

# Department of the Prime Minister and Cabinet

## Minister of Broadcasting, Communications and Digital Media Reports in June 2018

To increase transparency and open government, the Minister for Broadcasting, Communications and Digital Media has decided to make publicly available the regular reports she receives from officials. The Minister has released the following set reports provided by the Department of the Prime Minister and Cabinet's National Cyber Policy Office.

Some parts of these documents 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 sections of the Act that would apply have been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

**Title:** National Cyber Policy Office: June Reports.

**Information withheld with relevant section(s) of the Act:**

- s 6(a) –security or defence of NZ or international relations
- s 9(2)(a) – personal information
- s 9(2)(f)(iv) –confidential advice under active consideration
- s 9(2)(g)(i) –free and frank expression of opinions



Minister for Broadcasting, Communications and Digital Media  
(Hon Clare Curran)

### BRIEFING: Advice on Singapore International Cyber Week

<b>Date:</b>	31 May 2018	<b>Tracking number:</b>	DPMC-2017/ 18-1255
<b>Security classification:</b>	Unclassified	<b>Priority:</b>	Routine
<b>Action sought:</b>	<b>Note</b> the contents of this briefing. <b>Agree</b> that the Department of the Prime Minister and Cabinet release this briefing once it has been consulted with relevant agencies, and considered by your office.		
<b>Deadline:</b>			

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
Paul Ash	Director, National Cyber Policy Office	s9(2)(a)	s9(2)(a)	✓
Heather Ward	Team Leader, National Cyber Policy Office	s9(2)(a)	s9(2)(a)	

<b>Agencies consulted</b>
N/A

- Minister's office to complete:**
- |   |                                       |
|---|---------------------------------------|
| <input type="checkbox"/> Approved             | <input type="checkbox"/> Declined     |
| <input type="checkbox"/> Noted                | <input type="checkbox"/> Needs change |
| <input type="checkbox"/> Seen                 | <input type="checkbox"/> Overtaken by |
| <input type="checkbox"/> See Minister's Notes | <input type="checkbox"/> Withdrawn    |

<b>Comments</b>

Minister for Broadcasting, Communications and Digital Media  
(Hon Clare Curran)

**BRIEFING: Proposed visit to Singapore, 18-20 September 2018**

**Purpose**

- To provide you with preliminary advice for your proposed visit to Singapore from 18-20 September 2018 to attend Singapore's International Cyber Security Week and associated events.

**Recommendations**

The Department of the Prime Minister and Cabinet recommends that you:

- Note** the contents of this brief.

Yes / No

- Agree** that the Department of the Prime Minister and Cabinet release this briefing with redactions if appropriate, once it has been consulted with relevant agencies and considered by your office.

Yes / No

  
Paul Ash  
Director, National Cyber Policy Office  
Department of the Prime Minister and  
Cabinet

Date: 1 / 6 / 2018

Hon. Clare Curran  
**Minister for Broadcasting,  
Communications and Media**

Date: ..... / ..... / .....

## Invitation to the 3<sup>rd</sup> Singapore International Cyber Week, 18-20 September 2018

1. You have received an invitation from Singapore's Minister for Communications and Information and Minister-in-charge of Cybersecurity, Mr S. Iswaran, to attend Singapore's International Cyber Week (SICW) from 18-20 September 2018 (Attachment One). s9(2)(g)(i), s9(2)(f)(iv)

### What happens during Singapore International Cyber Week?

2. This is the third Singapore International Cyber Week since 2016. Activities during the week include a major industry-led cyber security exhibition and conference (GovernmentWare), and inter-governmental discussions. The event will be opened by Singapore's Deputy Prime Minister, Mr Teo Chee Hean. It is expected to attract 7,000 representatives from government, industry and academia from over 50 countries. s6(a), s9(2)(g)(i), s9(2)(f)(iv)

3. New Zealand has participated in Singapore's International Cyber Week at an officials' level to date. The event has enabled New Zealand officials to engage with both industry, international experts and representatives from governments in the region.

### The programme for 2018 Singapore International Cyber Week

4. The theme of the 2018 Singapore International Cyber Week is "Forging a Trusted and Open Cyberspace". Singapore will emphasise the importance of cross-border partnerships and cooperation for strengthening cybersecurity as a foundation for the digital economy. Singapore has proposed the "codifying of rules and norms of behaviour, built on the technology and infrastructure that can nurture growth"<sup>1</sup>.
5. At this stage, only a preliminary programme for the event has been released. We will update you when a full programme is available.

### ASEAN Special Session for Dialogue Partners: Opportunity to engage with ICT and Cyber Security Ministers

6. Singapore will host the 3<sup>rd</sup> Association of South East Asian Nations (ASEAN) Ministerial Conference on Cybersecurity (for ASEAN ICT and cyber security Ministers). This will be accompanied by a Special Session for ASEAN Ministers and

<sup>1</sup> 2018. Singapore International Cyber Week. <https://www.sicw.sg/about-event.html>



invited Ministers and Senior Officials of ASEAN Dialogue Partners, such as New Zealand.

