



Proactive Release

The following Cabinet paper and related Cabinet minute have been proactively released by the Department of the Prime Minister and Cabinet, on behalf of Hon Kris Faafoi, Minister of Broadcasting, Communications and Digital Media:

Refresh of New Zealand's Cyber Security Strategy:
Ensuring New Zealanders are Confident and Secure in the Digital World

Date of release: 23 August 2019

The following documents have been included in this release:

***Title of paper: Refresh of New Zealand's Cyber Security Strategy:
Ensuring New Zealanders are Confident and Secure in the Digital World
(DEV-18-MIN-0256 refers)***

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant section of the Act that would apply has been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Key to redaction code:

- 6(a): to avoid prejudicing the international relations of the New Zealand Government;
- 9(2)(f)(iv): to maintain the confidentiality of advice tendered by or to Ministers and officials; and
- 9(2)(g)(i): to maintain the effective conduct of public affairs through the free and frank expression of opinion.

Office of the Minister of Broadcasting, Communications and Digital Media
Chair, Cabinet Economic Development Committee

REFRESH OF NEW ZEALAND'S CYBER SECURITY STRATEGY: ENSURING NEW ZEALANDERS ARE CONFIDENT AND SECURE IN THE DIGITAL WORLD

Proposal

1. This paper seeks agreement to a refreshed Cyber Security Strategy (the Strategy) for New Zealand, to progress priority actions to give effect to the Strategy, develop a work programme to deliver the Strategy, and establish new ways of working to deliver a joined-up approach to cyber security in New Zealand.

Executive Summary

2. Being connected online has greatly benefited New Zealand. We are more closely connected than ever before, which has underpinned our prosperity and helps to negate the downsides of distance. Effective cyber security is fundamental to a thriving online society, especially as cyber risks continue to evolve.
3. Since the 2015 Cyber Strategy was developed, cyber threats have continued to grow in number, scope and scale. Our personal information, bank accounts, intellectual property and other data are at risk on a daily basis, threat actors are becoming more sophisticated, and as digital technologies continue to evolve at pace, the threat environment becomes more challenging. In light of this, in April 2018, Cabinet agreed it was timely to refresh the Cyber Security Strategy, to ensure that the government is investing the right resources in the right way across the system to respond to growing cyber security threats [CAB-18-MIN-0127].
4. The proposed 2018 Cyber Security Strategy has a vision that *New Zealand is confident and secure in the digital world* – it is about enabling New Zealand to thrive online. The Strategy's five priorities are:
 - Cyber security aware and active citizens
 - A strong and capable cyber security workforce and ecosystem
 - Internationally active
 - A resilient and responsive New Zealand
 - Proactively tackle cybercrime.
5. Once Cabinet has considered the Strategy, I propose to lead the development of a work programme to support the Strategy, with actions to further each of the priorities identified above, reporting back to Cabinet in the first half of 2019. 9(2)(f)(iv)

9(2)(f)(iv)

9(2)(f)(iv)

6. The government's current institutional arrangements have supported New Zealand's response to national cyber security risks to date. However, there are limitations with the existing arrangements, which need to change in order to take a more joined-up approach to deliver the Strategy, and deliver better cyber security and cyber crime outcomes for New Zealand. To support the transition to a future system where agencies work together to effectively prevent, prepare for and respond to cyber security risks I recommend:

- establishing a government Cyber Security Strategy Co-ordination Committee, ^{9(2)(f)(iv)} [redacted], to plan, monitor and govern the Strategy work programme
- applying the new Strategy principles to guide the work to give effect to the Strategy
- working more closely with organisations that have not been involved in developing cyber security policy, to get broader input and engagement
- 9(2)(f)(iv) [redacted]

7. I also seek Cabinet's agreement to develop the following ideas further, and report back on the feasibility, desirability and viability of creating:

- 9(2)(f)(iv) [redacted]
- [redacted]
- a new appropriation for cyber security system initiatives.

8. 9(2)(f)(iv) [redacted]

Background

Cyber security is fundamental to a robust and thriving digital society

9. New Zealand is increasingly connected – the Internet and information communications technologies (ICTs) are a core part of our personal and professional lives. The government has committed to building a connected nation and to harnessing digital technologies for economic growth, community benefit, and for innovation. This commitment is reflected in a range of other initiatives.

10. Effective cyber security is essential to ensure that the gains from digital technology are not eroded, to protect the information and networked systems that are important to us, and to empower New Zealanders to interact online without suffering harm. Good cyber security posture can help us to make the most of the opportunities that the Internet provides. Cyber security maturity may also facilitate greater economic competitiveness and offer other economic opportunities and benefits.

11. Key achievements of the 2015 Cyber Security Strategy are:

- the establishment of CERT NZ

~~BUDGET SENSITIVE~~

- the rollout of CORTEX by the Government Communications Security Bureau (GCSB)
- the development of a Cyber Credentials scheme for small-to-medium enterprises
- holding New Zealand's first Cyber Security Summit
- developing a cyber security qualification.

12. Despite these system gains, cyber security risks have continued to increase and evolve.

13. On 2 April 2018, Cabinet agreed it was timely to undertake a refresh of New Zealand's cyber security settings to ensure that the government is investing the right resources across the system to respond to growing cyber security threats. It was also noted as being complementary to this Government's other digital initiatives [CAB-18-MIN-0127]. The Chair of the Cabinet External Relations and Security Committee (ERS) subsequently agreed to extend the report back from July to October 2018 to accommodate a more collaborative engagement approach to the Refresh [ERS-18-MIN-0010].

