# Telecommunications industry – New framework for network security

**Agency Disclosure Statement**

1. This Regulatory Impact Statement has been prepared by the Ministry of Business, Innovation and Employment.

2. It provides an analysis of options to implement a new framework for network security, and to implement a compliance and enforcement framework.

3. The analysis is based on the assumption that the compliance and enforcement framework will be accepted in its entirety, thereby giving the government the tools to appropriately address issues of non-compliance.

4. The analysis in this statement includes an examination of the likely costs, benefits and risks of these actions. It also outlines the alternative options that were examined during the policy process but not recommended to Cabinet.

5. The recommended options are designed to assist network operators with their duties, to clearly set out when they need to approach government and about what, and to give reassurance that government will not have unfettered powers to direct their business decisions. The framework is based on constructive partnerships being built and maintained.

6. This Regulatory Impact Statement is one of two Regulatory Impact Statements prepared to inform changes to the Telecommunications (Interception Capability) Act 2004.

[Information withheld]

12 March 2013

## Part one

## Network security

### Introduction

7. Secure and resilient telecommunications infrastructure is key to protecting New Zealander's social and economic interests, and those of the nation as a whole. It is also fundamental to New Zealand's national, economic and security interests.

8. Individuals and businesses are increasingly relying on information and communication technology (ICT) to communicate, carry out transactions, and engage with a range of service providers (including government). Equally, a number of pieces of critical infrastructure (for example, hydro dams) are operated using telecommunications networks, and rely on a reliable and secure network to do so.

9. The government, telecommunications companies, businesses and individuals may each be adversely impacted by, and must collectively address, security threats to the confidentiality of information and the availability and integrity of telecommunications infrastructure.

**Problem definition**

10. Though not new, rapid advances in telecommunications and networking technology have increased the significance and potential impacts that cyber-borne threats can pose to the security and economic well-being of a nation. These threats have been described and confronted internationally through well publicised cases, such as the compromise of several US government agencies.

11. If not carefully managed, telecommunications network providers can unknowingly be exposing their users and customers to exploitation, and enable actors with malicious intent to conduct the theft of Intellectual Property; the theft of trade secrets; nationally sensitive data; the disruption, degradation or denial of services; inflict damage to critical national infrastructure; and potentially undermine New Zealand's political and business reputation.

12. It is difficult to accurately estimate the potential costs of insecure networks, but, for instance, an attack that disabled our electricity transmission infrastructure could have a debilitating impact on the security of the nation, the economy, and public health and safety by disrupting electricity supply. As a broad indicator of potential costs, work undertaken when considering options to ensure security of water supply for hydro-electric power generation noted the cost of rolling outages to consumers alone can be significant – one estimate was around $50 million a day.[1]

13. New Zealand does not presently have any formal scheme to effectively manage and address potential national security risks associated with design, build and operation of telecommunications infrastructure (and the data carried over it).

**Status quo**

14. The government currently works with individual telecommunications operators to exchange information and provide advice on security mitigations. This is a collaborative effort to resolve security concerns.

15. The government also has the role of detecting threats and incidents (such as Denial of Service or malware attacks), working with industry after an incident has occurred, and raising awareness (particularly of risk of attack and prevention measures).

16. This approach by government has limitations as it:

    a. relies heavily on industry understanding when to approach government, and on what matters, and feeling that they can do so safely and without risk of public exposure.

    b. does not provide industry with clarity about which parts of the network the government is most concerned about, or how to approach the government to discuss security issues;

    c. is not transparent. It is unclear to the public and international partners that New Zealand has a regime for addressing security concerns; and

[1] http://www.med.govt.nz/sectors-industries/energy/pdf-docs-library/electricity-market/implementing-the-electricity-market-review-recommendations/progress-on-review-measures/emergency-water-ris-.pdf.

d. does not provide the government with any formal enforcement rights for ensuring that agreed security mitigations are put in place.