7. In September 2017, an official (Paul Ash, Director of the National Cyber Policy Office) represented New Zealand at this Special Session in the absence of an available Minister (given New Zealand elections). New Zealand delivered a statement outlining its principled approach to cyber space, and supporting the development of norms of responsible state behaviour online. s9(2)(g)(i), s9(2)(f)(iv)

8. This event will enable you to engage with Ministerial counterparts from the Asia Pacific region on cyber security cooperation in the region, promote norms of responsible state behaviour in cyberspace, and share best practice on ICT and cyber security issues. s6(a)

with other countries sending senior officials responsible for cybersecurity. We can expect a similar high level of involvement from a range of countries this year.

#### **Other International events during the week**

9. New Zealand is a founding member of the Global Forum on Cyber Expertise (GFCE), which will have its third annual meeting during the week. The GFCE was launched at the Global Conference on Cyberspace in The Hague in April 2015. It brings together governments, international organisations and the private sector to coordinate on international cyber security capacity building.


10. There will also be a meeting of the Global Commission on the Stability of Cyberspace, which brings together 26 prominent Commissioners representing a wide range of geographic regions as well as government, industry, technical and civil society stakeholders. The NCPO has been contacted by the GCSC Secretariat, and asked to "save the date" for the meeting. Elements of the meetings of the Commission proper may be a closed event (although the Secretariat is keen to encourage New Zealand participation). There will be opportunities to meet with a number of Commissioners. Some are well known to New Zealand (e.g. former State Department Cyber Coordinator, Chris Painter, internationally recognised expert on cyber security and Programme Director of the Centre of Strategic and International Studies in Washington, Jim Lewis – the keynote speaker at the inaugural New Zealand Cyber Security Summit in 2016 - and Elina Noor, Director, Foreign Policy and Security Studies, Institute of Strategic and International Studies, Malaysia).

11. The 6th Europol-INTERPOL Cybercrime Conference will bring together representatives from law enforcement, the private sector, academia and international organizations.


#### **Strengthening our cyber relationship with Singapore**

12. New Zealand has a constructive cyber security relationship with Singapore. This follows the inaugural cyber dialogue with Singapore in May 2017; valued attendance at the Singapore International Cyber Week events in both 2016 and 2017; the visit to Wellington by former Singaporean Minister for Information and Communication, Dr Yaacob Ibrahim, in March 2018; and positive engagement with Singaporean officials in the margins of the ASEAN Regional Forum (ARF) Intersessional Meeting on ICTs Security.

13. Your visit to Singapore to attend the Straits Digital Exchange from 4-8 June 2018 is a further opportunity to strengthen this relationship with a broader focus on digital technology. s6(a), s9(2)(g)(i), s9(2)(f)(iv)



14. s6(a), s9(2)(g)(i), s9(2)(f)(iv)



15.



**Next Steps**

16. If you decide to attend Singapore International Cyber Week, we will make contact with New Zealand's High Commission in Singapore to develop a programme for your visit. We will also prepare a letter of response to the invitation.





Minister for Broadcasting, Communications and Digital Media  
(Hon Clare Curran)

**BRIEFING: Overview of approach and engagement for the refresh of the Cyber Security Strategy and Action Plan**

Date:	8 June 2018	Tracking number:	
Security classification:	Unclassified	Priority:	Routine
Action sought:	Advice on the proposed approach to the Refresh, including engagement and availability to open the first workshop in Wellington on 26 June 2018.		
Deadline for action:	Friday, 15 June 2018		

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
Paul Ash	Director, National Cyber Policy Office	s9(2)(a)	s9(2)(a)	✓
Heather Ward	Principal Adviser and Acting Team Leader National Cyber Policy Office	s9(2)(a)	s9(2)(a)	

**Consultation**

This paper has been consulted with the following agencies: The approach to the Cyber Security Strategy refresh has been discussed and approved by the Governance Group involving DPMC, GCSB, MBIE, NZ Police, MFAT, MoJ, GCDO/DIA, and SSC.

**Minister's office to complete:**

- |   |  |
|---|--|
| <input type="checkbox"/> Approved             | <input type="checkbox"/> Declined            |
| <input type="checkbox"/> Noted                | <input type="checkbox"/> Needs change        |
| <input type="checkbox"/> Seen                 | <input type="checkbox"/> Overtaken by Events |
| <input type="checkbox"/> See Minister's Notes | <input type="checkbox"/> Withdrawn           |

**Comments**

---

Proactively Released by the Minister for Broadcasting, Communications and Digital Media



Minister for Broadcasting, Communications and Digital Media  
(Hon Clare Curran)

## BRIEFING: Overview of approach and engagement for the refresh of the Cyber Security Strategy and Action Plan

### Purpose

- To update you on the collaborative process underway to refresh the Cyber Security Strategy and Action Plan, involving a number of agencies, extensive outreach and engagement with a diverse range of stakeholders, and opportunities for your involvement

### Recommendations

The Department of the Prime Minister and Cabinet recommends that you:

- Note** the collaborative approach for the refresh of the Cyber Security Strategy and Action Plan has been designed to ensure key agencies work closely together and engage with a broad range of stakeholders;

Yes / No

- Agree** to open the Wellington workshop at the Department of Internal Affairs Service Innovation Lab, if possible, on 26 June 2018 and/or have a video of the presentation relayed to the other workshops;

Yes / No

- Note** further opportunities for Ministerial engagement in the Refresh process;

Yes../..No

- Agree** that the Department of the Prime Minister and Cabinet release this briefing in full once it has been considered by you with specific dates (but not months) redacted from the three diagrams (paras 5 and 8, and the appendix) and contact details for officials withheld.

