

Cabinet

**PROJECT CORTEX BUSINESS CASE**

**Proposal**

1. The purpose of this paper is to seek Cabinet approval for CORTEX, a Government Communications Security Bureau (GCSB) project to counter advanced cyber threats.

**Executive Summary**

2. GCSB proposes acquiring capabilities to protect selected entities against advanced malicious software ('malware'). The proposal is consistent with and will contribute to the objectives of the New Zealand Cyber Security Strategy (2011). The proposal takes into account the amended GCSB Act and necessary warranting procedures, and will in all cases operate with the consent of the participating entities.
3. Detail on the proposal is set out in a business case that has been considered by Joint Ministers (the Minister of Finance, the Minister for Economic Development, the Minister for Communications and Information Technology, the Minister of Foreign Affairs, the Minister of Defence, the Attorney-General and the Minister Responsible for GCSB). Joint Ministers agreed the recommendations made in the business case and provided detailed direction on safeguards to be put in place regarding the protection of information supplied to GCSB by private sector and other consenting organisations. The safeguards will be specified in the warrants and access authorisations that will govern the operation of the capabilities. All points raised by Joint Ministers during review of the business case have been addressed.
4. The business case presents four options for investment and compares their expected benefits, risks and costs. A preferred option is identified and the remaining options are ranked in descending order of preference should Cabinet wish to select an alternative option.
5. The preferred option involves ■ entities – ■ government departments and ■ private sector organisations of national significance – receiving one or more layers of defence against advanced malware. The layers combine detection of advanced malware with technical countermeasures that actively disrupt it. Alerts and advisories generated from the malware detection service would be issued widely across the public and private sectors – to approximately ■ organisations in total – and so have a broader national benefit.
6. The capital expenditure requirements to deliver the capabilities have been estimated as ■. Delivery would occur over ■ months. The incremental operating expenditure required to operate the capabilities in-service has been estimated as ■ over 5-years, with ■ out-year operating costs from 2017/18. All costs would be met from a tagged contingency set aside for this purpose in 2012.
7. GCSB is not proposing to procure or develop bespoke systems. No material level of software development is required of GCSB or a second party. The proposal is to procure then integrate capability components already available and tested over several years, ■.

8. The malware detection and disruption services will operate in respect of foreign-sourced cyber threats that are particularly advanced in terms of technical sophistication and/or persistence. The focus will be on malware that cannot be meaningfully countered by commercial tools and which is [REDACTED]  
[REDACTED]

### **Background**

9. In March 2012 Budget Ministers agreed to set aside a tagged contingency of [REDACTED] over 5-years, including [REDACTED] for capital expenditure, to counter advanced cyber threats: SEC Min (12) 4/1 refers.
10. In December 2013 the Minister Responsible for GCSB wrote to the Minister of Finance with a proposal for use of the tagged contingency. It was subsequently agreed that:
  - a. GCSB would prepare a business case for the proposal, in accordance with Treasury guidelines; and
  - b. the business case would be considered by Joint Ministers comprising the Minister of Finance, the Minister for Economic Development, the Minister for Communications and Information Technology, the Minister of Foreign Affairs, the Minister of Defence, the Attorney-General and the Minister Responsible for GCSB.
11. Joint Ministers considered the business case in May and June 2014. They agreed the recommendations made in it and provided detailed direction on safeguards to be put in place regarding the protection of information supplied to GCSB by private sector and other consenting organisations. These safeguards will be specified in warrants and access authorisations that will govern the operation of the capabilities. The warrants and access authorisations will in all cases be approved by the Minister Responsible for GCSB and the Commissioner of Security Warrants.
12. The present paper summarises the business case proposal and incorporates Ministerial feedback on it. The paper seeks approval that the preferred option set out in the business case can be taken forward.