Malicious cyber activity is increasing and the threat will keep evolving

14. The nature of the cyber security threat facing New Zealand has changed since 2015. The threats are increasingly diverse and can affect anyone, from individuals, to businesses, and government, and critical national infrastructure such as banks and power companies. The potential harms include emotional distress, financial loss, reputational damage, loss of intellectual property, and disruption to critical services.

15. The volume of malicious cyber activity is growing, with cyber threat actors of all kinds becoming increasingly bold, brazen and disruptive:

- The National Cyber Security Centre (NCSC) in the GCSB recorded 396 cyber threats in the year ended 30 June 2017, up from 338 the year before.¹
- CERT NZ received over 700 reports in the second quarter of 2018, with \$2.2 million in reported losses.²
- 9(2)(f)(iv) [REDACTED]

16. These numbers are the tip of the iceberg, as many cyber incidents go unreported. As the use of Internet-connected devices increases, so too does the potential pay-off from cybercrime.

Technological change is rapid and unpredictable

17. As digital technologies continue to evolve at pace, the threat environment becomes more challenging. For instance, Internet-of-Things (IoT) devices (such as exercise trackers and connected home appliances, or industrial devices such as sensors) have become commonplace, bringing a much wider range of Internet-connected devices into homes and businesses across New Zealand. IoT devices can, and have, been used to launch attacks. For example, in October 2016, millions of IoT devices were taken over to

1 National Cyber Security Centre, *Unclassified Cyber Threat Report*, 2016/17.

2 CERT NZ, *Quarterly Report*, Q2: 1 April- 30 June 2018.

3 9(2)(f)(iv) [REDACTED]

form the Mirai botnet⁴, which was used to disrupt the Internet for almost the entire eastern United States.

18. It is not always possible to predict the full impacts of rapidly evolving technologies. The newest technologies, such as artificial intelligence, quantum computing, robotics and IoT, while providing benefits, also provide more opportunities for malicious actors. These technologies will continue to become increasingly available to a wider range of actors, both state and non-state. At the same time, some of these technologies can also be used to detect and disrupt malicious intrusions. In addition, the advent of 5G networks will create new network and national security issues for New Zealand.

Shifts in the international context have increased the risks for New Zealand

19. Changes in the international geopolitical landscape affect the cyber security risk facing New Zealand. Growing great power competition and increasing challenges to the rules-based international order are also reflected in and manifest through increased uncertainty in cyberspace. Nation states are using cyber tools for geopolitical advantage (one example being the reports of Russian interference in the 2016 United States Presidential election). The number of state-sponsored cyber operations is rising and more governments are openly developing offensive cyber capabilities. New Zealand needs to act to defend the rules-based international order and be ready to prevent, deter and respond to these risks when they arise.

A refreshed Strategy: New Zealanders are confident and secure in the digital world: Enabling New Zealand to thrive online

20. The draft Strategy was developed using a co-creation model and draws on a range of sources to ensure that we are adapting to the growing and evolving threat. The Strategy includes a narrative that sets out why we need a Cyber Security Strategy (including addressing the evolving risk and realising the opportunities of a connected world), the values and principles underpinning the Strategy, five priorities and a small number of priority actions that can be progressed now to contribute to achieving the Strategy. The draft Strategy is attached to this paper.
21. The Strategy has a vision that “**New Zealand is confident and secure in the digital world**” – it is about enabling New Zealand to thrive online. The vision articulates our aspiration that New Zealand (both New Zealand as a state and every person in New Zealand) is enabled to make the most of the opportunities offered by digital technologies, without suffering harm or loss. The vision was chosen to acknowledge that while Internet connectivity brings risks, we can take action to minimise those risks, and that connectivity is vital so that New Zealand and New Zealanders thrive and prosper.
22. The five priorities are collectively intended to empower New Zealanders online and to ensure that New Zealand is a safe and secure place in which to live and to do business.
23. The main changes from the 2015 Strategy are summarised in the table below:

Element	Strategy (2015)	Draft refreshed Strategy	Reason for the change
Vision	A secure, resilient and prosperous online New Zealand.	New Zealand is confident and secure in the digital world.	The new vision acknowledges that internet connectivity is an integral part of New Zealand’s economic

4 A botnet is a network of internet-connected devices that have been infected by malicious software.

~~BUDGET SENSITIVE~~

Element	Strategy (2015)	Draft refreshed Strategy	Reason for the change
			growth, and our response to the risk needs to be commensurate with our dependence – we need to empower New Zealanders to engage and be confident online.
Values	The principles from the 2015 Strategy are now the values of the draft refreshed Strategy.	<p>The 2015 principles were reframed as values:</p> <ul style="list-style-type: none"> • Partnerships are essential • People are secure and human rights are respected online • Economic growth is enabled • National security is upheld. 	<p>Engagement on the Refresh showed the 2015 principles remain valuable and should be retained. We reframed them as ‘values’ to reflect the role they play in decision-making and shaping our future.</p> <p>These values reflect the importance of collaboration in addressing cyber security challenges, the increasing significance of digital rights, and the criticality of the digital economy for New Zealand’s economic future.</p>
Principles	The principles from the 2015 Strategy are now the values of the draft refreshed Strategy.	<p>Five new principles have been introduced to guide how we work to deliver the vision. We will work with others in a way that:</p> <ul style="list-style-type: none"> • builds and maintains trust • is people-centric, respectful, and inclusive • balances risk with being agile and adaptive • uses our collective strengths to deliver better results and outcomes, and • is open and accountable. 	<p>Adding these principles acknowledges that cyber security is not a ‘problem’ the government can fix - it is everybody’s responsibility and means we are going to need to work together in different ways to get better results. These principles were designed using feedback from the workshops in the engagement rounds.</p>
Priorities	<p>The four intersecting goals were:</p> <ul style="list-style-type: none"> • Cyber capability • Cyber resilience • International co-operation • Addressing cybercrime 	<p>The proposed five priorities are:</p> <ul style="list-style-type: none"> • Cyber security aware and active citizens • Strong and capable cyber security workforce and ecosystem • Resilient and 	<p>Feedback from engagement was that the 2015 goals were still relevant, but they were too narrow, and instead we should be focusing on priorities that enabled us to be more ambitious. The addition of the ‘cyber security aware and active citizens’ priority reflects the</p>