Yes / No

Paul Ash  
Director, National Cyber Policy Office  
Department of the Prime Minister and  
Cabinet

Date: 8 / 10 / 18

Hon Clare Curran  
Minister for Broadcasting, Communications  
and Digital Media

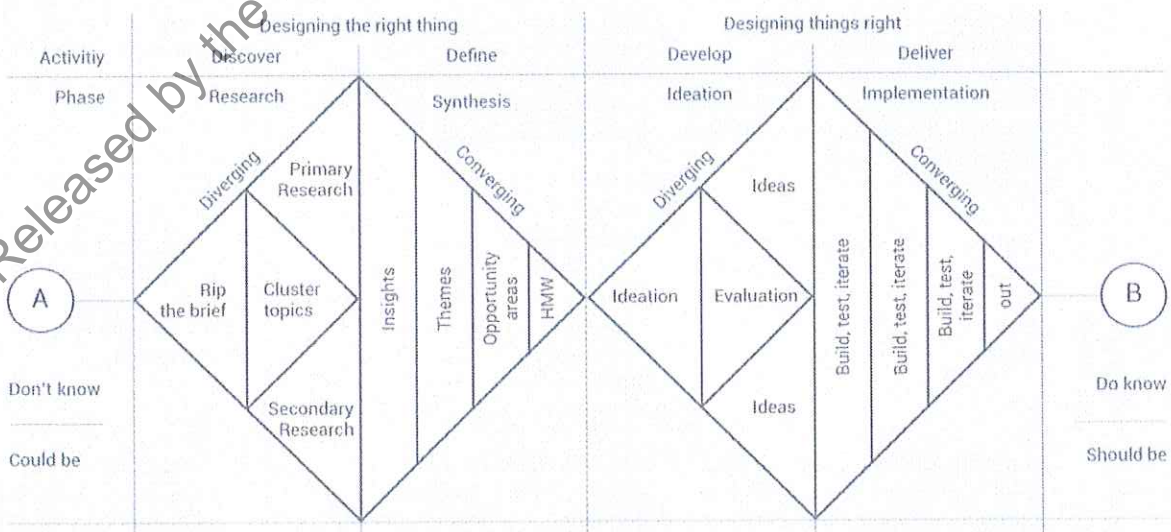
Date: ..... / ..... / .....

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



## A collaborative approach to refreshing the Strategy and Action Plan

1. Cabinet agreed on 2 April 2018 to the refresh of New Zealand's Cyber Security Strategy and Action Plan (the Refresh) [ERS-18-MIN-0004/CAB-18-MIN-0127].
2. The purpose of the Refresh is to take a comprehensive look at New Zealand's cyber security settings so that we have a framework for intensified government initiatives to improve New Zealand's cyber security.
3. In May 2018, you agreed to request an extension to the report back from the Cabinet External Relations and Security Committee (ERS) from July 2018 to October 2018. This will enable us to take a more collaborative engagement approach to the Refresh, involving outreach to a diverse range of stakeholders (the private sector, non-government organisations, civil society, and public sector entities). The Chair of ERS agreed to the extension [ERS-18-MIN-0010].
4. Extensive outreach and engagement is a key element in delivering a quality cross-government product, and generating buy-in for implementing the refreshed Strategy and Action Plan. We need to hear from a diverse range of stakeholders and enable them to contribute meaningfully to the process.
5. We adapted the 'double diamond' model (below) to design a collaborative and multi-layered approach for the Refresh. For the Refresh, 'A' is the current strategy and 'B' is the refreshed strategy. We will apply a mix of policy, strategy, design, and engagement practices throughout the different phases. In the diagram below, 'HMW' refers to the 'how might we' questions (e.g. 'how might we achieve [strategic objective Z]?') – in other words, open-ended questions to generate ideas.



