

13 August 2001

Hon. Trevor Mallard

**CABINET PAPER:
Centre for Critical Infrastructure Protection**

Proposal

1. This paper proposes that Cabinet agree to set up a Centre for Critical Infrastructure Protection (CCIP) within the Government Communication Security Bureau (GCSB) to improve the protection of critical national infrastructure and Government departments against information-borne threats, or *cyber-threats*.

Executive Summary

2. I recommend that Government set up, and fully fund, a Centre for Critical Infrastructure Protection (CCIP) to protect against cyber-threats because:
 - People and businesses in New Zealand are highly dependent on various infrastructure services.
 - These services are themselves operated or managed by IT systems which are vulnerable to a rapidly changing array of threats over the Internet and through dial-up access.
 - There is an increasing risk to businesses of damage through the activities of virus writers and "hackers", the vast majority of whom are not in New Zealand and may not even be traceable.
 - The risk is increasing dramatically and this trend is likely to continue.
 - Protection of the national infrastructure has been identified as a key Government objective.
3. Funding is sought for Vote: Intelligence and Communications Security for the additional operating costs estimated at \$450,000 (GST exclusive) in 2001/02 and \$847,000 (GST exclusive) in 2002/03 and outyears. A capital contribution of \$269,000 is sought in 2001/02.

Background

4. The National Information Infrastructure Protection Project was established under the E-government Programme to examine the state of protection of the nation's critical infrastructure from cyber-threat. In December 2000 officials provided me with a report¹ which identified a number of vulnerabilities and made recommendations for improvement, with which I agreed. One of those recommendations was to investigate setting up a New Zealand based security monitoring and incident handling organisation. Officials have now proposed that a centre for critical infrastructure protection be established within the Government Communications Security Bureau (GCSB). I agree with their recommendation.

Comment

Cyber-Threats to Critical Infrastructure

5. Critical infrastructure is that infrastructure necessary to provide critical services, whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement. New Zealand's critical infrastructure has been identified as those assets and systems required for the maintenance of: governance including law and order and national and economic security; telecommunications and the Internet; energy including electricity generation and distribution and the distribution of oil and gas; finance and banking; transport; and emergency services. Many of these are vulnerable to information related threats, or *cyber-threats*.
6. Research has highlighted various cyber-risks to New Zealand's critical infrastructure, in particular:
 - the lack of management-level understanding of the need for audited IT security;
 - the impact of ongoing 'denial of service' attacks over the Internet;
 - the sharply increasing number and types of attacks being perpetrated over the Internet; and
 - the challenges facing IT systems administrators who need to maintain security as vulnerabilities continually emerge in widely-used software.

Responsibility for Infrastructure Protection

7. Owners of infrastructure are responsible for all aspects of security and protection, and the proposed CCIP will not supplant that responsibility. Owners must ensure that adequate safeguards are in place to mitigate the threat of loss of service due to cyber-attacks.
8. The likelihood of inadequate risk management is increased in instances where the customer has no real choice, which is often the case for critical infrastructure providers. Therefore commercial realities may lead to a lesser level of infrastructure protection than is appropriate. Government departments are effectively monopoly providers of various services also, and face no less pressure on expenditure than private companies.
9. Every person in New Zealand is reliant on the nation's critical infrastructure. Therefore Government has a responsibility to ensure that that infrastructure is adequately protected.

The Case for a Centre for Critical Infrastructure Protection

10. New Zealand's critical infrastructure exists in a technical environment which is increasingly interconnected and harbours changing threats. It is vulnerable to attack over the Internet or even through dial-up from anywhere in the world.

11. Protection of New Zealand's critical infrastructure is identified as a key objective in "The Government's Defence Policy Framework" of June 2000. The proposed CCIP addresses the cyber-threat aspects of that objective.
12. The dramatic expansion of telecommunications and the Internet exposes Government and business to a range of rapidly evolving threats, many of which are poorly understood. For example, in the last two years:
 - The Melissa and ILOVEYOU viruses caused business and government disruption worldwide, with losses estimated to cost hundreds of millions of dollars.
 - A lone teenager attacked and crippled Internet businesses Amazon and eBay in February 2000.
 - In May 2000, an Australian hacker compromised the computer-based controls of a water system and caused the discharge of raw sewage into waterways on the Sunshine Coast.
 - In July 2000, two computer programmers from Kazakhstan broke into the global Bloomberg financial information network and then tried to extort money from its owner.
 - Since early this year, a major New Zealand infrastructure company has been under sustained attack over the Internet, degrading service on the Internet in New Zealand.
 - In April-May 2001 US and Chinese hackers engaged in a 'cyber-war' defacing numerous government and business web sites in China and the US respectively.
 - As this paper was prepared a New Zealand Government department's website was vandalised, apparently by hackers in Brazil. This was presented as "New Zealand Government hacked" by overseas wire services.
13. Threats are increasing rapidly in number and complexity. For example, the US CERT (a federally-funded computer emergency response team) has logged the following statistics demonstrating the order of growth of "incidents" - reports by US companies and agencies of attempts to gain access or otherwise attack their computer systems:

1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001 (Q1)
6	132	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859	21,756	7,047

Infrastructure Protection in Other Countries

14. Other countries have already moved to manage this risk.
 - The United Kingdom has created the National Infrastructure Security Coordination Centre - an inter-departmental organisation set up to co-ordinate and develop work within government departments and agencies and private sector organisations to defend the critical national infrastructure against electronic attack.
 - Canada has established the Office of Critical Infrastructure Protection and Emergency Preparedness to provide national leadership to

protect Canada's critical infrastructure regardless of the source of threat.

- Infrastructure Protection is a major focus of the US government. The National Infrastructure Protection Center, part of the FBI, is the government's focal point for threat assessment, warning, investigation and response for threats or attacks against critical infrastructures. There are a number of other US federal and private sector bodies which contribute to national infrastructure protection.
- In Australia this issue is still the subject of analysis and consultation. In the absence of an identified centre the critical infrastructure protection function is being undertaken by a government agency.

Proposed Centre for Critical Infrastructure Protection

15. I propose that risks to critical infrastructure be addressed in New Zealand, as they are in other countries, by the creation of a Centre for Critical Infrastructure Protection. Such a Centre, if established, would assist infrastructure owners, government agencies, and to some extent to the New Zealand public (collectively referred to as the CCIP's 'partners'). The CCIP will provide timely and relevant information about viruses, denial of service attacks, newly found flaws in software, and IT security issues in general. It will build strong relationships with overseas counterparts, with law enforcement and with infrastructure owners.
16. The CCIP's functions will be divided into three groups: a 24 hour watch and warn function; an investigation and analysis function; and an outreach and training broking function. As do its overseas counterparts, the CCIP will use open sources and classified intelligence to provide warning of threats and attacks.
17. The relationship with partners will be somewhat different for each partner group:
 - as the focus is on the protection of critical infrastructure, critical infrastructure providers will be given priority;
 - Government agencies will have full access to the CCIP (although critical infrastructure would take precedence); and
 - the New Zealand public will have access to an up to date CCIP web page with security information.

Location of the CCIP

18. Several factors require the CCIP to be a part of central government. It would, as discussed above, need access to intelligence some of which will be highly classified. It must have a culture of security both to safeguard this information and to gain the confidence of private sector infrastructure owners that their sensitive security and commercial information would be treated confidentially and not made available for exploitation by a competitor, customer or supplier. And only as a government agency will the CCIP be able to have a full and free exchange of information with international counterparts.

19. Overseas experience shows that the centre should not be part of a law enforcement agency, since this might reasonably focus on the pursuit of offenders to the detriment of rectifying damage and of confidentiality. The host agency would need skills in IT security, or at least the ability to manage those skills.
20. Several options for siting the CCIP have been examined. These range from the establishment of a separate department to creating a new function within an existing department. The latter approach has been selected on the basis of cost, and best conformance to Government policy.
21. A number of departments were considered against criteria of effectiveness, perception and cost. These included: the Department of the Prime Minister and Cabinet; the Ministry of Civil Defence and Emergency Management; the New Zealand Police; the New Zealand Defence Force; the State Services Commission; and the GCSB. Following a benefit/opportunity versus risk/threat analysis three options were selected for final analysis (see Annex 1).
22. The recommended option is **wholly within the GCSB**. The CCIP function is closely aligned to the GCSB's Information Systems Security role and would best be accomplished by creating the CCIP functions as a GCSB output.

Options for Funding the CCIP

23. The CCIP could be fully funded by the Crown, it could be funded by contributions from either or both of infrastructure owners and Government agencies, or it could be privately funded. The latter option is not appropriate for a government agency so has been discounted. The remaining options are compared below as "Wholly Crown Funded" and "Partly Crown funded" against the criteria shown below.