Element	Strategy (2015)	Draft refreshed Strategy	Reason for the change
		responsive NZ <ul style="list-style-type: none"> Internationally active Proactively tackle cybercrime 	extensive feedback we received that this needs to be a stronger focus.

The refreshed Strategy outlines five priorities

24. The Strategy will provide a framework for a range of new activities under five priorities to support the Government’s vision, and to deliver the Strategy:

- Cyber security aware and active citizens
- Strong and capable cyber security workforce and ecosystem
- Resilient and responsive New Zealand
- Internationally active
- Proactively tackle cybercrime.

25. For the purposes of the Strategy, cyber security refers to protecting people and their computers, networks, programmes, and data from unauthorised access, exploitation or modification. Cybercrime is defined as crimes directed at computers or networks, and cyber-enabled crime is any crime that is assisted, facilitated or escalated in scale by the use of technology. In this paper we use the term cybercrime to refer to both pure cybercrime and cyber-enabled crime.

Cyber security aware and active citizens

26. This priority is new and is about building a culture where people can operate securely and safely online and know what to do if something goes wrong. Our work will focus on:

- practical, targeted and regular awareness campaigns to build awareness and resilience among different groups of people
- making it easier for everybody to report cyber incidents and get help from relevant government agencies
- increasing the availability of educative tools so people can be secure and safe online
- increasing efforts to educate vulnerable users, such as the elderly, children and youth to prevent victimisation
- sharing research so people can understand the threat and vulnerability landscape for their businesses, communities and families.

A strong and capable cyber security workforce and ecosystem

27. New Zealand needs to be able to rely on a strong cyber security workforce, capable of preventing, adapting to, and responding to threats. Given it is a highly connected, educated and comparatively insulated market, New Zealand has the potential to become a hub for academic and other research.

28. Our work will focus on:

~~BUDGET SENSITIVE~~

- incentivising and increasing the supply of skilled cyber security workers
- supporting the expansion of roles and opportunities for cyber security workers
- incentivising the growth of the cyber security industry in New Zealand
- supporting industry and professional organisations to promote responsible management of cyber security across their organisations and workplaces
- encouraging the development of a world-class cyber security academic research community
- supporting high-quality cyber security research and encouraging links between academia and industry.

Internationally active

29. This priority is about ensuring that New Zealand's cyber interests will be advanced and protected through our international activity. We will influence internationally to promote our vision of an open, secure, free and multi-stakeholder cyberspace.

30. New Zealand's international engagement on cyber security issues will:

- build clearly prioritised international partnerships and cooperation at policy and operational levels
- influence to support the rules-based international order and a free, open, multi-stakeholder Internet
- prevent, detect, deter, and respond to malicious behaviour online
- secure our neighbourhood by strengthening regional capacity-building, confidence, and operational cooperation, including for law enforcement activities
- contribute to New Zealand's economic prosperity.

Resilient and responsive New Zealand

31. This priority is about ensuring that New Zealand can resist cyber threats and that we have the tools and know-how to protect ourselves. The focus of this area is expanding from building resilience in significant infrastructure to being able to respond to incidents across the system.

32. That wider system focus will include:

- vigorously protecting New Zealand's most important information infrastructures
- supporting businesses, NGOs, community organisations, and individuals to be protected from and resilient to major cyber incidents
- using cyber tools and partnerships to further New Zealand's interests, including national security and law enforcement activities
- supporting critical national infrastructure organisations and ensuring those organisations take responsibility for the security of their systems
- improving the information security capabilities and resilience of the public sector.

Proactively tackle cybercrime

33. This priority is focused on ensuring that New Zealand can proactively and collaboratively prevent, investigate, deter and respond to cybercrime.
34. Key areas of focus will include:
- seeking Cabinet agreement to accede to the Council of Europe Convention on Cybercrime (the Budapest Convention)
 - preventing cybercrime particularly for vulnerable groups
 - increasing support to people affected by cybercrime
 - encouraging reporting of cybercrime and improving sharing of information about cybercrimes
 - improving information-sharing between law enforcement and the financial sector to reduce victimisation
 - making the law fit-for-purpose to enable agencies to better manage and respond to cybercrime
 - investing more to contribute to international efforts to deter organised cybercrime at the source, before it affects our communities
 - investing more in skilled people and resources to combat cybercrime and cyber-enabled crime.