17. Continuing with the status quo is not an option if New Zealand wants to be, and be recognised as, a safe and secure place to operate in the ICT realm. Furthermore, whilst awareness raising is a sensible option and should continue, it should not be relied on as the sole intervention to ensure network security.

**Objectives**

18. The objectives of this legislative framework is to ensure risk-based and proportionate security outcomes on New Zealand's telecommunications networks from a national security perspective, premised on working with telecommunications providers, while also providing structure and transparency around roles and government powers. Specifically, this includes:

a. early identification of network security risks raising national security concerns, to enable these to be addressed in a way that supports normal business operations and aids New Zealand's economic growth,

b. risk-based security responses, proportionate to the level of national security risk involved, and

c. government requirements not imposing disproportionate cost on telecommunications users or network operators, nor unduly distorting competition or innovation in telecommunications markets.

**International context**

19. A number of other jurisdictions are equally facing the need to ensure that their telecommunications networks are secure, in the face of increasing reliance on ICT and the potential impact to national security that any significant security breach would have.

20. Australia and the United Kingdom already have broad tools available to address national security risks from telecommunications networks:

a. Australia has a general power to order a telecommunications company to suspend a specific service, or all services offered by a provider, where the supply of the service may be prejudicial to security[2], as well as an ability to refuse to grant a carrier licence where it would be prejudicial to security; and

b. the United Kingdom imposes an obligation on providers to take all appropriate steps to manage security risks to their network,[3] and has a power to order a telecommunications company suspend services on national security grounds[4].

21. Australia and the United States have made public pronouncements about network security, and specific vendors:

a. the Australian Government publicly banned Huawei from participating in the roll-out of their government funded national broadband network;

[2] Telecommunications Act 1997, section 581.
[3] Communications Act 2003, section 105A.
[4] Communications Act 2003, section 132.

b. the United States House of Representatives Intelligence Committee released a report into both Huawei and ZTE recommending the United States block acquisitions, takeovers, or mergers involving Huawei and ZTE, that government systems should not involve Huawei or ZTE, and that private entities should consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services.

22. [ Information withheld ] In Australia, a Parliamentary Joint Committee on Security and Intelligence has held hearings into government proposals which, amongst other things, suggest a network security legislative framework.

23. Given the degree of publicity that network security has attracted in the last year, and the different approaches taken in some countries, the government will inevitably face questions about whether the intention of the proposed network security framework is to targeting particular vendors or suppliers of equipment and services and/or is targeted towards particular countries.

24. The proposed framework is not directed towards any specific vendor(s). Instead, it allows the government to assess levels of risk that particular decisions raise: which may be a combination of the type of equipment, the particular area in the network, vendor, and the operational model. While, the regime may have the effect of reducing vendor choices in some limited parts of the network (based on an assessment of risk), the intent is not to ban specific vendors. Clear communications messages would be released emphasising this.

25. Network security issues can change rapidly as technology evolves and those trying to breach security get more sophisticated in their methods. As shown in the paragraphs above, there is yet to be an approach that is considered to be "international best practice". It is recommended that officials continue to share information with counterparts from likeminded jurisdictions and monitor progress and successes in those countries.

**Options**

Option one – a two-tiered framework (not recommended)

26. A two-tiered framework would see a general obligation placed on all network operators to ensure that their infrastructure, the business information held about their customers, and their customers' private information are all protected from unauthorised interference. More extensive requirements would be placed on some network operators, depending on their size, particular traffic carried over their network, or the nature of their customer base.

27. The intention of the general obligation would be to raise awareness of the importance of network security, and to allow government to work with network operators to support them in addressing risks. To assist the industry in meeting this obligation the government would provide information on security risks to the industry (where appropriate), as well as guidelines and briefs on the types of security strategies the industry can put in place to minimise national security risks when developing infrastructure and service plans. Government would provide information, where possible, so that risks could be identified early, allowing operators to take these risks into account in decision making and minimise costs. It is expected that the industry would similarly provide government with any relevant information they have.

28. The more extensive obligation would apply to network operators identified as fitting the criteria, and would be gazetted under the legislation at the time of enactment and a letter from the Director of GCSB to the companies. Network operators could also be added over time if the nature or size of their operation changed.

