



Proactive Release

The following documents have been proactively released by the Department of the Prime Minister and Cabinet (DPMC), on behalf of Hon Ginny Andersen, Minister for the Digital Economy and Communications.

[Proactive Release] Cyber Security Advisory Committee (CSAC) documents

The following documents have been included in this release:

Title of paper: New Zealand Cabinet Cyber Security Advisory Committee Report back on Workstreams 1/2/3

Title of paper: Proposal on Cyber Security Single Front Door

Title of paper: Briefing: Reflections on CSAC Advice and Next Steps

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 codes:

- section 9(2)(ba)(i), to protect the supply of similar information in the future
- section 9(2)(g)(ii), to prevent improper pressure or harassment
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials
- section 18(d), that the information requested is or will soon be publicly available



Coversheet

Briefing: Reflections on CSAC Advice and Next Steps

Date:	8 September 2022	Report No:	DPMC-2022/23-7
		Security Level:	[IN CONFIDENCE]
		Priority level:	[LOW]

	Action sought	Deadline
Hon Andrew Little Minister Responsible for the GCSB	Indicate any further directions on CSAC recommendations.	-
Hon Dr David Clark Minister for the Digital Economy and Communications		

Name	Position	Telephone	1 st Contact
Halia Haddad	Manager, National Cyber Policy Office	s9(2)(g)(ii)	✓
s9(2)(g)(ii)	Principal Policy Advisor, NCPO	s9(2)(g)(ii)	

Departments/agencies consulted on Briefing
CERT NZ, DIA, MBIE, NZ Police & GCSB have been consulted on this brief.

Minister's Office

Status:

Signed

Withdrawn

Comment for agency

Attachments: Yes

Briefing

Reflections on CSAC Advice and Next Steps

To: Hon Andrew Little
Minister Responsible for the GCSB

Hon Dr David Clark
Minister for the Digital Economy and Communications

Date	8/09/2022	Security Level	[IN CONFIDENCE]
------	-----------	----------------	-----------------

Purpose

1. This paper provides an overview of the full set of recommendations of the Cyber Security Advisory Committee (CSAC), provides officials' views on these, and seeks Ministers' direction on the CSAC's recommendations in the context of current work programmes. This briefing is largely focused on providing a reflection on the recommendations in CSAC papers that have not been covered in advice to Ministers elsewhere.
2. It also seeks confirmation that the CSAC's term will end on 15 October, in line with its Terms of Reference.

Executive Summary


3. The CSAC's reports have set out a range of initiatives that broadly focus on improving the cyber security services that government provides to business, and placing obligations on firms and organisations that provide internet infrastructure.
4. The initiatives proposed by the CSAC through these reports are largely in alignment with those developed by officials during the development of the cyber security resilience Cabinet papers, including some already underway.
5. The CSAC has provided valuable insights in relation to the Terms of Reference they were set, which are being incorporated into the development of cyber security policy and service design of cyber security services to support businesses. Their insights are helping inform the current cyber security resilience workstreams, in particular the single front door workstream.
6. It is important to highlight that the CSAC's Terms of Reference were narrower than the objectives of the Cabinet papers, and also that the CSAC responses and recommendations reflect a particular focus on medium to large businesses – which is an important group to consider, but is just one part of the audience cyber policy and strategy needs to address.
7. The CSAC's term is due to conclude on 15 October, following submission of their final report on the single front door. There is scope to further extend their term, however officials see risks in the ongoing development of parallel advice on projects that are in implementation phase. Officials recommend formal disestablishment of the CSAC to ensure expedient implementation, s9(2)(f)(iv)

Recommendations


We recommend you:

1. **note** that the CSAC has provided several reports to Ministers on the results of their workstreams, findings from their sector engagement, and will be providing further advice on their current work on the single front door;
2. **note** that the CSAC's reports include a range of interconnected recommendations, which are aligned to the overall cyber security work programme agreed by Cabinet and work underway through the Cyber Security Strategy;
3. **note** that the CSAC's recommendation to investigate the cyber insurance market is the only recommendation that is not, in part, covered by the current work programme;
4. **indicate** in Annex A any areas among the CSAC recommendations where you are seeking a greater or lesser emphasis in the current cyber security work programme; and
5. **agree** that the CSAC should conclude its term on 15 October, and
6. **note** that officials propose to provide letters for your signature for each CSAC member, prior to formal disestablishment.