Delivering the Strategy: Seven short-term priority actions, followed by an annual work programme

35. If Cabinet agrees to the attached Strategy, I will lead the development of a work programme to support the Strategy and actions to further each of the priorities identified above. I will report back to Cabinet in 2019 with the work programme that includes actions from each of the following categories:
- *Finish* – actions from the 2015 Strategy that will be delivered in the first year of the refreshed Strategy; for example, seeking Cabinet approval to accede to the Budapest Convention.
 - *New* – developing new actions the Government will start and aim to deliver over the next five years of this Strategy (2019 – 2023), including seven priority actions to be developed in the short term.
 - *Explore* – identifying and defining actions to respond to emerging and complex challenges and opportunities over the first couple of years to inform our work programme for the latter years of the refreshed Strategy and shape our future.
36. This sequenced approach will enable prioritised actions to be progressed and allow time for more detailed engagement with relevant government and non-government stakeholders on new initiatives that require further scoping. These actions, taken together, will support a cyber security system shift to enable New Zealanders to be confident and secure in the digital world.


37. 9(2)(f)(iv)

9(2)(f)(iv)

~~BUDGET SENSITIVE~~


38. A few basic changes to consumer attitudes and cyber security behaviours would deliver a significantly more robust security environment. Population-wide behaviour change is a significant challenge and requires a long term, multifaceted approach, but we know from previous campaigns in other areas (such as smoking cessation) that it is achievable.

39. 9(2)(f)(iv)



40. CERT NZ runs an annual cyber security awareness week (Cyber Smart Week). This action will make use of and build on this and other existing awareness raising events.

9(2)(f)(iv)



- 45. New Zealand's cyber security industry, while highly skilled, has not grown to match the pace at which New Zealand's economy has become digitised. Growing the New Zealand cyber security industry would make cyber security services more available to businesses and consumers - making New Zealand a more secure place to do business - and ensure that security keeps pace with the digitisation of the economy.
- 46. There is also a significant export opportunity. The global security market is estimated to be worth more than \$100 billion – and is expected to more than double by 2020. Developing a world-class domestic industry will open the door to this globally competitive industry, contributing to New Zealand's economic growth.

47. 9(2)(f)(iv)

48.

9(2)(f)(iv)

49. 9(2)(f)(iv)

50. 6(a), 9(2)(f)(iv)

51.

52.

9(2)(f)(iv)

Proactively released by the Minister of Broadcasting, Communications and Digital Media

61. 6(a) [Redacted]

62. 6(a), 9(2)(g)(i) [Redacted]

63. 6(a) [Redacted]

64. 6(a) [Redacted]

65. Enhancing our cyber defence capabilities will also enhance New Zealand's abilities to deliver the other priority actions, for instance, 9(2)(f)(iv) [Redacted]

9(2)(f)(iv) [Redacted]

66. People and businesses wanting cyber security help, or to report cybercrime and other cyber-related harm, are currently faced with a confusing set of options. It is not always easy to get the help that is needed, and the data that could inform public and private sector responses from reporting could be shared differently to get better results for everyone.

67. The reasons for seeking help or reporting an incident vary depending on the person or entity. Some want law enforcement to pursue the perpetrator, stop ongoing victimisation, retrieve defrauded money, and/or connect people to support services; others seek remediation advice or simply want information useful for technical responses and mitigation.

68. 9(2)(f)(iv) [Redacted]

- 9(2)(f)(iv) [Redacted]
- [Redacted]

- 9(2)(f)(iv)

69. 9(2)(f)(iv)

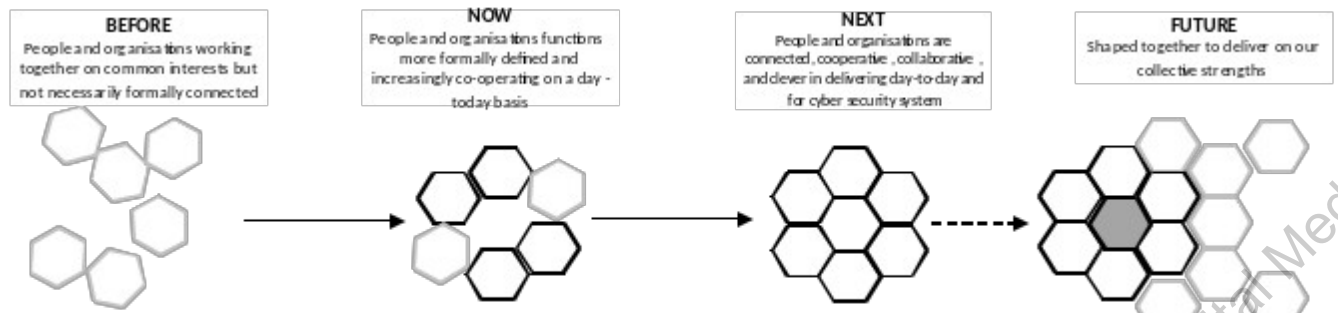
70. 9(2)(f)(iv)

Delivering the Strategy: working together more effectively

71. Over recent years, government has contributed to important advances in response, awareness, and good practice for cyber security. The government, however, cannot address cyber security challenges alone. Cyber security is not a closed system or service provided and managed exclusively by government: digital technology and cyber security crosses business, professional, personal, and national borders.
72. The government is not usually the first place people go for help with cyber security problems. A person may call their internet service provider, the retailer, the company, or a family member before seeking help from, or informing, the government. Partnering and working with these parties, businesses, NGOs, and education, research, and community organisations is essential to delivering the refreshed strategy.
73. The government's current institutional arrangements have supported New Zealand's response to national cyber security risks to date. Government's cyber security system involves agencies carrying out a range of cyber security functions. This reflects the increasingly digitally connected way in which people, government, businesses, and community organisations operate on a daily basis – no one agency has an exclusive mandate and there are benefits to agencies retaining connections with the functions that complement their cyber security activities within their agencies.
74. There are five primarily operational agencies: National Cyber Security Centre (GCSB), CERT NZ, NZ Police, Department of Internal Affairs (Electronic Messaging Compliance, and Censorship Compliance teams), and NetSafe (an NGO contracted to government to provide cyber safety services to the public).⁵ There are an additional seven agencies with policy and strategic interests in cyber security: National Cyber Policy Office (DPMC), Ministry of Foreign Affairs and Trade, Ministry of Business, Innovation and Employment, Ministry of Justice, Government Chief Digital Officer, Ministry of Defence, and the New Zealand Defence Force.
75. The diagram shows the proposed shift for government over time. Ultimately, we want to be in a position where government is playing an integral role, closely connected to domestic and international partners to improve cyber security outcomes.