### **Why investment is needed**

13. The Internet is of immense economic and wider benefit to New Zealand. For New Zealand firms, it allows global access to suppliers and markets, mitigating the impact of geographic isolation. Benefits to New Zealand citizens arise in many practical ways, including in terms of the efficiency and cost of interaction with government. However there is a downside of ever-increasing use of the Internet: greater exposure to cyber-borne threats. Countering such threats is a Government priority, as set out in the New Zealand Cyber Security Strategy (2011).
14. The business case is concerned with cyber-borne threats that are foreign-sourced and particularly advanced in terms of technical sophistication and/or persistence. The harms at issue – theft of intellectual property, or damage to IT system, for instance – are caused by malicious software ('malware') that cannot be adequately countered by commercially-available tools and that are [REDACTED]. These harms are being felt in New Zealand, as overseas. Advanced malware is being directed against networks or systems owned by:
  - a. key economic generators. For example, over several months in 2012 the network of a large New Zealand firm was compromised in separate attacks [REDACTED]  
[REDACTED];

- b. niche exporters including in knowledge-intensive industries;
- c. major IT service providers. In this case the attacks are of particular concern because exfiltration of data could extend to customer networks; and
- e. government agencies including [REDACTED]

#### **Short-listed options**

15. The business case considers a wide range of ways in which the threat posed by advanced malware could be countered. The four short-listed options are summarised below, contrasted with the status quo – the 'Do Nothing' option. Incremental 5-year costs are stated for each option.

- a. **Option 0 'Do Nothing'**: limited visibility of the threat from advanced malware. Detection depends almost entirely on GCSB's access to networks owned by government departments. [REDACTED].
- b. **Option 1 'Do Minimum'** ([REDACTED] including [REDACTED] capital): [REDACTED] government agencies – [REDACTED] more than at present – receive a GCSB-supplied advanced malware detection service. This will allow greater visibility of the advanced malware threat and increased 'network hardening' (vulnerability reduction) as a consequence. No active disruption of advanced malware.
- c. **Option 2 'Modest'** ([REDACTED] including [REDACTED] capital): as for option 1 except that the advanced malware detection service is provided to [REDACTED] government agencies plus [REDACTED] organisations of high economic value and/or operating critical national infrastructure.
- d. **Option 3 'Active'** ([REDACTED] including [REDACTED] capital): GCSB delivers an advanced malware detection services to [REDACTED] entities: [REDACTED] government agencies plus [REDACTED] organisations of high economic value and/or operating critical national infrastructure. In addition GCSB delivers a limited malware disruption service to [REDACTED] of the same [REDACTED] entities. This option will provide substantially greater visibility and understanding of the advanced malware threat, so improved vulnerability reduction. Because there is active disruption of advanced malware through technical countermeasures, there will be direct – before-the-fact – mitigation of harm as well.
- e. **Option 4 'Proactive'** ([REDACTED] including [REDACTED] capital): as option 3 except that, in addition, GCSB shares technology and classified information with an Internet Service Provider so that it can disrupt advanced malware for [REDACTED] of its customers under pilot conditions in the first instance. As in option 3, advanced malware will be 'blocked' and not just 'detected'.

#### **Assessing the options**

16. Because the main benefits at issue cannot be monetised, the short-listed options were assessed through use of multi-criteria decision analysis (MCDA), in line with Treasury guidance. The MCDA considered how each option compared to all other options (including 'Do Nothing'), against pre-defined criteria relating to cost, benefit and risk. The criteria themselves were weighted. Senior policy leads drawn from DPMC, MBIE, NZSIS and GCSB participated in the process. An independent decision sciences

consultancy was appointed to test the robustness of the selection and evaluation of options.

17. The key finding of the MCDA is that option 4 offers greatest value for money in terms of balancing benefit, risk and cost. The second best option is option 3 and least preferred option is Option 1. Sensitivity analysis performed on the MCDA shows that the selection of Option 4 is highly robust. However the other short-listed options, option 1 aside – which offers less value for money than even the status quo – are viable alternatives. The main trade-offs in selecting between the options are summarised in the table below. The options are contrasted with option 4.