YES / NO


Tony Lynch
 Deputy Chief Executive,
 National Security Group
 13/09/22

Hon Dr David Clark
 Minister for the Digital Economy and
 Communications


Lisa Fong
 Deputy Director-General, National
 Cyber Security Centre, GCSB
 13/9/22

Hon Andrew Little
 Minister Responsible for the GCSB

Background

8. Since its establishment on 15 December 2021, the CSAC has provided advice on options to strengthen New Zealand's cyber security and resilience. The CSAC was originally appointed for a six-month term, and had its term extended until 15 October 2022. The CSAC has sought to provide Ministers with insights from an industry perspective on ongoing work to lift cyber security and resilience.
9. The CSAC's Terms of Reference tasked them with providing advice on the four core workstreams listed below:
 - Lifting the cyber security capability of the private sector and its resilience when under threat;
 - Providing recommendations around a scalable cyber security framework for New Zealand companies and organisations;
 - Providing insight and recommendations around the customer orientation of government agencies working on cyber security matters; and
 - The design and establishment of a permanent public-private collaboration forum on cyber security with the aim of better connecting and harnessing the New Zealand cyber security ecosystem.
10. Work since their extension has focused on considerations for the design of a 'single front door' for reporting cyber incidents.
11. The CSAC has provided the following reports to Ministers:
 - A report back on Workstreams 1-3, provided on 24 March 2022;
 - A report back on Workstream 4 provided on 22 May 2022;
 - A "supplementary issues" paper, provided on 28 June 2022; and
 - Feedback on the 'Strengthening resilience in the wider economy' Cabinet paper (June Cabinet Paper), provided on 26 July 2022.
12. Much of the CSAC's advice from its first paper covering Workstreams 1-3 was integrated into the June Cabinet paper on building resilience in the wider economy. s9(2)(f)(iv)
[REDACTED]
13. The CSAC's advice from its supplementary issues paper covered a range of issues that built on the recommendations of their earlier reports.
14. This briefing is largely focused on providing a response to the recommendations in the CSAC reports that have not been covered elsewhere in advice to Ministers (particularly via Cabinet papers s9(2)(f)(iv)
[REDACTED]
15. Further advice is being prepared by the CSAC to inform the design of a single front door. This work is progressing in parallel to officials' development of advice to Ministers on implementation of the single front door. In preparing advice and recommendations for Ministers, officials are drawing on aspects of the CSAC's advice as it is being developed.
16. Once the CSAC submits their final report on the single front door, this will conclude their work. The CSAC's term is due to expire on 15 October.

The CSAC has recommended a range of business-focussed actions

17. The CSAC's Terms of Reference set out that the committee would provide independent expert advice to the Government on options to improve the cyber security and resilience of the private sector and broader society.
18. In forming its advice, the CSAC members led interviews of 20 companies that had recently experienced cyber incidents and drew on the broad ranging experience of its members. The survey provided useful qualitative insights on the experiences of small, medium and large organisations, cyber security providers and Māori enterprises, but did not seek to be a survey of the full range of cyber security needs across the wider economy.
19. Overall, the recommendations predominantly relate to improving the cyber security services that government provides to business, and placing obligations on firms and organisations that provide internet infrastructure.
20. The full set of recommendations from all papers are summarised below:

Workstreams 1-3

- I. The creation of a 'single front door,' providing companies and organisations a single agency for reporting attacks, obtaining meaningful advice and accessing practical help in recovery.
- II. Recognition and assessment of impact and loss across all 'capitals', including cultural capital, and a dedicated workstream to address Māori data governance and data sovereignty.
- III. The implementation of minimum cyber risk management guidelines for companies, expressed as a simplified form of the widely-understood NIST Cybersecurity Framework.
- IV. The introduction of mandatory reporting of cyber incidents and ransom payments for those organisations and sectors upon which society relies.
- V. Sustained oversight of and investment into building cyber capability and capacity in the labour market, through work visa enablement and funding of cyber security education.
- VI. A strengthened oversight regime for Internet Service Providers (ISPs) and Managed Service Providers (MSPs), with regard to their capability and their controls of cyber security risk, and subjecting them to mandatory cyber incident reporting.

s9(2)(f)(iv)

Supplementary issues paper

- IX. New Zealand commits to achieving cyber defence parity with our Five Eyes partners as a matter of national importance and international citizenship.
- X. NCSC works with industry professionals to develop templates and playbooks for the most common incidents. This would likely include DDoS, ransomware, data theft and extortion.