29. After reviewing comment from network operators through the targeted consultation process, officials do not believe this to be a practical option as:

    a. the general obligation is too broad and does not give guidance to industry as to what parts of the network the government has a particular interest in

    b. it touches on the areas of privacy and information security, which are outside the intended scope of the framework

    c. it is not immediately clear to network operators if they would be required to have more extensive obligations

    d. there is no certainty for network operators about when to engage with government and about what.

30. Although this option meets the objectives stated in paragraph 18, officials consider that the impracticalities of it outweigh any benefits. Therefore, this option is not recommended.

Option two – an obligation to engage on areas of network security that are relevant to national security (preferred option)

31. This obligation would see industry having to approach government at an early stage (preferably before procurement) for new networks or any significant changes to their existing networks. The obligation would be based on the decisions made regarding design, build or operation of a network, rather than the size or customer base of the network operator.

32. Areas of interest would be prescribed in legislation would include, but not be limited to:

    a. Network Operations Centres (including the outsourcing of these functions) [ Information withheld ]

    b. lawful interception equipment or functions [ Information withheld ]

    c. those parts of the network that manage or store (1) aggregated customer information, including authentication credentials or (2) administrative (privileged user) authentication credentials [ Information withheld ]

    d. those places in the network where data aggregates in large volumes as a result, for example, of an architectural choke point or a storage capability, in practice this may be large international and domestic gateways and/or data centres [ Information withheld ]

    e. any other area which may, in the view of the network operator, raise network security risks significant enough to impact on national security or require Government advice.

33. The legislation would also include a set of principles providing for:

a. early identification of network security risks raising national security concerns, to enable these to be addressed in a way that supports normal business operations and aids New Zealand's economic growth;

b. risk-based security responses, proportionate to the level of national security risk involved; and

c. government requirements not imposing disproportionate cost on telecommunications users or network operators, nor unduly distorting competition or innovation in telecommunications markets.

34. To make this framework efficient, the following process is proposed: (see appendix 1)

a. Both parties will share information relevant to network security and the national security risk. There will be a legislative obligation to engage in good faith.

b. A network operator approaches the GCSB if a new network, or changes to their existing network, fall within the areas of interest (listed above in paragraph 32) or can be approached by the GCSB if it has specific information relating to the network (which it may have gained through engagement or a response to an information request).

c. The GCSB will respond with risk information as soon as practicable.

d. The network operator will propose risk mitigations or solutions.

e. If the proposed mitigations and solutions are satisfactory, the GCSB will issue the network operator with a letter stating that there are no further concerns with the proposed network changes. This creates a legislative obligation on the operator to implement the agreed changes.

f. If the proposals are not satisfactory, and the risk is significant for national security, the GCSB can apply to the Minister to issue a direction for the network operator to take a specific course of action. (For full details of the Ministerial direction power, see the Compliance and Enforcement section of this document.)

35. There is a proposed compliance and enforcement framework (set out in part two of this paper) to make this option effective.

*Requirement on network operators to notify government about decisions relating to areas in the network of significant security interest (recommended)*

36. This option would include a requirement on network operators to notify government about decisions relating to areas in the network of significant interest from a national security perspective, during the planning phase for the procurement of network equipment, systems or services. Requiring engagement at this point will allow the GCSB to work with network operators earlier, which both increases the likelihood risks can be addressed, and allows for a network operator to better understand the costs and benefits of a decision (potentially reducing compliance cost).

37. To provide clarity and transparency about the kinds of decisions that raise the potential for significant security risks and receive notification, the legislation would specify those network areas of significant national security interest. These are set out in paragraph 32. The would be provision for additional network areas of significant security risks being added to the TICA over time by way of Order in Council.

38. It is also proposed that there be a threshold about the nature of decisions to be notified to ensure that government is not approached about every decision made in relation to those

areas (however insignificant) with the associated compliance cost for both industry and government. The threshold would be for proposed changes (1) to equipment used in those areas or (2) the ownership/control/oversight or supervision of those areas.