Option 3	<ul style="list-style-type: none"><li>• A 10 per cent reduction in cost (████ over five years)</li><li>• A third of benefits would be foregone. Far fewer organisations would receive an active malware disruption service – █ organisations rather than █</li><li>• A reduction in security risk relating to the unauthorised disclosure of classified tools. Option 3 does not involve GCSB sharing technology ██████████ with an Internet Service Provider.</li></ul>
Option 2	<ul style="list-style-type: none"><li>• A 44 per cent reduction in cost (████ over five years)</li><li>• 60 per cent of total weighted benefits would be sacrificed. There is a significant reduction in benefits because the number of entities receiving a malware detection service would reduce from █ to █ and because there would be no active disruption of advanced malware</li></ul>
Option 1	<ul style="list-style-type: none"><li>• Option 1 is not recommended</li><li>• It would increase visibility of the advanced threat to government agencies. However the translation into vulnerability reduction for operators of critical national infrastructure or key economic generators could be limited and the benefits would not be outweighed by the delivery risks and costs.</li></ul>

### **Proposal – the preferred option**

#### *Capabilities*

18. The foundation of the preferred option is a malware detection service delivered to █ consenting organisations. █ of the █ organisations will be government agencies. The other █ will be drawn from a list of approximately █ organisations of national importance developed by DPMC's National Cyber Policy Office (NCPO) and approved by ODESC on 7 June 2013. The list includes key economic generators, niche exporters, research institutions and operators of critical national infrastructure.
19. Alerts and advisories generated from the malware detection service will be distributed widely, including to all government departments and all █ organisations on the NCPO list. Benefits from the investment would be realised across the public and private sectors and have a national impact.

20. The proposal includes an active disruption capability as well as malware detection. GCSB will deploy technical tools to 'block' advanced malware targeting ■ of the ■ organisations receiving the malware detection service.
21. In addition, technology will be shared with an Internet Service Provider – a provider of email, internet or network security services – so that it can disrupt advanced malware for ■ of its customers. This will occur under pilot conditions because of the need to test how the technology would operate in a commercial context. If the pilot is successful a proposal will be prepared for Ministerial consideration outlining the costs and benefits of wider deployment. This wider deployment would be led by industry, on a cost-recovery/profit basis, not by GCSB.

*Statutory framework and policy*

22. The GCSB Act has recently been amended. A key driver of these amendments was to ensure the continued lawfulness of GCSB's information assurance and cyber security activities. Those amendments have also made the processes for obtaining interception warrants and access authorisations (pursuant to which such activities must be undertaken) far more prescriptive than previously.
23. In particular, information assurance and cyber security-related warrants and authorisations cannot be issued unless both the Minister Responsible for the GCSB and the Commissioner for Security Warrants are satisfied that GCSB is capable of meeting certain statutory thresholds, including implementing "satisfactory arrangements" appropriately regulating what information is collected, how it is collected, and how it is stored and used. Further, it is the responsibility of the Inspector-General of Intelligence and Security to audit the effectiveness and appropriateness of controls in these (and other) respects.
24. This framework ensures not only that cyber security activities are always undertaken pursuant to an appropriate legal authority (i.e. a warrant or access authorisation) but that the manner in which it is undertaken is subject to externally audited controls ensuring that such activities are appropriate, including proportionate in terms of balancing privacy and security interests.
25. The CORTEX proposal is consistent with the amended GCSB Act and necessary warranting procedures, and will in all cases operate with the consent of the participating entities. The warranting procedures involve a two-step process with the overall effect that GCSB staff will have access to 'personal communications' (a term of defined by relevant warrants and access authorisations) only when it is relevant to a specific threat and when needed to confirm or mitigate it. Technology can be used to separate personal communications from other data, so that privacy issues associated with GCSB activities to be proportionate to cyber threats.
26. GCSB is subject to some of the principles governing the privacy of personal information under the Privacy Act 1993, as well as the principles governing collection, retention, use and disclosure of personal information set out in the amended GCSB Act. A Privacy Impact Assessment (PIA) has been prepared for the project. It concludes that, because of controls that will be put in place, the proposed capabilities do not give rise to any material privacy issues.
27. The controls in question – which Joint Ministers have considered when reviewing the CORTEX proposal – will be specified in relevant warrants and access authorisations. They will include attention to how data is accessed, stored, sharing and disposed of. There will be no 'mass surveillance', and data will be accessed by GCSB only with the consent of owners of relevant networks or systems.