- XI. An investment plan, supported by a transformational strategy for cyber resilience developed by the single front door, must be elaborated, tabled and provided for.
- XII. A strengthened focus upon the building blocks of cyber capacity across organisations and government agencies (this recommendation discussed cyber hygiene, social engineering and emerging technologies).
- XIII. review of all relevant legislation and policy frameworks with implications for cyber security, particularly for the oversight of sectors of national significance and IT managed service and security providers.

s9(2)(f)(iv)

- 22. The CSAC's advice has been iterative, and recommendations of the first four workstreams have been refined over the CSAC's term.
- 23. The 13 recommendations across the CSAC's reports can be grouped into six main themes, which are discussed below.
- 24. A more detailed assessment of the individual recommendations from the CSAC's reports are attached in Annex A.
- 25. Ministers are asked to indicate, within the Annex, any areas in the CSAC's recommendations where you are seeking a greater or lesser emphasis in the current cyber security work programme. It is important to note that any additional tasking is likely to require the de-prioritisation of current work.

Theme 1: Creating a 'single front door' for reporting cyber incidents

- 26. The CSAC's recommendations on the single front door generally aligned with standing assumptions that businesses and individuals have difficulty identifying where to go to seek help and advice during a cyber incident.
- 27. Significant structural reform of the institutions supporting businesses to improve the delivery and provision of cyber security support is the CSAC's most substantial and detailed recommendation. The CSAC sees this as a matter of urgency.
- 28. As directed by Ministers, the committee is using the remainder of its term to continue to develop its single front door model. Officials will consider any new recommendations or advice from the CSAC during the development of a new single front door, as outlined in recent briefings to you.

Theme 2: Applying a te ao Māori perspective to cyber security

- 29. The CSAC identified the absence of specific consideration of the government's obligations as a Treaty partner in cyber security policy, and the need to consider a te ao Māori perspective in service provision and cyber security policy more generally. This is a similar issue that has been identified in wider national security policy, and which is being addressed in ongoing work on a new National Security Strategy. The government's obligations as a Treaty partner will also be a key consideration when the 2019 Cyber Security Strategy is refreshed.
- 30. A number of the issues touched on in the CSAC's recommendations regarding Treaty obligations are related to issues much broader than cyber security, such as Māori data governance. Stats NZ is currently co-designing a Māori data governance model in partnership with the Data Iwi Leaders Group. The Department of Internal Affairs is currently undertaking a co-design process to support decision-making regarding Māori data in relation to the cloud.

31. Integrating te ao Māori and Treaty obligations into future cyber security policy will be a feature of ongoing work programmes, including the current single front door and critical infrastructure resilience workstreams. Officials are developing a National Cyber Security Risk Assessment, which will also assist in identifying what data sets and information infrastructures are important to Māori; and will assist government to meet its obligations as a Treaty partner.

Theme 3: Setting standards and applying rules

32. The CSAC proposes a range of initiatives largely focused on providing more user-friendly advice and guidance for businesses, and regulating service providers and internet infrastructure. These recommendations are being picked up through the single front door and critical infrastructure workstreams – which will include improving guidance and advice as a necessary input into providing better support for individuals and organisations.

33. The CSAC's final recommendations on critical infrastructure are for government to undertake consultation with business with a view to introducing mandatory standards and incident reporting for Nationally Significant Organisations and some critical infrastructure. s18(d)

34. One recommendation the CSAC has made that is not supported by officials is a review of the cyber insurance market. While it is not contested that some firms are unable to find insurance products that meet their needs, the issues raised by CSAC are not specific to the New Zealand market. Globally, the cyber insurance market has been changing in the face of the changing impacts of cybercrime, particularly ransomware, and the incidence of state-sponsored actors causing disruption to civilian networks and infrastructure. The cyber insurance market is dealing with considerable uncertainty in the nature and extent of risks, and is adjusting coverage in response. Officials' view is that the review the CSAC has suggested is highly unlikely to be able to resolve these issues of uncertainty around risk; nor would it influence insurance firms to provide particular types of coverage.

Theme 4: Addressing workforce pressures

35. The CSAC identified the same issues with the cyber security workforce that have been identified through agency work and industry feedback. The CSAC's prescription for action in this area, which includes adjusting immigration settings, is in line with that proposed through other industry engagements on workforce issues both within and outside the digital sector.