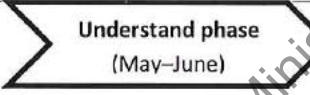
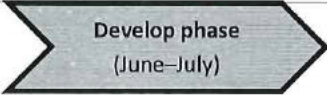
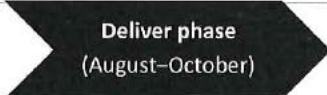
SOURCE OF DOUBLE DIAMOND DIAGRAM: Medium.com (<https://medium.com/digital-experience-design/how-to-apply-a-design-thinking-hcd-ux-or-any-creative-process-from-scratch-b8786efb812>)

6. The work of the sub-Working Groups and Working Group will require targeted engagement and consultation to understand the problems and opportunities in these specific areas, and develop actions and initiatives to respond accordingly:

- the **Working Group** is focusing on the overall approach to the Refresh and cross-cutting issues including:
  - the “institutional issues” such as assessing whether we have the optimal arrangements for effectively addressing cyber security efforts across government
  - ensuring system-wide understanding and mitigation of cyber security risks to government agencies
  - exploring innovative models to achieve strong cyber security collaboration between the government and the private sector and non-government organisations
- the **sub-Working Groups** are responsible for specific elements of the Refresh such as:
  - addressing cybercrime
  - international cooperation
  - the cyber security eco-system involving cyber security skills, research and development, growth of the sector and challenges of emerging technology.

7. This engagement will happen in parallel, and in coordination with over-arching engagement and consultation. There will be three key points during the process (**‘joint engagement activities’**) when all of the strands of the Refresh are brought together for collaborative interaction with stakeholders. These important junctures will provide opportunities for your involvement – and potentially other Ministers, if you agree. We will also report to you following these ‘joint engagement activities’ – and recommend, if you agree, that these reports are forwarded to other relevant Ministers for their information.

8. The table below shows, at a high level, the purpose, joint engagement activity, and key deliverables for each phase of the Refresh:

	 Understand phase (May–June)	 Develop phase (June–July)	 Deliver phase (August–October)
Purpose	Research and analyse the possible vision, goals and principles (potential framework for the Strategy) to understand what’s important for cyber-security in New Zealand from a range of perspectives and lenses.	Test the potential framework for the Strategy, and research, develop, and evaluate possible actions and initiatives to achieve the vision and goals.	Test and refine draft refreshed Strategy and Action Plan
Joint engagement activity	Workshop with stakeholders and outreach to key stakeholders. Also investigating using a survey and other methods to reach a wider audience.	Workshops and targeted consultation with interested stakeholders to develop and test possible framework for the Strategy (vision, goals and principles) and develop potential actions and initiatives.	Invite feedback on the draft refreshed Strategy and Action Plan (e.g. walkthroughs, workshops, further outreach and submissions)
Key deliverables	Report to Minister summarising insights from workshop and other outreach. Provide initial thinking about possible framework for the Strategy (vision, goals and principles) (due: s9(2)(f)(iv))	Report to Minister summarising insights from engagement and proposing a ‘strawman’ for the draft refreshed Strategy and Action Plan (due: s9(2)(f)(iv))	1. Report to Minister summarising insights from engagement, and final draft of refreshed Strategy and Action Plan (due: s9(2)(f)(iv))  2. Final Cabinet paper (due: s9(2)(f)(iv))



9. Each phase of the Refresh will be informed by insights from outreach and engagement, research, and analysis of the preceding phase(s). The A3 diagram in the Appendix shows an integrated view of the anticipated timing/phases, approach, key deliverables, and engagement activities.

## Goals and outcomes for outreach and engagement

10. To support our outreach and engagement activities, minimise disruption for stakeholders and maintain good faith, we identified goals and outcomes:
- **engagement goals:**
    - we will take a coordinated approach to engagement with stakeholders (given the interconnected nature of cyber security issues, many stakeholders will have perspectives on multiple elements of the Refresh – hence the need for a coordinated approach);
    - we will ensure a consistent narrative for outreach and engagement across stakeholders at each phase of the process;
    - we will enable sub-Working Groups and the Working Group to research and test proposals with targeted stakeholders (there are three key points in the process where the ‘threads’ of the process are brought together);
    - we will look for opportunities for agencies to join-up when engaging with stakeholders;
    - we will invite stakeholders to participate in a meaningful and open way, respecting their views, and keeping them informed throughout the Refresh;
    - we will invite stakeholders to assist with outreach and engagement in support of the Refresh.
  - **outcomes from engagement:**
    - stakeholders will know what the Refresh is about, the approach we are taking, and how to engage with us and contribute to the process;
    - we will have heard and considered a diverse range of views from as broad a range of stakeholders as possible;
    - there will be a range of opportunities and a range of ways for stakeholders to share their views and contribute to the Refresh;
    - the refreshed Strategy and Action Plan will reflect insights gathered through engagement activities.

## Approach to first ‘joint engagement activity’ during the ‘Understand’ phase

11. The first joint engagement activities (workshops) in the week of 25 June straddle the ‘discover’ and ‘define’ stages of the ‘understand’ phase. The workshops will be held in Wellington, Auckland, and Christchurch. In the ‘understand’ phase, we want an understanding of the breadth of views, interests, experiences and insights into what stakeholders think should be prioritised.
12. Workshops will be designed, with the support of facilitators and design-thinking, to hear from a diverse range of stakeholders. We anticipate this session will pose **broad questions** along the following lines:

- What do you think about cyber-security in New Zealand?
  - What are your experiences with cyber-security?
  - What do you see as the challenges and opportunities for cyber security? Now and in the future? Why?
  - What is important to you about cyber-security?
  