⁵ Netsafe is an independent, non-profit New Zealand organisation focused on online safety. It helps people stay safe online by providing online safety education, advice and support. It can provide information and advice about using digital technology safely, and about managing online challenges like online harassment, bullying abuse and scams

BUDGET SENSITIVE



76. During the Refresh, behavioural and procedural barriers to working together more effectively, and with the private and NGO sectors, were identified. This is to be expected given agencies are at different levels of maturity: the system in general, and for some agencies in particular, has been in growth and establishment phases, especially since 2011. All agencies appear to be on an upward capability trajectory, and building on current areas of maturity will deliver benefits.

77. At this stage, resolving current challenges does not require structural reform. This would risk undermining progress and responsiveness when agencies need to be growing capability in the face of an evolving threat. In addition, State Sector Act reforms may facilitate new institutional arrangements, which could help support the refreshed Strategy in the future. Therefore, I do not propose changing the current form of agency cyber security functions, including those of CERT NZ, or establishing a new single cyber security agency.

78. The current institutional arrangements rely on agencies to plan, deliver, and engage with people and stakeholders separately with the broader cyber-security system goals in mind, and voluntarily participate across agencies to give effect to the current Strategy. There are limitations to what agencies can achieve for the cyber security *system* and for the refreshed Strategy through these practices. The three main challenges with the current approach that need to be addressed across all agencies with cyber security functions to transition from 'now' to 'next' are:

- a. **improving the reach and quality of engagement** - adoption of effective cyber security practices is not happening at the scale and pace necessary to minimise preventable harm and disruption caused by cyber security breaches. To maximise the benefits of the government's contribution, it needs to better understand the needs of people, businesses, and community organisations; and design solutions with them (or with what they've told us in mind) so that we can deliver value for money, and get the desired outcomes.
- b. **adopting a system approach** - agencies are often limited to seeing part of the picture due to the natural gaps and overlaps within the cyber security system, and expertise is spread across the public, private and NGO sectors. This means that working 'alone' (within an agency) increases the risk of delivering services and policies that do not adequately meet the needs of users, partners, and participants. Given the complex and changing nature of cyber security, rigidly pinning down every detail is likely to inhibit the flexibility needed to respond to evolving threats.
- c. **applying system governance and leadership** - agencies want to do more but the 'voluntary engagement' model has limitations because agencies are only responsible and accountable for delivering on their contributions through their

~~BUDGET SENSITIVE~~

agency. In addition, projects that cross agency 'boundaries' and would further the system (though not necessarily the agencies' priorities) are sometimes deprioritised in favour of business-as-usual or agency-specific projects because they are resource intensive and internal projects are easier to manage.

- 79.** To minimise preventable harm and disruption at the desired scale and pace, the government needs to work together and with people, businesses, and community organisations in different ways to reach more people, and get the depth of skills and volume of information needed to effectively prevent, prepare for, and respond to, cyber security risks.
- 80.** The changes and ideas outlined below reflect solutions agencies identified to address the above challenges. Some of the challenges are familiar, and can be addressed through good practice. Others, however, are complex - so we need to develop, assess, adopt, and evaluate these ideas as they form into emerging practice. One of the ways of managing the risk associated with emerging practice is to start small and scale according to scope, time, functions, and participants depending on the results of assessments and evaluations; and the changing cyber security system.
- 81.** To support the transition from 'now' to 'next' so that the government can address the above challenges and foster a more joined-up approach to delivering the Strategy, I propose that relevant agencies:
- a. establish a government Cyber Security Strategy Co-ordination Committee, ^{9(2)(f)(iv)} [REDACTED], to plan, monitor, and govern the annual work programme. This will focus on governing joint-agency projects to tackle shared problems. Membership and functions of this Committee will need to be aligned to others within government, for example, the Government Chief Digital Officer and the proposed Government Chief Information Security Officer, noting however that the Committee's focus will be 'whole of New Zealand', as distinct from a focus solely on the government's own systems
 - b. apply the new Strategy principles during the planning, conduct, and assessment of projects and initiatives to give effect to the Strategy
 - c. work more closely with other organisations, including those outside ICT and cyber security, and participate in events to get broader input and engagement with people, businesses, and community organisations (including, for example, the small business roadshow, and forums with Māori, Pasifika, consumers, older people, and youth)
 - d. ^{9(2)(f)(iv)} [REDACTED]
- 82.** Appendix A presents these changes to ways of working in more detail, including the desired outcomes, how the proposal addresses the challenges, the key risks, and timing and resources.
- 83.** Three of the proposed changes to ways of working come with risks because they may involve the government adopting emerging practice, and have funding and resource implications. I seek Cabinet's agreement to develop these ideas further to assess their feasibility, desirability, and viability:

a. 9(2)(f)(iv)



b. 9(2)(f)(iv)



- c. create a new appropriation for cyber security *system* initiatives: this appropriation would fund joint agency projects on the Strategy's work programme only. It is not intended to amalgamate all the appropriations for cyber security work. The work programme development process would identify projects, and necessary reprioritisation of funding, and budget bids for this appropriation. It could include club-funding, reprioritised funds, or new funding depending on the future work programme.