36. Making consequential change to the supply of skills for cyber security would require significant investment or reform. The skills workstream of the Digital Technologies Industry Transformation Plan (DTITP) remains the key vehicle for the delivery of initiatives to grow the cyber security workforce, and cyber security is being explicitly included in a number of actions under the skills workstream of the DTITP.

37. Officials will also continue other activities, such as current research underway to better understand the current workforce and thereby better identify opportunities for potential government intervention and collaboration with industry, and the Cyber Skills Aotearoa project which is due to be launched on 27 October.

s9(2)(f)(iv)

s9(2)(f)(iv)

Theme 6: Increased government spending on cyber security

40. The CSAC notes in its first report that a significant lift in capability will require significant investment. Throughout its reports, the CSAC has a clear view that further resourcing will be required for implementation of their recommendations. Most significantly, the references to retaining 'parity' with Five Eyes partners imply that considerably greater investment overall is required to raise domestic cyber security capability.
41. Furthermore, across many of the recommendations, there is an implicit proposal to establish an entity similar to Australia's ACSC – which is central to achieving the CSAC's vision.
42. In general, 'parity' would require an increase in expenditure in line with the higher spending on national security and defence by close partners, notwithstanding that international comparisons are difficult in this area.

Work continues on areas beyond the CSAC's Terms of Reference

43. The CSAC's reports have provided significant value and insight, but their focus on delivering better services to business does not present a comprehensive assessment of New Zealand's response to cyber security. In line with their Terms of Reference their recommendations do not cover in-depth:
 - Individual victims of cybercrime or home users seeking cyber security guidance; and
 - Protection of national infrastructure from advanced threats.
44. Work on better supporting the individual victims of cybercrime and providing advice to home users is an area that will be considered as part of officials' work on developing a single front door. While this was not a focus for the CSAC, from a national resilience and wellbeing perspective, support for individuals is an important priority.
45. It is also the case that better cyber literacy across the economy and society has a flow on effect to business owners and employees. As acknowledged in the CSAC reports, there are a range of workstreams touching on reporting of cybercrime and online harms, including the response to the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (RCOI).
46. International cyber security cooperation, responding to the perpetrators of cybercrime, and addressing online harms fell outside the CSAC's Terms of Reference. These issues will be considered when looking to implement the CSAC's recommendations and the Cabinet agreed priorities for cyber security, as well as recommendations from the RCOI.

Next steps for the CSAC

47. The CSAC is currently developing further advice to Ministers on its consideration of what a single front door needs to achieve and how it should be implemented. They are anticipating delivering this report in early October. The CSAC's extended term is due to conclude on 15 October.
48. Officials recommend that the group be disestablished at this point as per their extended Terms of Reference. This will allow officials to focus on providing advice on implementation of the key initiatives being progressed.

s9(2)(f)(iv)

- 49. Should Ministers wish to see the CSAC term extended, there is a risk that the CSAC and officials developing parallel advice on agreed policy initiatives will complicate and significantly slow down agencies' advice on implementation of the initiatives.
- 50. Any extension would also require redirection of agency resource from implementation of the agreed initiatives in order to progress an APH extension, and to provide ongoing support to the CSAC.
- 51. We also understand at least one CSAC member will need to step down from the committee from 15 October, to focus on other commitments.
- 52. If Ministers agree, officials will draft thank you letters for Ministers to sign, for provision to each of the CSAC members on submission of their final report. The letters will reference potential continued engagement by interested and available CSAC members on an ad hoc basis with Ministers and officials in relation to the ongoing implementation of the single front door. However, it should be noted (and will need to be outlined in the letters) that any such engagement will be on an informal and unpaid basis, since without a formal APH extension of the CSAC's term there is no basis for continuing to pay the members of the committee for their time (nor do we currently have funding available for an extension of their term).

s9(2)(f)(iv)

Next steps

- 54. As noted above, it is expected the CSAC's final report will be provided to Ministers in early October. Officials are engaging with the CSAC on their advice, and considering how and whether to incorporate the CSAC's recommendations into advice to Ministers on how best to resolve the issues related to cyber incident reporting and response.
- 55. Officials are also focussed on progressing the critical infrastructure workstream.
- 56. These two areas of work represent a full cyber security policy programme for the foreseeable future. Further updates on these workstreams will be provided to Ministers later this month.

Attachments:	Title	Security classification
Annex A:	CSAC Recommendations	IN CONFIDENCE

Annex A: CSAC Recommendations

The table below sets out the core individual recommendations of the CSAC's reports, and outlines the related ongoing work by agencies that is relevant to them. Ministers are asked to indicate whether they require a lesser or greater focus within current cyber security work programmes.