39. The legislation would provide the GCSB with statutory authority to issue statements to providers that specified changes or classes of change (for example, the replacement of a previously approved piece of equipment with the same model/type) do not meet the national security threshold and do not need to be notified.

*Obligation on network operators to engage in good faith on network security (recommended)*

40. It is proposed that there be a broad obligation on "network operators" to engage in good faith on network security matters which have the potential to impact national security *and* which relate to the design, build or operation of networks (and the data thereon) including interconnections to other networks.[5]

41. The practical corollary to this requirement is that government will provide information (where appropriate) about network security risks, and increase network operators' knowledge in this area.

42. The obligation for network operators to engage in good faith would be reinforced by a power for government to require prompt disclosure of relevant information. In accordance with current Official Information Act timeframes on government, network operators would be required to respond as soon as reasonably practicable, and no later than 20 working days after the request.

43. The legislation would also include a provision, to put the matter beyond doubt, that companies have the legal authority to provide the requested information (despite, for example, other legal or contractual requirements).

**Benefits and costs**

44. The anticipated benefits and costs to both government and industry from the proposed new network security framework are detailed in the table below.

| | Government | Industry |
|---|---|---|
| Benefits | • Removes the reliance on industry understanding when to approach government by giving clear guidance on what matters in relation to national security<br><br>• Greater transparency allows shows both the public and [ information withheld ] that there is a clear and enforceable regime for addressing security concerns | • Provides industry with clarity about which parts of the network the government is most concerned about, and how to approach the government to discuss security issues<br><br>• Gives a mandate to industry to discuss security issues with government, and confidence to know that government will not be able to direct decisions about the |

[5] By providing for interconnections to other networks, this captures where the data is routed once it leaves a network.

| | | |
|---|---|---|
| | | design, build or operation networks in an unfettered way<br><br>• Network operators will have greater access to information that may help them make more informed decisions, relating to planning and procurement |
| Costs | • The GCSB may face increased costs from the operational and liaison work to underpin the proposed framework. The GCSB will absorb those costs from within baseline and/or reprioritisation | • It is not possible to quantify costs for industry as they would differ markedly in each case. The types of costs likely to be incurred are:<br>o Collating and providing information to GCSB;<br>o Engagement with GCSB;<br>o Costs to implement the actions in a Ministerial direction.<br><br>• Some of these costs are already incurred by those members of industry with whom the government has an established relationship under the status quo; in the main the proposals build on existing practice, while providing some enforcement and direction powers to government. |

45. It is not possible to undertake a full benefit/cost analysis as the cost of a breach of national security occurring cannot be quantified in monetary terms. Serious national security issues may not end with the loss of life or commodities, but it could see, for example, the severe disruption to services (such as electricity or banking facilities), the theft of Intellectual Property, or damage New Zealand's reputation as a safe nation to transact with.

**Risks**

*Perception that the GCSB will be able to direct decisions in relation to network operation*

46. Network operators may perceive that the GCSB would have unconstrained rights of direction in relation to the operation of their networks.

47. To mitigate this, there are clear protections for industry proposed in the legislation, such as the obligation to engage in good faith, the right for the network operator to propose their own mitigations, and the right to submit directly to a Minister if a direction power is being considered.

48. [ Information withheld

49.

50.

] 

**Net impact**

51. Overall, this option will give network operators a clear steer as to which parts of the network are critical for national security, and give them the mandate to approach government on this issue.

52. This option gives government the necessary tools to engage constructively with industry, and to compel network operators to disclose important information and engage when necessary.

[ Information withheld

]

53. This option meets all of the objectives stated in paragraph 18, particularly early identification of network security risks raising national security concerns, risk-based security responses.

**Part two**

**Compliance and enforcement framework**

**Status quo**

54. There is no provision in legislation for the government to formally manage and address potential national security risks associated with design, build and operation of telecommunications infrastructure (and the data carried over it). Instead, the Government has relied on (1) being approached by telecommunications companies before significant changes are made to networks and (2) agreeing the steps required to address any potential risks to national security raised by any such change.