84. 9(2)(f)(iv)



85. Additional detail about the desired outcomes, how the proposal addresses the challenges, the key risks, and timing and resources for these ideas is set out in Appendix B.

86. If Cabinet agrees, I will report-back, when the work programme is submitted for Cabinet approval, with the results of the analysis of the above ideas, including any funding and structural implications, and the feasibility and viability of them. For example, there may be implications for the functions of the National Cyber Policy Office.

87. 9(2)(f)(iv)



Next steps

88. If Cabinet agrees to the proposed Strategy 9(2)(f)(iv), I will prepare the Strategy for public release. Officials will also commence work to ensure the Strategy can

be delivered, 9(2)(f)(iv) [REDACTED]. The proposed Cyber Security Co-ordination Committee will commence work to develop the work programme to include additional actions relating to each of the priorities. I will report back to Cabinet with the proposed work programme and on the proposals to develop a more joined up approach to deliver the Strategy, in the first half of 2019.

89. As noted above, new funding will be required to deliver the package of priority actions. To resource this, officials will develop the joint cyber security initiatives for Budget 2019. A sector-wide initiative will facilitate system-wide consideration of how cyber security is resourced and ensure that the initiatives are complementary to each other and to existing cyber security spending.

Consultation

90. The following government agencies were consulted during the development of the Strategy refresh and this Cabinet paper: Government Communications Security Bureau (including the National Cyber Security Centre), New Zealand Security Intelligence Service, CERT NZ, Ministry of Business, Innovation and Employment, Ministry of Defence, New Zealand Defence Force, Ministry of Foreign Affairs and Trade, Department of Internal Affairs, Ministry of Justice, New Zealand Police, State Services Commission, The Treasury.
91. Officials engaged with stakeholders from a range of non-government and private sector organisations and the public through workshops, online feedback form, and discussion groups in Auckland, Wellington and Christchurch. Over 200 participants joined the workshops, representing multi-national organisations (Google, Microsoft, IBM), telecommunications (Vodafone, Spark, 2 Degrees, Kordia), energy companies (Mercury, Vector, Genesis), banks, insurance companies, cyber security and IT providers, universities and education providers, and NGOs.

Financial Implications

92. 9(2)(f)(iv) [REDACTED]

93. It is expected that, 9(2)(f)(iv) [REDACTED], further initiatives to support the Strategy will be proposed for 20/21 and outyears.

Legislative Implications

94. There are no direct legislative implications arising from this paper. Some of the work signalled in the Strategy may require legislative amendments. Cabinet approval will be sought in each case.

Impact Analysis

95. There are no regulatory implications.

Human Rights

96. The Strategy explicitly acknowledges the importance of protecting human rights and privacy online. The actions to deliver the Strategy and work programme will be designed to be consistent with the New Zealand Bill of Rights Act 1990, Human Rights Act 1993, and Privacy Act 1993.

Publicity

97. The Strategy is intended for public release. A communications plan will be developed to support the release of the Strategy and any announcements on the priority actions.

Proactive Release

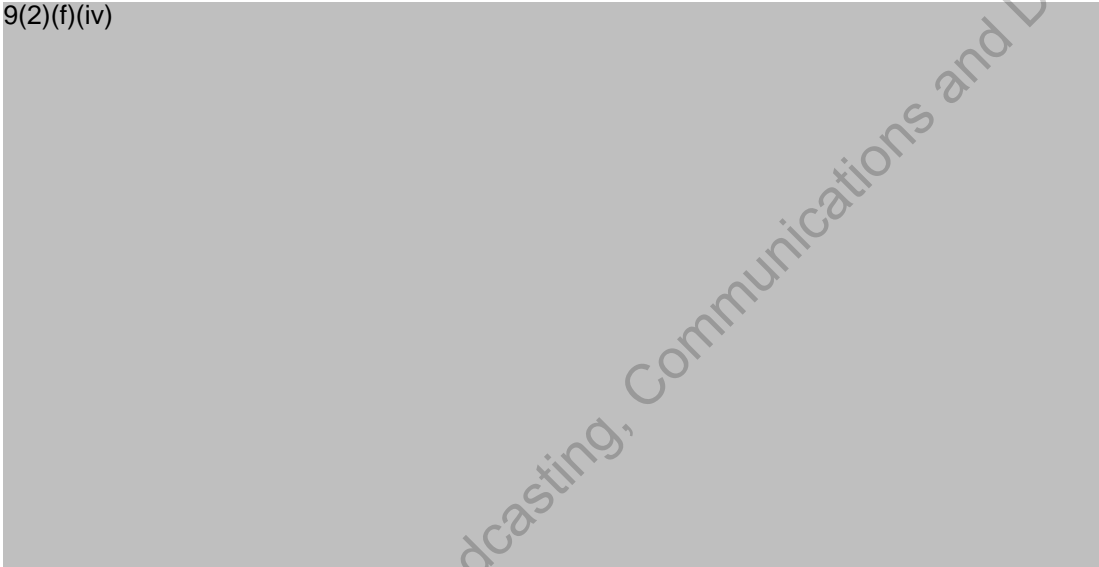
98. I propose to proactively release this Cabinet paper, with appropriate redactions, on DPMC's website.