- What do you think of the current Strategy?
  - Does the vision describe the future state of cyber security that New Zealand should be aiming for?
  - Do the principles reflect what's important to us? What else should be considered?
  - Will the intersecting goals support us to achieve our vision? Is there anything missing – if so what, and why should it be included?
  
- What else should we be looking at?
  - What are the gaps or overlaps?
  - What are your priorities? What is important to you, your business/organisation, and your stakeholders?
  - Are there other opportunities?
  - What could make the biggest difference to New Zealand's cyber-security?
  - What do you think New Zealand should be known for in the cyber-security space?
  
- How do participants want to be involved in the Refresh? For example, would they like to:
  - attend workshops
  - engage directly with us
  - send us their thoughts
  - respond to a survey
  - receive updates
  - a mix of the above.

13. In addition to the workshops, there will also be opportunities to engage separately with stakeholders more directly involved in cyber security issues on the more specific areas for potential change highlighted in the Cabinet paper [ERS-18-MIN-0004/CAB-18-MIN-0127]. For example, we will seek their insights and views about:

- institutional cyber security arrangements (e.g. what innovative models could deliver strong cyber security collaboration between the government, and the private sector and non-government organisations?);
- government information security (e.g. how could we improve the system-wide understanding and mitigation of cyber security risks to government agencies?);
- addressing cybercrime (e.g. is our policy and legislative framework fit for the purpose of dealing with cybercrime in the digital age?);
- cyber diplomacy and deterrence (e.g. how can we ensure New Zealand is seen and heard in global dialogue on norms of acceptable state behaviour in cyberspace, the applicability of international law, and the importance of an open, free and secure Internet?);



- opportunities in cyber industry, research and skills (e.g. how could we expand New Zealand's cyber security industry, invest in cyber security research and development, and deal with the shortage of skilled cyber security workers?);
- security challenges of emerging technology (e.g. what role do you think the government should play to address security challenges arising from the Internet of Things and other emerging technologies such as Artificial Intelligence or Quantum computing?).

14. The desired **outcomes from the workshops** in this 'understand' phase are:

- insights into stakeholders' experiences and thoughts about cyber security, and its future challenges and opportunities;
- a clearer sense of stakeholder views and priorities on cyber security in New Zealand to inform our analysis on the vision, goals, and principles for the refreshed Strategy, and where to start with actions and initiatives for the Action Plan;
- for stakeholders to appreciate the breadth of views and interests, and to be recognised as contributors to the Refresh.

### **International experts**

15. We are exploring opportunities to invite international experts to visit New Zealand to provide independent advice, inform the consultation process and promote dialogue within New Zealand on cyber security.

### **Ministerial engagement opportunities**

16. We are exploring opportunities for you to be actively involved in this process.

17. We recommend that you are involved in the three 'joint engagement activities' across the three phases as these are key junctures in the process. For example, we suggest you provide an introductory presentation to kick off the Wellington workshop planned for 26 June (which we anticipate will be the largest). This could be videoed for relaying at the other workshops in Auckland and Christchurch if you are unable to be there in person. The Department of Internal Affairs Service Innovation Lab is hosting the Wellington workshops so this would also be an opportunity for you to be welcomed into their new space, and learn more about their current projects after the opening. The video could also be available on the Connect Smart website which will become a key vehicle for communicating progress on the Refresh.