CSAC RECOMMENDATION	PROBLEM ADDRESSED	CURRENT STATUS	AGREED ACTIONS/ RECOMMENDATION FOR FOLLOW-UP	MINISTERS' DIRECTION
Creating a 'single front door' for reporting cyber incidents				
The creation of a 'single front door,' providing companies and organisations a single agency for reporting attacks, obtaining meaningful advice and accessing practical help in recovery.	Advice is being developed by the CSAC and officials in parallel on this. Officials will provide further briefings on the design of a single front door, which will capture officials' views on the CSAC recommendations, ahead of the report back to Cabinet in November.			
Applying a te ao Māori perspective to cyber security				
Recognition and assessment of impact and loss across all 'capitals', including cultural capital, and a dedicated workstream to address Māori data governance and data sovereignty.	A te ao Māori perspective on cyber security has not been applied in any systemic way to cyber security policy. There is, consequently, not a good understanding of the cyber risks that apply to Māori data or Māori organisations, including how they differ from other data and organisations.	DPMC, in conjunction with other agencies, is developing a national cyber security risk assessment. This will rank risks according to their potential impact on New Zealand and the urgency with which they need to be addressed. Included in the assessment will be the impact of cyber security	Officials to continue with development of risk assessment, including exploring how best to engage with Māori so that important data sets and information infrastructures important to Māori are identified. s9(2)(f)(iv)	

<p>Establishment of a workstream focusing specifically on New Zealand data governance with a focus upon Māori data governance, Te Tiriti o Waitangi/The Treaty of Waitangi, and meeting our obligations under the UN Declaration on the Rights of Indigenous People. CSAC understands there are several government agencies working across these issues, however unified oversight and suitable resourcing is required, with urgency.</p>		<p>incidents on social and cultural capital.</p>	<p>s9(2)(f)(iv)</p> <p>Government efforts to address Māori data governance issue will continue as part of Stats NZ and DIA work programmes related to their Mana Ōrite agreements.</p>	
<p>Setting standards and applying rules</p>				
<p>The implementation of minimum cyber risk management guidelines for companies, expressed as a simplified form of the widely-understood NIST Cybersecurity Framework.</p>	<p>Organisations across New Zealand are not implementing basic cyber security measures. More than 90 per cent of the cyber security incidents CERT NZ responds to could be prevented if people and organisations (public and private) chose to implement basic cyber security measures. Research found SMEs are often hindered by a lack of dedicated IT staff or support, not knowing where to begin or failing to understand weaknesses in security practices, underestimating the risk and consequences of a cyber incident, and a gap in planning for and responding to incidents.</p> <p>Information from government on managing cyber security risks is not</p>	<p>The NCSC is has developed a NIST-based cyber security framework for the state-sector. This framework will likely form the basis for broader guidelines for the wider economy s9(2)(f)(iv)</p>	<p>NCSC to continue development and implementation of the NIST-based cyber security framework and mandatory standards with a view to final product being appropriate for supporting organisations outside the public sector.</p>	
<p>A strengthened focus upon the building blocks of cyber capacity</p>				

<p>across organisations and government agencies. The CERT Critical Controls, supported by effective, targeted education and outreach would form part of any transformative strategy for improvement, along with consideration for the creation of cyber risk controls for emerging technology and the risk vectors associated with this.</p>	<p>well coordinated across agencies and can be difficult for organisation to understand what is relevant to their circumstance.</p>		
<p>A review of all relevant legislation and policy frameworks with implications for cyber security be undertaken, particularly for the oversight of sectors of national significance and IT managed service and security providers. This should be supported by sufficient oversight, resources and support to guide industry and provide government assurance of compliance once implemented.</p>			
<p>A strengthened oversight regime for Internet Service Providers (ISPs) and Managed Service Providers (MSPs), with regard to their capability and their controls of cyber security risk, and subjecting them to mandatory cyber incident reporting.</p>	<p>ISPs and MSPs are critical infrastructure for the digital economy. Ensuring resilience within these classes of organisations underpins the resilience of New Zealand's broader online environment.</p>	<p>s9(2)(f)(iv)</p>	
<p>The introduction of mandatory reporting of cyber incidents and ransom payments for those</p>	<p>s18(d)</p>		