Recommendations

99. The Minister for Broadcasting, Communications and Digital Media recommends that the Committee:
1. **note** that on 2 April 2018, Cabinet agreed that it was timely to undertake a comprehensive refresh of New Zealand's cyber security settings to ensure that the government is investing the right resources in the right way across government to respond to growing cyber security threats [CAB-18-MIN-0127];
 2. **note** that the Chair of the Cabinet External Relations and Security Committee subsequently agreed to extend the report back on the Strategy refresh from July to October to accommodate a more collaborative engagement approach to the refresh [ERS-18-MIN-0010];
 3. **note** that the 2015 Cyber Security Strategy, Action Plan and National Plan to Address Cybercrime have provided an over-arching framework for cross-government work under four goals (cyber resilience, cyber capability, addressing cybercrime, and international cooperation), and that good progress has been made;
 4. **note** that work will continue to deliver actions outlined in the existing Action Plan, including seeking Cabinet agreement to accede to the Council of Europe Convention on Cybercrime;
 5. **note** that New Zealand's cyber security policy settings must adapt to take advantage of the opportunities offered by digital technologies and in response to the evolving threat;

6. **agree** to the proposed cyber security Strategy framework, with a vision of “New Zealand is confident and secure in the digital world”, underpinned by four values and five principles and with five priorities for action;
7. **agree** to the public release of the attached document as *New Zealand’s Cyber Security Strategy 2018*;
8. **authorise** the Minister for Broadcasting, Communications and Digital Media to approve any necessary minor or technical amendments to the wording of *New Zealand’s Cyber Security Strategy 2018* before publication;

9. 9(2)(f)(iv)



10. **agree** that the Minister for Broadcasting, Communications and Digital Media will report back to Cabinet in 2019 with a work programme to deliver the strategy, including a range of further actions to advance each of the five priorities in the Strategy;

11. **agree** that relevant agencies implement the refreshed Strategy by:

- a) establishing a government Cyber Security Strategy Co-ordination Committee 9(2)(f)(iv) ;
- b) applying the new guiding principles during the planning, conduct, and assessment of projects and initiatives to give effect to the Strategy;
- c) working more with other organisations, including those outside ICT and cyber security, and participating in events to get broader input and engagement with people, businesses, and community organisations;

d) 9(2)(f)(iv)



12. **direct** the new Cyber Security Strategy Co-ordination Committee to commission agencies to develop ideas for creating:

a) 9(2)(f)(iv)



BUDGET SENSITIVE

- b) 9(2)(f)(iv) [REDACTED]
- c) a new appropriation for cyber security system initiatives to give effect to the refreshed Strategy;
13. **direct** the new Cyber Security Strategy Co-ordination Committee to report back to Cabinet at the same time as the annual work programme on the feasibility, desirability and viability of the ideas in recommendation 12 and, if the assessment is favourable, proposals for how to implement the ideas.
14. **note** that I will be seeking funding for the implementation of *New Zealand's Cyber Security Strategy 2018* in a Budget 2019 initiative 9(2)(g)(i) [REDACTED];
15. **note** that departments are coordinating a number of Budget 2019 initiatives related to cyber security, across Votes, as noted in paragraph 65;
16. **note** that the launch of *New Zealand's Cyber Security Strategy 2018* will need to be coordinated with Budget 2019 decisions and announcements;
17. **agree** that the Minister for Broadcasting, Communications and Digital Media will report back to Cabinet in the first half of 2019 with a proposed work programme to support the five priorities in *New Zealand's Cyber Security Strategy 2018*.

Authorised for lodgement

Hon Kris Faafoi

Minister of Broadcasting, Communications and Digital Media

APPENDIX A: summary of ways of working together to implement the refreshed Strategy


In addition to the below, agencies will also jointly develop and implement new practices to improve day-to-day collective action, strengths-based activity, and tackle shared problems. While the items below are written with government in mind, our aim is to encourage our private and NGO sector partners to adopt similar practices and contribute to implementing the Strategy.

Description	Desired outcomes	Challenges addressed	Key risks	Resourcing and timing
<p>Cyber Security Strategy Co-ordination Committee ^{9(2)(f)(iv)}</p> <p>This Committee (which could be a sub-committee of the Security and Intelligence Board) would include senior officials from agencies with cyber security functions, and would be responsible for governing the delivery of the Strategy, including approving the work programme, monitoring progress, and improving interagency cooperation. The Committee would focus on joint agency projects, and be informed about agency-specific projects (ie. it is not intended to make decisions about agencies' business-as-usual work or projects).</p> <p>^{9(2)(f)(iv)}</p>	<p>Collective leadership and prioritisation of the work programme to deliver the Strategy, including determining the optimal allocation of resources and funding to deliver on Strategy initiatives.</p>	<p>Addresses: adopting a system approach; and applying system governance and leadership challenges.</p> <p>The Committee would bridge the gap between individual agency endeavour and shared responsibility for implementing the Strategy through collective decision-making about the work programme, and coordination of resources and the institutional arrangements to deliver it.</p> <p>^{9(2)(f)(iv)}</p>	<p>Increasing the number of decision-makers can reduce responsiveness; this can be mitigated through the scheduling of meetings (including ad hoc meetings), ensuring the schedule is aligned with budget and planning cycles; and tight and independent chairing.</p> <p>Increased compliance burden for officials for papers taking time away from core work; design the systems and reporting requirements with users in mind to make compliance straightforward and minimise disruption.</p> <p>Some members not having the appropriate clearance to receive necessary information to; structure the meeting so that these matters can be dealt with using a different quorum.</p>	<p>No additional funding or resourcing is required for the Committee.</p> <p>Propose implementing this Committee before 31 January 2019 so that it can be in place in time for directing and endorsing the work programme and liaison about budget bids and allocation of resources for 2019/2020.</p> <p>^{9(2)(f)(iv)}</p>