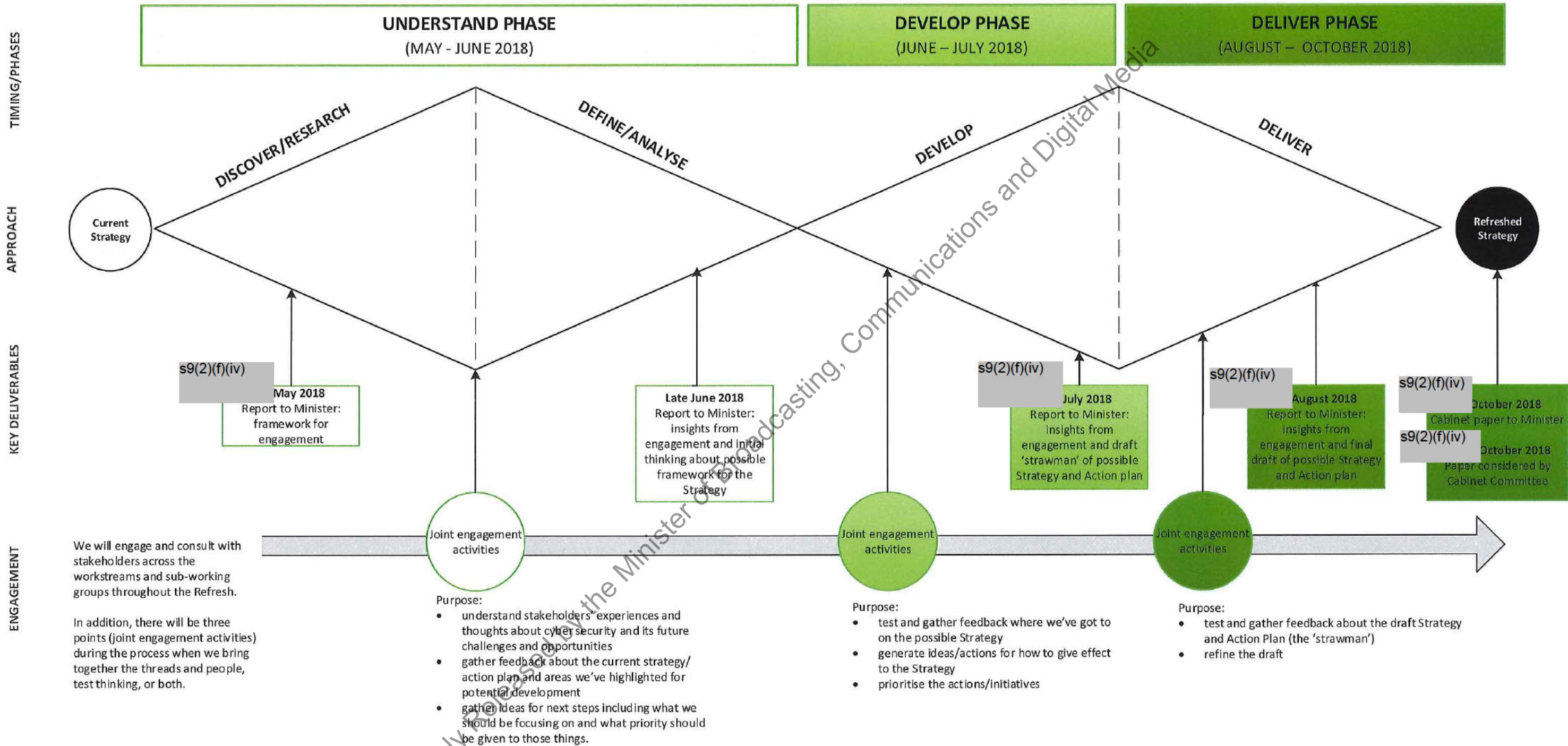
18. Proposals for the second and third 'joint engagement activities' will be refined once we have evaluated the first 'joint engagement activity'. But we envisage a role for you on those occasions and will provide further advice.

19. We will propose specific engagements with key stakeholders. You are meeting, for example, with the Chief Executive of InternetNZ on 11 June. If you agree, we could arrange roundtable meetings with key representatives of a particular sector. If you already have meetings with stakeholders who may also have a perspective on cyber security (e.g. civil society, the telecommunications sector, etc), we can provide briefing and background about the Refresh.

20. As we develop the strawman for the refreshed Strategy and Action Plan, and draw up possible initiatives, we also recommend early engagement with other relevant Ministers and, as appropriate, other Parties. We will provide brief updates on the Refresh in our weekly reports and fuller reports as outlined in the Appendix.

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

**APPENDIX: overview of the approach, engagement, and timing for the Refresh**



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





Minister for Broadcasting, Communications and Digital Media  
(Hon Clare Curran)

**BRIEFING: Meeting with InternetNZ, 11 June 2018**

Date:	8 June 2018	Tracking number:	
Security classification:	Unclassified	Priority:	Routine
Action sought:	<p><b>Note</b> the contents of this brief.</p> <p><b>Agree</b> that the Department of the Prime Minister and Cabinet release this brief in full once it has been considered by you, aside from the contact details of officials which will be withheld under OIA 9 (2) (a).</p>		
Deadline for action:	11 June 2018		

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
Paul Ash	Director, National Cyber Policy Office	s9(2)(a)	s9(2)(a)	✓
Heather Ward	Principal Adviser and Acting Team Leader National Cyber Policy Office	s9(2)(a)	s9(2)(a)	

Consultation
CERT NZ, DIA and MBIE have contributed to this paper.

**Minister's office to complete:**

- |   |  |
|---|--|
| <input type="checkbox"/> Approved             | <input type="checkbox"/> Declined            |
| <input type="checkbox"/> Noted                | <input type="checkbox"/> Needs change        |
| <input type="checkbox"/> Seen                 | <input type="checkbox"/> Overtaken by Events |
| <input type="checkbox"/> See Minister's Notes | <input type="checkbox"/> Withdrawn           |

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



Comments

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



Minister for Broadcasting, Communications and Digital Media  
(Hon Clare Curran)

## BRIEFING: Meeting with InternetNZ

### Purpose

- To brief you ahead of your meeting with InternetNZ representatives at 11.30am on Monday 11 June 2018.

### Recommendations

The Department of the Prime Minister and Cabinet recommends that you:

- Note** the contents of this brief.

Yes / No

- Agree** that the Department of the Prime Minister and Cabinet release this brief in full once it has been considered by you, aside from the contact details of officials which will be withheld under OIA 9 (2) (a).