Wholly Crown Funded	Partly Crown Funded
<i>Criterion 1 - Safeguarding New Zealand's people, businesses and international reputation</i>	
Crown funding of this service would demonstrate the Crown's interest in avoiding the harm to New Zealand people businesses and international reputation resulting from critical infrastructure failure.	Partner funding would recognise that partners (critical infrastructure owners and government agencies) would benefit in that their business assets would gain improved protection.
<i>Criterion 2 - Avoiding the Private Capture of Benefits</i>	
Every New Zealand resident is reliant on services provided over the critical infrastructure. The CCIP contributes to the integrity of these essential services to individuals, but it does not supplant owners' responsibilities.	Owners will remain fully responsible for protection of their systems, and so are already contributing to infrastructure security. As the CCIP improves their awareness of vulnerabilities they may face further costs for increased security.
<i>Criterion 3 - Minimising the Crown's Legal Liability</i>	
Crown funding would make it easier to disclaim liability for any errors or omissions of which the CCIP might be accused.	Crown liability would be disclaimed, but it would be harder to argue that the Crown bore no responsibility if services were charged for.
<i>Criterion 4 - Wide Participation</i>	
All critical infrastructure owners will subscribe to	The imposition of costs will reduce the uptake of

the CCIP if there is no direct cost to them.	CCIP services, and adversely impact the effectiveness of the CCIP.
--	--

24. In none of the overseas models researched are infrastructure owners expected to pay for this service. Those jurisdictions consider the public interest arguments to be overwhelming.

Performance Measures

25. GCSB has agreed to establish the CCIP functions as a new output. Performance measures will be agreed as part of this process.

Consultation

26. Officials have consulted extensively with infrastructure providers and Government agencies throughout the development of the December 2000 report and the subsequent investigations leading to the recommendation to establish the CCIP. Infrastructure owners include: banks (including the Reserve Bank); telecommunications and Internet providers; Transpower (which has engaged the power industry on the issue); and the Airways Corporation. Agencies include: the New Zealand Police; the Treasury; the Department of the Prime Minister and Cabinet; and the GCSB.
27. Formal consultation on this submission has been completed with:
- The Treasury;
 - The Department of Prime Minister and Cabinet;
 - The New Zealand Police;
 - The New Zealand Security and Intelligence Service;
 - The Ministry of Foreign Affairs and Trade;
 - The New Zealand Defence Force; and
 - The GCSB.
28. This submission was also considered by the Officials' Committee for Domestic and External Security Co-ordination (ODESC(T)) at its meeting on 26 June 2001. ODESC(T) strongly supported the establishment of the CCIP, its location within GCSB, and public funding of the Centre. The need to fund the CCIP outside the normal budgetary cycle was debated. In the event ODESC(T) agreed that, as the risk from cyber-threat continued to rise dramatically, the Centre should be established as soon as possible.

Financial Implications

29. The additional operating costs are estimated at \$450,000 (GST exclusive) in 2001/02 and \$847,000 (GST exclusive) in 2002/03 and outyears:

	\$000	2001/02	2002/03
Personnel costs		298	580
Other operating costs		133	216
Depreciation		19	51

Total operating cost (excluding GST)	450	847
---	------------	------------

30. Additional operating funding is sought to fund these costs.
31. Information technology hardware and software, together with some minor office fitout costs, are estimated to cost \$269,000 (GST exclusive). A capital contribution of \$269,000 is sought in 2001/02, with outyear capital to be absorbed by GCSB.

Treasury Comment

32. Treasury has been consulted on this paper and agreed with the desirability of a Centre for Critical Infrastructure Protection, and that it should be sited within GCSB.
33. However, Treasury would prefer to see more rigorous analysis of the funding options. On the face of it, there appeared to be a case for third party funding to some extent - especially from commercial companies that will gain a significant private benefit (for example Telecom and Transpower). Treasury acknowledged, however, that there may be significant administration costs for GCSB in setting up invoicing and such other arrangements should Cabinet decide on third party funding. Treasury recommended the department remain open to consider the option of third party funding, should special assignments warrant service from GCSB that:
- provides significant private benefit to a commercial organisation; and
 - incurs a significant cost in relation to the total cost of outputs provided for the new function approved in this paper.

Human Rights Implications

34. None.

Legislation Implications

35. None.

Regulatory Impact and Compliance Cost Statement

36. None.

Gender Implications

37. None.

Publicity

38. It is recommended that Government issue a press release advising of the decision to set up the CCIP, its objectives, location and cost. This will

provide the public, infrastructure providers, and the international community with assurance that the New Zealand Government is taking the cyber-threat issue seriously and is taking positive action to address the threat.

Recommendations

39. It is recommended that the Committee:

- a. **note** that New Zealand's critical infrastructure has a number of areas of vulnerability to attacks over the Internet;
- b. **note** that governments in other countries have recognised this threat and have moved to mitigate it by setting up government agencies or functions within government to provide infrastructure protection;
- c. **agree** to set up the Centre for Critical Infrastructure Protection (CCIP) within the Government Communications Security Bureau (GCSB);
- d. **agree** to fully fund the CCIP, as set out below:

	All figures are \$m, GST inclusive				
	2001/02	2002/03	2003/04	2004/05	Outyears
Operating provisions	0.506	0.953	0.953	0.953	0.953
Capital provisions	0.269 (excl)	-	-	-	-
Outside the provisions	-	-	-	-	-
Total impact	0.775	0.953	0.953	0.953	0.953