55. While this approach is workable for telecommunications companies with whom the government has an established relationship, it cannot apply in an effective way across the telecommunications industry.

56. Continuing with the status quo is not recommended. Where there is a significant risk to national security associated with telecommunications infrastructure, the government needs the ability to compel network operators to put in place mitigations or solutions.

**Objectives**

57. The objective of a compliance and enforcement framework prescribed in legislation is to:

    a. provide the GCSB with a practical ability to compel network operators to engage with it on matters of network security; and

    b. include a formal escalating enforcement process for responding to minor breaches of administrative requirements (to be dealt with by way of a breach notice), through to instances of serious non-compliance, with the High Court process or a Ministerial direction power available as an option of last resort.

58. If these objectives are met, it is more likely that government will be able to effectively respond to network security issues that may impact on national security. It is also more likely that network operators will comply, as these obligations should increase awareness of network security issues at the Board and Chief Executive level within many companies.

**Proposals – compliance**

*Proposal one – registration (recommended)*

59. It is proposed to require all network operators (and any service providers deemed in to interception capability obligations) to register with government, and provide specified information relating to interception capability and network security. Registration would ensure government has key information relating to those telecommunications companies.

60. To register, companies will be required to provide the following information to the agencies:

    - Name of legal entity

- Name of contact(s) for interception and security
- Address for service of warrants
- Total number of end customers and total estimated number of end users (for retailers) and total number of connections (for those who are wholesale only)
- Geographical coverage (eg. national or name of region)
- Types of services provided eg. mobile, email, VoIP (from a provided list by agencies).

61. Asking for more detail at the time of registration (for example, listing every service offered) was considered and rejected as industry indicated that this could impose heavy burdens on large operators who are generally complaint anyway.

62. The TICA would specify a statutory role to which registrations must be submitted, and give this role the statutory power to maintain a register.

63. When submitting this information, the director in each company will also be required to acknowledge that the company has legal obligations under the TICA, and that enforcement action under the TICA may be taken in cases of non-compliance.

64. Companies will be required to update this registration annually, or where there are changes to any of the answers. Changes to the number of customers or end users would only need to be reported if it were a significant change. Agencies would publish guidance on how to estimate numbers of end users, and what kinds of changes in customer or end user numbers are considered 'significant'.

65. Failure to register, and submit the required information would be subject to an escalating enforcement process, set out in paragraph 90 below.

*Proposal two – have someone with security clearance (recommended)*

66. To ensure that an effective partnership between government and network operators is established, where sufficient and timely information from Government is provided to network operators about relevant security risks to enable them successfully address them, it is important that individual(s) from network operators obtain appropriate government sponsored security clearance so that they are able to have the necessary conversations.

67. In the Interception Capability Regulatory Impact Analysis, it is proposed that there be ability for government to require security clearance for network operators with over 10,000 end-users, and this ability should also apply for network security.

68. To be consistent with the proposal in the Interception Capability proposal, there would be an ability for the GCSB to require that large and medium network operators[6] (and any service providers with standard have interception capability requirements) employ, within their company, someone who has, or is in the process of, obtaining secret level government sponsored security clearance. Where a higher security clearance is advisable, the GCSB could encourage the network operator to do this, but they would not be able to require it.

[6] That is, those network operators with over 10,000 end-users.

69. It is proposed that there be an exception for companies with under 10,000 end users, ie those who are proposed to have a 'readiness' obligation for interception capability, from the requirement to constantly employ staff who have security clearance. In practise, if needed, surveillance agencies would request relevant personnel to apply for a confidential-level security clearance or criminal record check, as appropriate, and require that they sign a non-disclosure agreement. This practise would be consistent with the current practise when working with companies who do not already have cleared staff. This process does not need to be provided for in the legislation.