~~BUDGET SENSITIVE~~

Description	Desired outcomes	Challenges addressed	Key risks	Resourcing and timing
<p>Apply new principles to Strategy initiatives</p> <p>Agencies will apply the new principles (para 23) to the planning, conduct, and assessment of Strategy initiatives.</p> <p>Agencies have the option of apply these principles to their other cyber security work.</p> <p>Government will encourage the private and NGO sectors to use the principles as part of their contributions to delivering the Strategy.</p>	<p>People have a common understanding about what to expect from each other, and can hold each other to account constructively when this does not happen.</p>	<p>Addresses: improving reach and quality, and adopting a system approach challenges.</p> <p>The new principles are a practical way of giving effect to the values that underpin the Strategy, and get more effective results. Officials developed the new principles using what participants at the public workshops thought was important to enable everyone to work together effectively.</p> <p>Applying the principles to guide <u>how</u> we work ensures that we are using the right mindsets to plan and deliver Strategy initiatives, and is a 'good practice' response to situations where a wide range of interests can result in complication.</p>	<p>The way the principles apply will vary according to the context of the Strategy initiative; to manage expectations the initiative will need to describe how principles will apply for that work.</p> <p>Some Strategy initiatives may take longer because engagement with a wider range of stakeholders can take more time; if, however, the result is feasible and viable, and scalable, then this is likely to reduce rework later.</p>	<p>No additional funding or resourcing is required.</p> <p>It is common practice for project teams to consider engagement timeframes and expertise needed to deliver a project, and some agencies may need to draw on expertise from others to meet those needs.</p>
<p>Connect and collaborate with other organisations</p> <p>Agencies will work more with organisations beyond government and the cyber security community, and participate at their events to get broader input and engagement with people, businesses, and community organisations.</p>	<p>More people across a wider range of sectors are aware of cyber security, what they need to do, and the career and investment opportunities it presents. Government is better informed about the needs of New Zealanders and business, and can (re)design its services and policies with this in mind.</p>	<p>Addresses: improving reach and quality, and adopting a system approach challenges.</p> <p>Government needs to maximise the value of its contribution and connect with a wider range of people. Working in with others is one of the ways to achieve this, and lend support to others' work.</p>	<p>Increased demand on government exceeds available resources; need to factor this into medium-long term planning, and work with private sector and NGO partners to ensure they can support their customers.</p> <p>Expectation that government will endorse particular vendors or institutions; ensure clear communications about role.</p>	<p>While agencies already meet with and connect with those outside government; additional funding is likely to be required where this approach is applied as part of specific Strategy initiatives.</p>

9(2)(f)(iv)



Proactively released by the Minister of Broadcasting, Communications and Digital Media

APPENDIX B: Summary of ideas for further analysis and development to improve working across public, private, and NGO sectors

These ideas are listed in paragraph 82 as ideas for further analysis and development with public, private, and NGO sectors to see if they could deliver better results and a more joined-up approach to achieving the refreshed Strategy.

Description	Desired outcomes	Challenges addressed	Key risks	Resourcing and timing
9(2)(f)(iv)				

~~BUDGET SENSITIVE~~

Description	Desired outcomes	Challenges addressed	Key risks	Resourcing and timing
9(2)(f)(iv)				
<p>Create a new appropriation for cyber security system</p> <p>This appropriation would fund joint agency projects on the Strategy’s work programme only. It is not intended to amalgamate all the appropriations together for cyber security work.</p> <p>The work programme</p>	<p>Important and system focused work is being prioritised, appropriately resourced, and delivered.</p> <p>Agencies are proactively using joint-agency or co-design projects to</p>	<p>Addresses: adopting a system approach; and applying system governance and leadership challenges.</p> <p>Establishing an appropriation from which agencies can be funded for joint agency and co-design projects creates an incentive to tackle shared problems, and innovate. It also requires agencies to take shared responsibility, and be</p>	<p>System-wide appropriations with joint responsibilities is an emerging practice. Ensuring the appropriate accountability for funding is a risk; one Chief Executive would be the appropriation administrator and would make allocations from it only in accordance with decisions made collectively by the Chief Executives of the departments represented on the Co-ordination</p>	<p>If the creation of a new appropriation is approved, then the work programme development process will identify projects, and necessary reprioritisation of funding, and budget bids for this appropriation.</p>

~~BUDGET SENSITIVE~~

Description	Desired outcomes	Challenges addressed	Key risks	Resourcing and timing
<p>development process will identify projects, and necessary reprioritisation of funding, and budget bids for this appropriation.</p> <p>It could be made up of club-funding, reprioritised funds, or new funding depending on what is on the work programme.</p>	<p>collaborate and tackle shared problems.</p>	<p>collectively accountable for work that will deliver the Strategy.</p> <p>9(2)(f)(iv)</p>	<p>Committee.</p> <p>Chief Executives having insufficient information to make funding decisions; to mitigate, any decisions about funding joint agency projects, funding would be approved by the Chief Executives on the Security and Intelligence Board after they had been endorsed by the Co-ordination Committee.</p>	