redacted] to address increasing customer demand and deliver on government priorities and policies.
2. **Note** increases in NZIC's capability and capacity since the development of the original SCRR programme in 2015 have improved understanding of national security challenges facing New Zealand and our region and the technology required to keep pace with those challenges.
3. **Note** ^{6(a)} [redacted]
4. **Agree** that as a result of changes to New Zealand's strategic environment, including the Christchurch terrorist attacks, and the pace of technological acceleration, ^{6(a)} [redacted]
5. **Note** NZIC is developing a four year investment plan from 2020 and will report to ERS on this work later in 2019.

Annex One: update on increase in NZIC capability from 2016 – 2020 SCRR investment

1. As signalled in the ERS Cabinet paper, below is a further update on increases in core NZIC capability and capacity.

6(a)

2. 6(a)

3. 6(a)

6(a)

4. 6(a)

6(a)

6(a)

6(a)

6(a)

6(a)

6(a)

5. 6(a)

6. 6(a)

7. 6(a)

6(a)

8. Protective Security Requirements: NZSIS and GCSB continue to work towards providing better support for New Zealand Government agencies in dealing with protective security issues, in line with the Cabinet-approved Protective Security Requirements (PSR) framework. A key initiative to support this was the recent designation of the Directors-General GCSB and NZSIS as functional leads for government information security (GCISO) and protective security (GPSL) respectively. This is currently supported out of baseline, in limited form. These designations were communicated to Government Chief Executives in October and agencies are developing engagement and policy programmes to work across the sector to help lift security resilience.

Further information: Government began a security and privacy review in 2012 following several high profile security breaches across the State Sector. As a consequence the Protective Security Requirements (PSR) were approved by Cabinet in 2014. The PSR outline Government's mandatory requirements for managing personnel, physical and information security, in order to successfully protect people, information, and assets. Four years later we have seen significant capability lift – albeit from an initial low base. This has materially reduced the probability of security breaches across the State Sector. With the framework being open-source, and best practice, NZSIS has engaged with nearly 6(a) across the country. The GCSB through its National Cyber Security Centre has worked with 250 organisations of national significance to develop an understanding their cyber security resilience and provide guidance on how resilience can be increased in four key areas; governance, investment, readiness and supply chain security.

9. Proactive cyber protection: While funded outside of SCRR, GCSB provides world-leading advanced protection from cyber threats to 6(a) through its CORTEX capabilities. In March 2018, Cabinet authorised GCSB to offer one of those capabilities, Malware-Free Networks (MFN) to up to 6(a) organisations of national significance over the two years from 2018/19. Since then GCSB has worked 6(a) National Cyber Security Centre (NCSC) can work collaboratively with them to efficiently and effectively mitigate cyber threats.
10. This work has established that the NCSC provides unique cyber threat information 6(a)
11. The MFN project is on track to deliver a cyber threat disruption service which can be offered to an expanded range of customers by June 2020.

Further information: CORTEX customers include Government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. CORTEX allows for the detection of advanced cyber threats that a number of companies and institutions would not be able to mitigate by themselves. GCSB estimates that in the 2017/18 financial year the operation of CORTEX cyber defence capabilities reduced harm from advanced cyber threats, to New Zealand's organisations of national significance by nearly \$27 million. This comes to a total of nearly \$67m over the past two financial years.

6(a)

12. [REDACTED] 6(a)

13. [REDACTED] 6(a)

14. [REDACTED] 6(a)

[REDACTED] 6(a)

Customer-centric approach

15. We have used additional funding allocated in Budget 2016 to enhance the way the NZIC engages with customers and delivers high value intelligence and assessments, which better meet the needs of Ministers and officials.

16. [REDACTED] 6(a)

17. [REDACTED] 6(a)

18.

6(a)

Further information:

6(a)

Working as a community

19. NZIC agencies have made concerted efforts to work better as a community to improve collaboration, including the establishment of a Joint Leadership Team with senior representatives from GCSB, NZSIS and DPMC responsible for high level strategic planning and oversight of significant investments. Legislative changes in the Intelligence and Security Act 2017 have further enhanced the ability of NZIC agencies to cooperate at both an operational and strategic level. DPMC has enhanced its coordination capabilities to better fulfil its stewardship role in relation to the national security sector.
20. The 2018 PIF follow up report states that while good progress has been made in collaboration and coordination across the NZIC, more needs to be done. ^{6(a)}

21. The GCSB and NZSIS have established common enablement functions, such as finance, human resources, policy and technology. While not funded through SCRR an additional project being undertaken by the joint GC ^{6(a)}
the development of the NZ Top Secret Network.

Further information: *Intelligence agencies must frequently coordinate their efforts in order to fulfil the National Security and Intelligence Priorities and effectively contribute to the policy process. Some formal mechanisms for doing so already exist: DPMC's National Cyber Policy Office coordinates strategic planning and policy advice on a systems level, while a Counter-Terrorism Coordinator attempts to steward the system on issues relating to violent extremism.* ^{6(a)}

⁵ Follow-Up Review for the New Zealand Intelligence Community, Sandi Beatie, Geoff Dangerfield, August 2018

22. In addition to SCRR capability increases the GCSB and NZSIS have implemented regulatory processes and carry out security assessments of space-related activities, in line with new regulatory functions set out in the Outer Space and High-altitude Activities Act 2017 (OSHAA). ^{6(a)}