- e. **approve** the following changes to appropriations to put into effect the decisions in recommendations 1 to 4 above:

	\$m - increase/(decrease)					
	2001/02	2002/03	2003/04	2004/05	Outyears	GST
<i>Vote Communications Security and Intelligence</i>						
Departmental output class:						
Communications Security and Intelligence (funded by revenue Crown)	0.506	0.953	0.953	0.953	0.953	incl

- f. **agree** that the increases in appropriations in 2001/2002 above be included in the 2001/2002 Supplementary Estimates and that, in the interim, these expenses be met from Imprest Supply;
- g. **approve** a capital contribution to the Government Communications Security Bureau for purchase of additional physical assets to implement the CCIP:

	\$m - increase/(decrease)					
	2001/02	2002/03	2003/04	2004/05	Outyears	GST
<i>Vote Communications Security and Intelligence</i>						

Capital contributions to the department:						
Capital investment	0.269	-	-	-	-	n/a

- h. **direct** the GCSB to implement the CCIP so that it is operational by 1 April 2002;
- i. **direct** the GCSB to report back to Cabinet by 30 June 2002, through the Officials' Committee for Domestic and External Security Coordination, on the Centre's implementation and performance; and
- j. **agree** to announce this decision as soon as possible.

Hon Trevor Mallard
Minister of State Services

ANNEX 1 - ASSESSMENT OF LOCATION OPTIONS

The following location options, chosen on the basis of a "whole of government" focus and security expertise, have been assessed:

- a. wholly within SSC;
- b. in SSC with out-of-hours cover in GCSB; and
- c. wholly within GCSB.

These options are assessed below.

Criteria

Analysis of these options is driven by the criteria of:

- *Effectiveness*, i.e. how well the proposed structure will permit the CCIP to achieve its objectives of promoting and supporting the protection of critical infrastructure from cyber-threats. This depends on the skills, tools and information available to the CCIP.
- *Perception* of the CCIP by partners, potential partners and overseas counterparts, especially in the areas of confidentiality and technical credibility. This is crucial to the effectiveness of the organisation. This is not necessarily the same as public perception. For instance, while some members of the public mistrust the GCSB, corporate decision-makers tend to see it as an effective and discreet organisation. (Although this criterion could be seen as just a component of overall effectiveness it is assessed separately because it is influenced by different factors from the other components.)
- *Least cost*. Establishment costs will increase if additional physical security of the host premises is required while staffing requirements (influenced by the host's existing skills base and ability to supplement CCIP) will have the greatest affect on operating costs.

Analysis of Options

Option	Benefit / Opportunity	Risk / Threat	Summary
<i>a Wholly within SSC</i>	<p>+ SSC has cross-government function</p> <p>+ Could be managed as a single operational unit with potential new E-government operations.</p>	<p>- SSC is not currently an operational organisation, and has no 24x7 facility.</p> <p>- Security issues - staff and building, mix of public and secure operations.</p> <p>- SSC perceived as bureaucratic.</p>	<p>Effectiveness MEDIUM</p> <p>Perception MEDIUM</p> <p>Cost HIGH</p>
<i>b SSC, with out-of-hours cover in GCSB</i>	<p>+ SSC has cross-government function</p> <p>+ Could be managed as a single operational unit with potential new E-government operations.</p>	<p>- SSC is not an 'operational' organisation.</p> <p>- Security issues - staff and building, mix of public and secure operations.</p> <p>- Discontinuities between contacts in-hours and out-of-hours; will be harder to manage and harder to form relationships with partners and overseas counterparts.</p> <p>- Potential for highly negative public perceptions since GCSB involvement may be seen as covert.</p>	<p>Effectiveness MEDIUM</p> <p>Perception LOW</p> <p>Cost HIGH</p>
<i>c Wholly within GCSB</i>	<p>+ Already has secure environment, staff all security cleared, has 24x7 operations and secure communications with overseas agencies.</p> <p>+ Has necessary skill base. CCIP function is compatible with GCSB information systems security output</p> <p>+ GCSB support is required for all options. This option alone makes GCSB involvement overt.</p> <p>+ Would be perceived to offer highest level of confidentiality for partners' information shared with CCIP.</p>	<p>- Potential for negative public perception. Could mitigate by launching alongside a new image for information systems security function.</p>	<p>Effectiveness HIGH</p> <p>Perception HIGH</p> <p>Cost LOW</p>

Conclusion

Based on the analysis above, the recommended option is wholly within the GCSB. This would best be accomplished by creating the CCIP functions as an output of GCSB.

Footnote:

1

Protecting New Zealand's Critical Infrastructure from Cyber-Threats State Services Commission, December 2000