70. [ Information withheld

]

*Proposal three – direction power in relation to security measures (recommended)*

71. As a tool of last resort it is proposed there be provision for a Ministerial direction. This would be available where significant national security concerns are raised in relation to an existing or future threat, or course of action (proposed or already taken) by a network operator.

72. It would only be available:

a. the GCSB has 1) informed the network operator of a security risk, and 2) believes that the proposed action (or lack thereof) in relation to that risk raises significant national security concerns; or

b. a network operator has 1) failed to comply with one of the requirements in the Act[7], 2) has since followed or proposed a course of action in relation to those matters and 3) this raises significant national security risks.

73. In those cases, the Director of GCSB would apply to the relevant Minister to exercise the direction power (see paragraphs 78-79 below for options as to which Minister would exercise the power).

74. The Director of GCSB would also be required to advise the affected network operator of this request in writing, informing the network operator of a statutory ability to submit directly to the relevant Ministers on the statutory threshold and considerations set out below. It is not proposed to extend the ability to submit more broadly to other potentially affected parties (for example, a network equipment supplier). The legislative relationship is between network operators and the government, and it is preferable for network operators to manage their commercial relationships.

75. In making the application for a direction, and in approving it, the Director of GCSB and the Minister would need to be satisfied that the direction:

a. is required to address a significant risk to national security; and

b. complies with the principles in the TICA.

[7] Specifically, to engage in good faith, comply with an information request, or notify government about specified areas.

76. The scope of the direction power would be to carry out specific steps to remedy, mitigate or avoid the security risk (which may include ceasing to take or undoing a particular course of action).

77. Given the ability for network operators to submit directly to Ministers, and the requirement for Ministers to agree (with each Minister representing a different portfolio interest), and that judicial review would remain available (please see paragraph x for proposed protections applying to any court proceedings), no right of appeal is proposed. [103]

*Options for which Minister exercises the direction power*

78. Three options are available regarding which Minister exercises the direction power:

a. the Minister responsible for the GCSB, following consultation with the Minister for Communications and Information Technology and the Minister of Trade[8];

b. the Minister for Communications and Information Technology, following consultation with the Minister responsible for the GCSB and the Minister of Trade; or

c. a wholly independent Minister (for example, the Attorney-General), following consultation with the three Ministers above.

79. Given the paramount purpose of the framework is national security, the preferred option is that the Minister responsible for the GCSB exercises the direction power.

80. While the Minister for Communications and Information Technology has a portfolio interest, in that it will impact on a member of the telecommunications industry, that portfolio does not extend to national security. A wholly independent Minister may be perceived as being in a position to better balance the interests of national security, as against the impact on a network operator, but may complicate the process (given a lack of involvement to that point).

*Proposal four – right of request to enter and inspect (not recommended)*

81. As a further means by which the authorised agencies can measure levels of compliance with both interception and security requirements, it was proposed that there be a power for a designated officer from a surveillance agency to request entry and inspection for interception compliance purposes.

82. These would be exercised where:

a. a company refuses to participate in compliance testing;

b. information was requested but not provided or provided outside timeframes;

c. information is provided that is suspected to be false or is inadequate; or

d. it is suspected that the company is non-compliant.

83. While this is appropriate and recommended in relation to interception, it was not considered appropriate for network security. After consideration, it was agreed that there would be no apparent benefit for the GCSB to be able to enter a premises to inspect.

8. [ Information withheld ]

84. This option is consistent with the objectives in paragraph 57, but for the reasons above, officials do not recommend it.

*Proposal five – compliance testing (not recommended)*

85. [ Information withheld

86.

*Proposal six – right to formally request specific action be taken in relation to security measures (not recommended)*

87. Consideration was given to providing the Director of GCSB with the right to formally request that a network operator take, or not to take, a specific course of action in relation to security measures. It was thought that this could be applied an intermediate step between engaging with a network operator and applying to the Minister for a direction power.

88. While there seemed to be merit in the proposal, the Director of the GCSB is unlikely to ever formally request a network operator take specific action without first discussing this with, and getting the agreement of, the Minister responsible for the GCSB. Therefore, it would in effect duplicate the proposed direction power (set out in proposal eight below).