*Benefits*

28. The proposal is consistent with and will contribute significantly to the overall policy objective of countering advanced cyber intrusions, which is one aspect of the New Zealand Cyber Security Strategy.
29. Investment would reduce the economic and broader national security harms caused by advanced malware. Networks of high national interest would be made less vulnerable to attack, because of provision of alerts and advisories, and attempted intrusions would be blocked through technical means before harm is caused.
30. Such investment would align with the Business Growth Agenda (because protections will be afforded to key economic generators and operators of critical national infrastructure) and to Better Public Services Result Areas 9 & 10 (because advanced malware targets public networks as well as private sector ones).
31. The economic harm caused by advanced malware is significant, although hard to quantify at the macroeconomic level or even for individual organisations. It is hard to quantify because, for example, in the case of loss of intellectual property (IP) – often the most immediate target of a successful malware attack – there is no widely accepted means of valuing IP prospectively.
32. Investment is justified in financial terms even if only a small number of advanced malware attacks are frustrated each year. The direct cost of resolving an attack after the fact can be high. It requires extensive work to clearly identify the nature of the intrusion and to remove it, which can take months. It often requires taking the system off-line for the actual removal, which can result in days or weeks of system downtime. This is not acceptable in the case of key infrastructure, such as power generation systems. Replacement of entire systems may be more financially viable than cleaning them.

**Financial implications**

33. The business case details the cost implications of the preferred option and plans the year-on-year funding requirements. The predicted spending profile for the preferred option is summarised below.

	\$m – increase/(decrease)					
	2013/14	2014/15	2015/16	2016/17	2017/18 & outyears	5-year
Estimated Operating Expenditure	■	■	■	■	■	■
Estimated Capital Expenditure	■	■	■	■	■	■
Total	■	■	■	■	■	■
less GCSB Operating contribution	■	■	■	■	■	■
less GCSB Capital contribution	■	■	■	■	■	■
Total	■	■	■	■	■	■

34. The 5-year through life cost has been estimated as ■. The capital expenditure requirements to deliver the capabilities have been estimated as ■. The incremental operating expenditure required to operate the capabilities in-service has been estimated as ■ over 5-years, with ■ out-year operating costs from 2017/18.

35. The estimated costs were subjected to Quantitative Risk Analysis (QRA) by a consultant from the State Services Commission panel of QRA providers. The QRA indicates that [REDACTED] of the [REDACTED] capital expenditure allocated to GCSB should be held back by the Director, GCSB as a contingency for the project. The contingency will not be used for new items or increased scope without referral back to Joint Ministers.
36. The table above includes GCSB baseline contributions. By re-prioritising existing plans and resources, GCSB can meet all 2013/14 operating expenditure ([REDACTED]) and [REDACTED] of total capital expenditure.
37. In 2013/14 fiscal year GCSB moved to a single-line appropriation that includes operating, depreciation expense and capital. This will ensure the security of GCSB financial information going forward. Any underspend is returned to the Crown therefore cash does not accumulate on the balance sheet for future re-investment. A consequence is that GCSB is limited in its expenditures per fiscal year to the single-line appropriation. A project the size of CORTEX will require incremental capital funding on an on-going basis to ensure timely replacement of assets. Any capital funding required beyond the five years of this business case, which is likely to equal the value of the on-going depreciation of the original asset, will be either (1) negotiated with Treasury or (2) presented in a separate business case and subject to Ministerial approval.
38. The business case explains that user charging was considered as a possible option but rejected for the short term. An immediate reason is that user charging could not proceed without amendment to the GCSB Act.
39. Treasury has confirmed that the spending profile is within the overall tagged contingency to which paragraph 8 refers. The tagged contingency is as follows:

	\$m – increase/(decrease)					
	2013/14	2014/15	2015/16	2016/17	2017/18 & outyears	5-year
Operating	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Capital	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Total	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

### **Implementation matters**

#### *Risk*

40. A risk management strategy and initial risk register have been established for the project and shared with monitoring agencies. The risk register records that key risks exist around scarcity of specialist technical staff over the next 12 months and around GCSB's ability to retain and recruit staff in sufficient numbers to operationalize and then maintain the new capabilities. The mitigation strategy for these risks involves outsourcing key recruitment tasks, improving the timeliness of vetting processes, and the targeted use of security cleared contractors for some aspects of system engineering and certification.

#### *Technology*

41. GCSB is not proposing to procure or develop bespoke systems. No material level of software development is required of GCSB or a second party. The proposal is to

procure then integrate capability components already available and tested, [REDACTED]

[REDACTED]. The hardware and software components range from widely available commercial-off-the-shelf (COTS) systems, through to single-source COTS, to systems only available through government-to-government agreement. All of the technology has been in use for some time, [REDACTED].

42. The Government Rules of Procurement have been integrated into the proposed commercial approach. Aspects of Government Chief Information Officer's (GCIO's) Government ICT Strategy and Action Plan, and the Government Enterprise Architecture, have been incorporated as well.

*Selection of private sector organisation*

43. Sign-off for service delivery to a particular organisation will form part of the warrant and access authorisation process – i.e. subject to approval of the Responsible Minister and Commissioner for Security Warrants. As noted above, a condition of service delivery will be that the organisation consents to it.
44. Senior officials will oversee the process by which candidate organisations are identified. Three criteria will be involved in the selection process:
  - a. The extent to which the entity owns or operates 'an information asset of national interest', as drawn from NCPO list;
  - b. Ensuring there is a broad coverage of sectors represented; and
  - c. Intelligence or other evidence that an organisation, or particular sector, has or is likely to be targeted by advanced malware.

*Project assurance*

45. GCSB has prepared a project assurance plan for CORTEX, in line with requirements of the GCIO. This plan has been reviewed by monitoring agencies. These agencies will have an on-going role in reviewing progress on the project.

*Schedule*

46. A summary of the project plan is presented in the business case. It shows delivery would be phased over [REDACTED] months, with discrete capabilities becoming operational [REDACTED] months after project approval.

**Consultation**

47. This paper and the supporting business case were prepared by GCSB in consultation with DPMC (NCPO), MBIE and the NZ Security Intelligence Service. The State Services Commission has been informed.
48. Treasury has reviewed this paper and the supporting business case. Project assurance responsibilities of the GCIO have been undertaken by Treasury's Portfolio Performance Monitoring team. Comments have been provided to GCSB and these have been responded to satisfactorily, with changes incorporated where appropriate.
49. To confirm that the proposed capabilities would be welcomed – and consented to – by potential beneficiaries of them, GCSB has held discussions with [REDACTED] major private sector firms that feature on the NCPO list of organisations of national importance. All



of these firms have confirmed interest in engaging further on the proposals in the event that funding is secured.

**Human rights, disability and gender implications, regulatory impact assessment**

50. The proposal involves the interception of communications and as such may engage the right against unreasonable search and seizure affirmed by s 21 of the New Zealand Bill of Rights Act 1990. This issue was considered in the Bill of Rights Act analysis prepared by Crown Law at the time of the passage of the GCSB Amendment Bill in 2013. In relation to the s 21 right, Crown Law concluded that the defined scope and applicable safeguards for the exercise of interception powers are broadly consistent with accepted requirements for such powers in the context of intelligence-gathering, and are therefore consistent with the right against unreasonable search and seizure. The interception of communications under the CORTEX proposal is entirely within the scope of the GCSB Act as described in the Crown Law analysis. There are therefore no human rights impacts associated with the proposal.
51. Regulatory impact analysis requirements do not apply. There are no gender or disability implications associated with this proposal.