<p>organisations and sectors upon which society relies.</p>	<p>The international cyber insurance market is currently in flux. Some insurers are reducing coverage and increasing prices. Most recently Lloyd's of London announced it will stop covering losses from certain nation-state cyber attacks and those that happen during wars. Some consumers are having difficulty acquiring suitable and affordable coverage. There is a lack of reliable data on the impact of cyber incidents alongside a rapidly evolving threat landscape. This is a global issue and the experiences of domestic firms appear to be similar to those offshore. It is likely that most organisations have comparatively limited knowledge of cyber security risks. This may be a contributing factor the cyber insurance market being less developed than some other markets.</p>	<p>Government has been observing developments in the cyber security insurance market but has not identified any obvious market failures related to the insurance market itself. There is considerable uncertainty that insurers face globally in pricing risk in the face of an extremely dynamic risk landscape. The changing risk profile means that this market may not stabilise in the near future. A review of the cyber insurance market, given offshore experience and the uncertainty around risk, means that a review by regulators is unlikely to identify solutions to problems this market faces.</p>	<p>The CSAC report will be referred to insurance market regulators, including to the Reserve Bank, for their consideration. Cyber security officials will continue to engage with the insurance industry as part of ongoing private sector engagement. There is an opportunity for the insurance sector and cyber security officials to collaborate to provide information about what types of insurance are available and what good practice risk management looks like.</p>	
<p>Addressing workforce pressures</p>				
<p>Sustained oversight of and investment into building cyber capability and capacity in the labour market, through work visa</p>	<p>Cyber security skill shortages are an enduring problem both domestically and internationally.</p>	<p>The primary initiative to support workforce development will be through the Digital Technologies Industry Transformation Plan (DTITP). In the absence of any</p>	<p>Officials to continue to develop workforce initiatives that can be undertaken with industry (such as</p>	

<p>enablement and funding of cyber security education.</p> <p>Access to skilled workers is a foundational enabler and will make or break efforts to lift cyber security at a system level. We urge Ministers to front-foot talent constraints by engaging with industry to effect swift changes to immigration rules allowing the most urgent gaps to be filled with skilled talent, while activating a strategic plan for capability and capacity development across educators, industry and government agencies.</p>	<p>The problem is reflective of an overall skills shortage affecting the digital economy and skills shortages throughout the wider economy.</p>	<p>intensive government investment in the cyber security industry specifically, the DTTP is the key means for delivering any cyber-specific initiatives in this area, noting there is limited additional resourcing for the DTTP skills workstream. Potential areas for alignment within the DTTP's skills workstream include improving the visibility, access to and coordination of pathways to cyber careers for youth; workforce upskilling/reskilling and career development; enhancing diversity in the sector (targeted at, for example, women and Māori).</p>	<p>the Cyber Skills Aotearoa project), where limited funding is available.</p>
--	---	---	--

s9(2)(f)(iv)

Increased government spending on cyber security

<p>New Zealand commits to achieving cyber defence parity with our Five Eyes partners as a matter of national importance and international citizenship. This will require effort from government agencies to develop a shared strategy for cyber defence.</p>	<p>CSAC notes that the resources committed by our Five Eyes partners to cyber security are proportionally greater than those committed by New Zealand. The investment that these countries are making in cyber security appears to be accelerating relative to New</p>	<p>s9(2)(f)(iv)</p>	
--	--	---------------------	--

<p>An investment plan, supported by a transformational strategy for cyber resilience developed by the single front door, must be elaborated, tabled and provided for. New Zealand's Five Eyes partners have all announced significant new funding for cyber defence and capability uplift over the last 18 months. Through stronger public-private collaboration, we can leverage our unique advantage of being a first-world country, with a small market, to potentially be a leader. New Zealand must punch at its weight or better.</p>	<p>Zealand's expenditures. Direct comparisons of expenditure are difficult as nations often re-announce previous spending and spending between cyber security, national defence and law enforcement is often blurred.</p> <p>The current 2019 Cyber Security Strategy largely sets out Government policy but does not outline clear cyber security policy objectives. Likewise it does not set out a pathway to achieve any specific end-state or goals.</p> <p>s9(2)(f)(iv)</p>	<p>s9(2)(f)(iv)</p> <p>Budget bids for 2023 are underdevelopment including those flagged in recent Cabinet papers.</p> <p>Any significant expansion of the New Zealand government's cyber security capability is likely to be subject to workforce pressures in line with other digital sectors.</p>	<p>s9(2)(f)(iv)</p>
---	--	--	---------------------