89. This option is consistent with the objectives in paragraph 57, but for the reasons above, officials do not recommend it.

**Proposals – enforcement**

*Proposal seven – basic non-compliance (recommended)*

90. Basic non-compliance which, for network security, would include:

a. failure to respond, within the statutory timeframe, to the requirement of registration (including failure to provide one of the component parts of the registration, such as specified information);

b. failure to comply with a request that a network operator employ someone within their company that has the required secret security clearance;

c. failure to meet the notification requirements on specified network security matters;

d. failure to comply with a request for information under the Act; and

e. failure to propose a response (in writing) to address a risk that the GCSB has informed the network operator about.

91. Breaches falling into this category involve straightforward issues of fact, and be considered at the minor end of the scale (in terms of gravity and impact).

92. For basic non-compliance, it is proposed that the GCSB would send a notice of breach to a network operator, setting a defined period of time within which the provider must comply (for example, 10 working days), and advising that if the company does not respond within

that period, the breach will become *serious non-compliance* and be dealt with through the process for serious non-compliance.

93. For consistency and certainty for both government and industry, it is proposed that the notice of infringement be prescribed in legislation.

*Proposal eight – serious non-compliance (recommended)*

94. It is proposed that the Crown would send a notice of serious non-compliance to a telecommunications company, advising that they will initiate High Court proceedings under the Act, in which they will seek pecuniary penalties at the current level in the TICA (maximum of $500,000, and $50,000 per day for so long as the breach continues).

95. The process for responding to serious non-compliance for network security differs from that contemplated for interception capability (and the current process in the TICA). Given the breaches are framed in a way that they can be straightforwardly determined, the Crown would not be required to seek a compliance order from the High Court. Instead, once a breach has occurred, the Crown could proceed directly to the imposition of civil pecuniary penalties through the High Court. It is also worth noting that the penalties scheme includes an implicit incentive to address the non-compliance, given a penalty of $50,000 per day can be imposed for so long as non-compliance continues.

96. As with the notice of infringement, the notice of serious non-compliance would be prescribed.

*Proposal nine – arbitration in cases of serious non-compliance (not recommended)*

97. To provide for a faster enforcement process, where the decision-maker would have greater specialist expertise, the option of providing the agencies with the ability to go to arbitration under the *Arbitration Act 1996* in cases of serious non-compliance was considered.

98. The arbitrator would have had the same ability as the High Court to impose a compliance order, and pecuniary penalties where a network operator breaches the compliance order.

99. This was considered for both the interception capability and network security regimes. In both cases, the intention of allowing an arbitration process was to allow government and network operators to work through differences without the publicity of the High Court, and to have another step in the escalation process before going to Court. However, arbitration is used to deal with disputes rather than issues of non-compliance, so the proposal is not suitable.

**Benefits and costs**

100. The anticipated benefits and costs to both government and industry from the compliance and enforcement frameworks are detailed in the table below.

| | Government | Industry |
|---|---|---|
| Benefits | • Greater ability for government to compel industry to approach before decisions are made about new networks or significant | • Graduated enforcement framework means that there are several points at which network operators can negotiate successful outcomes |

| | | |
|---|---|---|
| | changes to networks<br><br>• Ability to try to resolve issues at an early stage to lessen the chance of a public Court case | before any Court action is pursued |
| Costs | • While the GCSB may face increased costs from the proposed compliance and enforcement framework, the GCSB will absorb those costs from within baseline and/or reprioritisation | • There may be costs for individual network operators if enforcement action is taken, [ information withheld ]<br><br>• There could be costs for individual network operators to implement the actions in a Ministerial direction. These costs would differ in every case. [ Information withheld ] |

101. This option meets the objectives stated in paragraph 57.

**Risks**

*Exposing weak points in the network*

102. If a case of non-compliance was taken to the High Court, it could expose weak points in networks. This could lead to malicious actors exploiting those weaknesses.