Yes / No

Paul Ash  
Director, National Cyber Policy Office  
Department of the Prime Minister and  
Cabinet

Date: 2 / 6 / 18

Hon Clare Curran  
Minister for Broadcasting, Communications  
and Digital Media

Date: ..... / ..... / .....

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

1. **Jordan Carter**, the Chief Executive of InternetNZ, will call on you at 11.30am on Monday 11 June. He will be accompanied by **Brent Carey**, the new Domain Name Commissioner and Dr **Ellen Strickland**, Policy Director.
2. InternetNZ have provided you with a note ahead of this meeting (see Attachment A) covering .nz domain name changes; refresh of the Cyber Security Strategy; telecommunications law; digital divides; and the future form of CERT NZ. **Talking points** are provided for your discussion.

### **Refresh of the Cyber Security Strategy and Action Plan**

3. NCPO (Paul Ash and Heather Ward) met with InternetNZ on Wednesday 6 June to have an initial discussion about the refresh of the Cyber Security Strategy. We are setting up an inter-agency meeting with the InternetNZ team in the coming week to have a more extensive discussion on issues that might be addressed in a refreshed Strategy. We also propose to have more detailed meetings with InternetNZ as we develop and refine particular proposals.
4. We briefed InternetNZ on our approach to the refresh of the Cyber Security Strategy. We noted that we now had an extended timeframe for the refresh until end of October. This would enable us to carry out the extensive outreach and engagement that will be essential for the delivery of a quality cross-government product, and to generate buy-in from a broad range of stakeholders for implementing the refreshed Strategy and Action Plan.
5. We have designed a collaborative and multi-layered approach to the refresh involving three-phases: Understand, Develop and Deliver.
6. We are currently in the "understand" phase. This involves discovery and research, and open engagement with stakeholders, including at facilitated workshops ('Joint Engagement Activity' – likely to be in the week of 26 June). Our objective in this phase is to understand views about cyber security and gather feedback on potential areas for action. This first 'Joint Engagement Activity' will take place in parallel with targeted engagement with key stakeholders on particular issues and in coordination with, over-arching engagement and consultation.
7. There will be three key points during the process ('joint engagement activities') when all of the strands of the refresh are brought together for collaborative interaction with stakeholders.
8. Jordan Carter asked whether the strategy would be a government strategy or a New Zealand strategy. He emphasised the **importance of a multi-stakeholder approach to the refresh** in order to find the best possible means to improve New Zealand's cyber security.
9. We responded that, at the end of the day, this would be a government strategy for New Zealand, but that it would be developed in a collaborative way, involving a broad range of stakeholders, underlining the importance of partnership to address cyber security. Realistically, this process may not be the kind of "co-creation" envisaged by InternetNZ - but it will be inclusive and transparent; it will reflect collective public and private sector responsibility for cyber security; and it will deliver well-informed proposals for the Strategy and Action Plan.
10. InternetNZ was also interested to know **whether we envisaged a "major deliverable"** as part of this Strategy refresh (compared with the establishment of CERT NZ with the 2015 Strategy).



We noted that there were a number of other significant developments under the 2015 Strategy (e.g. CORTEX, a Level 6 qualification, cyber credentials for small businesses).

11. We ran through some of the areas highlighted in the Cabinet paper such as considering institutional arrangements and resources; addressing cybercrime; advancing cyber diplomacy and deterrence mechanisms; expanding the cyber security industry, investing in research and development, and growing the cyber security workforce; and addressing the security challenges of emerging technology.

12. s9(2)(ba)(i) We agree with InternetNZ's suggestion for engagement with the members of the Digital Economy and Digital Inclusion Ministerial Advisory Group (DEDIMAG) to ensure alignment with the broader Digital Strategy work.

### CERT NZ future form

13. You opted for the status quo of CERT NZ remaining a branded business unit within MBIE for the time being. This decision does not preclude the role of CERT NZ or other agencies involved in cyber security being considered in the context of the refresh of the Cyber Security Strategy. The Cabinet paper on the refresh indicated that there would be an assessment of whether we have the optimal arrangements and resources for effectively addressing cyber security issues.

14. There was a delay in confirming the status quo outcome with stakeholders while the extension of the CERT NZ Establishment Advisory Board (EAB) was organised and the report back to Cabinet on Future Form was confirmed as cancelled.

15. InternetNZ was informally advised of the outcome once this was done. They may, however, raise an issue around the communication of the outcome to the community.

16. The **CERT NZ Establishment Advisory Board** has had its term extended until 30 September, and will continue to advise and help ensure CERT NZ remains focused on engagement with the private sector. NCPO has also met with the CERT NZ Establishment Advisory Board to seek their views on the refresh of the Cyber Security Strategy. Members of the Board will be invited to the refresh workshops and other engagement activities.

### CERT NZ and InternetNZ

17. CERT NZ is continuing to work with Internet NZ on the planning for joint events such as **cyber smart awareness week**. Rob Pope and Jordan Carter are planning to catch up in the coming weeks as part of their ongoing relationship.