**Legislative implications**

52. There are no legislative implications associated with this proposal.

**Publicity**

53. No publicity is planned.

**Recommendations**

54. The Minister Responsible for GCSB recommends that Cabinet:

*Background*

- a. **note** that countering advanced cyber threats is a Government priority, as set out in the New Zealand Cyber Security Strategy (2011);
- b. **note** that in March 2012 Budget Ministers agreed to set aside a tagged contingency of [REDACTED] over five years, including [REDACTED] for capital expenditure, to counter advanced cyber threats: SEC Min (12) 4/1 refers;
- c. **note** that in December 2013 the Minister Responsible for GCSB wrote to the Minister of Finance with a proposal for use of the tagged contingency and that GCSB would prepare a business case for the proposal (project CORTEX), in accordance with Treasury guidelines;
- d. **note** that in May and June 2014 the business case was reviewed by Joint Ministers comprising the Minister of Finance, the Minister for Economic Development, the Minister for Communications and Information Technology, the Minister of Foreign Affairs, the Minister of Defence, the Attorney-General and the Minister Responsible for GCSB.

*Implementation*

- e. **note** that CORTEX:
  - i. is consistent with and will contribute significantly to the overall objective of countering advanced cyber intrusions;

**UNCLASSIFIED [PREVIOUSLY SECRET//NEW ZEALAND EYES ONLY]**

- ii. will operate under the provisions of the amended GCSB Act and warrants and access authorisations approved by the Minister Responsible for GCSB and the Commissioner for Security Warrants; and
- iii. will in all cases operate with the consent of the participating organisations;
- f. **agree** the preferred option is Option 4 ('Proactive');
- g. **direct** the Government Communications Security Bureau to implement the preferred option;

**Resource**

- h. **note** that the capital expenditure requirements to deliver the capabilities have been estimated as [REDACTED];
- i. **note** that the incremental operating expenditure required to operate the capabilities in-service has been estimated as [REDACTED] over 5-years, with [REDACTED] out-year operating costs from 2017/18;
- j. **note** that [REDACTED] capital and [REDACTED] operating expenditure can be met from GCSB baseline;
- k. **agree** to increase expenditure to provide for costs associated with the decision in recommendation (g) above, with a corresponding impact on the operating balance and debt:

	\$m – increase/(decrease)				
Vote Communications Security and Intelligence Minister Responsible for the Government Communications Security Bureau	2013/14	2014/15	2015/16	2016/17	2017/18 & outyears
Operating Impact	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Debt Impact	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Totals	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

- l. **approve** the following changes to appropriations and net assets to give effect to the decision in recommendation (g) above:

	\$m – increase/(decrease)				
Vote Communications Security and Intelligence Minister Responsible for the Government Communications Security Bureau	2013/14	2014/15	2015/16	2016/17	2017/18 & outyears
Intelligence and Security Department Expenses and Capital Expenditure: Communications Security and Intelligence (Funded by revenue crown)	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

- m. **agree** that the operating balance and debt impacts in recommendation (j) above of expenses and capital expenditure incurred under recommendation (k) above be charges against the Initiative 7418 tagged contingency established in SEC Min (12) 4/1 as modified by CAB Min (13) 30/25;

- n. **note** that it is anticipated that in future years beyond 2017/18, the GCSB will require Crown appropriations (limited by the value of depreciation funds returned from GCSB to the Crown) to replace and maintain project assets beyond 2017/18;

*Reporting*

- o. **direct** GCSB to report back to Cabinet on progress of project CORTEX by September 2015.

Rt Hon John Key

Minister Responsible for the

Government Communications Security Bureau

\_\_\_\_ / \_\_\_\_ / 2014