103. To mitigate this, the framework gives the GCSB and industry many chances to negotiate solutions and mitigations out of the public eye. If the relationship had broken down to the extent that Court action was the only option, it is proposed that protections be put in place to keep classified documentation out of public scrutiny.

**Net impact**

104. Overall, having a compliance and enforcement framework will allow the GCSB to ensure that network operators are complying with their obligations, and gives them a means to check compliance, and , when necessary, to take appropriate enforcement action.

105. For network operators, this framework will give clarity about what is expected of them, and should increase the likelihood of compliance. Having a graduated enforcement regime will make it more likely that compliance will be enforced. There may be increased costs if enforcement action was taken, or to implement actions specified in a Ministerial direction power, however, [information withheld]

**Part three**

**Conclusions and recommendations**

106. The Ministry of Business, Innovation and Employment recommends that:

a. The proposal to have a two-tiered network security framework does not proceed

b. The proposal to have an obligation to engage on areas of network security that are relevant to national security proceeds

c. The compliance and enforcement framework, as described in part two, proceeds in its entirety.

**Implementation**

107. [ Information withheld

108. ]

**Monitoring, evaluation and review**

109. At this stage there is no plan do undertake any formal review or evaluation after implementing the legislation. Officials will monitor the operation of the provisions and report to relevant Ministers if any issues arise.

**Part four**

**Industry consultation**

110. In developing the above proposals [Information withheld] telecommunications industry members were consulted.

111. Wider consultation with industry was not undertaken, given the technical and sensitive nature of the subject-matter, [ Information withheld

]

**Departmental consultation**

112. The proposals have also been developed with significant input from, the Government Communications Security Bureau, and the National Cyber Policy Office (within the Department of the Prime Minister and Cabinet).

113. The Treasury was consulted. The Ministry of Justice, Ministry of Foreign Affairs and Trade and the Privacy Commissioner were consulted on the proposals in this paper. New Zealand Customs and the Department of Internal Affairs were informed of the proposals in this paper.

# Appendix One: Network Security

## *General Obligations*

Network operators register under the Act

(Breach = basic non-compliance)

Network operator required to have staff member with security clearance

(Breach = basic non-compliance)

Obligation for network operator to engage in good faith

(Breach = if a network operator withholds relevant information, and there are significant national security concerns with a subsequent course of action – Ministerial direction power may be exercised)

Network operator to comply with requests for specific information

(Breach = basic non-compliance. However, if information is withheld, and there are significant national security concerns with a subsequent course of action – Ministerial direction power may be exercised)

Network operators notify of changes in relation to areas of significant concern in the network

(Breach = basic non-compliance. However, if there is a failure to notify, and there are significant national security concerns with a subsequent course of action– Ministerial direction power may be exercised)

## *Specific security risks identified*

Network operator informed of risk by GCSB

Network operator proposes a response (in writing) to address risk

(Breach (ie no written response) = basic non-compliance. However, if there is no response and there are significant national security concerns with a subsequent course of action – Ministerial direction power may be exercised)

The GCSB assesses the proposed response.

Response satisfactory: GCSB informs the operator (in writing), and network operator obliged to implement (unless subsequently varied by mutual agreement).

(Breach (ie failure to implement) = serious non-compliance)

Response unsatisfactory: if significant national security concerns – direction power may be exercised

Response unsatisfactory, but does not raise significant national security concerns: this does not link to the enforcement framework because there is no 'breach', and it does not raise concerns at a level the Ministerial direction power should be exercised.

## *Compliance and enforcement*

Ministerial direction power (where significant national security concerns raised).

If non-compliance, it becomes serious non-compliance

Basic non-compliance (notice of non-compliance, with specified time to address): failure to - register/clear staff/comply with information request/notify of changes in relation to areas of significant interest /propose a response in writing to address a risk.

If continuing non-compliance, it becomes serious non-compliance

Serious non-compliance (High Court directly for pecuniary penalties): includes continuing non-compliance / failure to implement agreed mitigations (as set out in writing by GCSB) / failure to comply with a Ministerial direction power.