18. CERT NZ is seeking to conclude a MoU with the Domain Name Commissioner (who reports to Jordan Carter), which will ensure CERT NZ retains full access to **.nz registrar information for cyber security investigation and remediation purposes**. CERT NZ, in part because of its role and absence of regulatory, law enforcement or intelligence functions, will likely be the only organisation to be given the option to enter into such an agreement, and appreciates the opportunity to do so.



## ICANN and WHOIS

19. InternetNZ has a strong interest in the effect of the EU's General Data Protection Regulation (GDPR) on the WHOIS system. The WHOIS system enables users to see the details of people who register domain names ('registrants'). The Internet Corporation for Assigned Names and Numbers (ICANN) sets policies for most types of domain (except country-based domains – see below), including policies relating to the WHOIS system. ICANN's response to the GDPR means that users of the WHOIS will no longer have automatic access to the personal information in the WHOIS system.
20. The potential loss of public access to elements of the WHOIS<sup>s6(a)</sup> [REDACTED] MBIE and NCPO are working closely together (and with operational agencies) to manage the impact of the GDPR on WHOIS. We anticipate this work will involve two streams of work:
- In the shorter term, attempting to mitigate the impact of the GDPR on WHOIS through coordinating a NZ Government response (including working with the Government Chief Privacy Officer).
  - In the longer term, working with ICANN (and other countries) to help develop a more durable solution that enables government users (and others) with legitimate purposes to have access to personal information in the WHOIS.
21. InternetNZ sets policies for .nz domain names independently of ICANN. InternetNZ has recently reviewed the balance between privacy and transparency in the New Zealand WHOIS system. As part of this review, it has created the Individual Registrant Privacy Option. This enables individual registrants (i.e. not companies or other organisations) to have some of their personal information withheld from public display if they choose. InternetNZ has also restricted bulk access ('Port 43' access) to New Zealand WHOIS information in an attempt to protect registrants' information from automated harvesting.
22. As .nz domains are open to anyone in the world, Europeans may purchase .nz domains and therefore InternetNZ is affected by the GDPR. To address this issue, we understand InternetNZ's terms and conditions state that registrants are covered by New Zealand law in relation to their .nz domain.

## Telecommunications Amendment Bill

23. The Telecommunications (New Regulatory Framework) Amendment Bill has now been reported back to the House, following Select Committee consideration.
24. Internet New Zealand has been an active participant in the Select Committee process, and has been supportive of the Bill. Jordan Carter has called for the swift completion of the legislative process in his oral submission.
25. Internet New Zealand supports the general focus and intent of the Bill but has continued to encourage the fibre anchor product to be set at a higher level than that provided for in the Bill. Internet New Zealand continues to advocate for an ambitious mid-market anchor product, set at a high speed, such as a 1 Gigabit per second (Gbps) service, rather than the 100/20 Megabit per second (Mbps) anchor provided for in the Bill.

## Digital Inclusion

26. Jordan Carter is a member of the Digital Economy and Digital Inclusion Ministerial Advisory Group (DEDIMAG) sub-group focussing on Digital Inclusion. Officials from the Department of Internal Affairs are continuing to work with the Digital Inclusion sub-group to shape the approach to the blueprint for Digital Inclusion. In particular, they are focussing on the vision statement and timeframes for delivery. The Digital Inclusion sub-group will provide a written update to the wider DEDIMAG ahead of the next Zoom meeting which is scheduled for 19 June 2018. In addition to Digital Inclusion, there are four other sub-groups in DEDIMAG (ICT/Tech sector, SME/non-tech business, Digital connectivity, Adapting to disruption).
27. MBIE has recently initiated some research into developing an outcomes framework for digital inclusion and associated indicators, and is working closely with DIA on this work. Officials will be engaging with InternetNZ and the DEDIMAG as part of this research.
28. InternetNZ recently released the position paper *Solving Digital Divides Together*. The paper calls for a target of Universal Access for all New Zealanders and we know that InternetNZ is focused on Government investment as a means to close digital divides.
29. Jordan Carter may raise the approximately 16,000 households that will still not be covered by a high-speed internet network following the UFB2 and RBI2 projects. The recent InternetNZ paper notes that a subsidised satellite internet connection is a viable option for these households - it calculates this access could be provided for \$17 million up-front (installation costs) and a further \$14.2 million per annum in subsidised connection fees.

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



## Talking Points

- **Cyber Security Strategy refresh:** The refresh involves a collaborative and multi-layered approach in three phases: Understand, Develop and Deliver.
- The current “understand” phase involves discovery and research, and open engagement with stakeholders, including at facilitated workshops (planned for the week of 26 June).
- Our objective in this phase is to understand views about cyber security and gather feedback on potential areas for action.
- Throughout the refresh, there will be multiple ways for stakeholders to contribute. My aim is for the refresh to be inclusive and transparent; to reflect collective public and private sector responsibility for cyber security; and to deliver well-informed proposals for the Strategy and Action Plan.
- We welcome the active involvement of InternetNZ and value your insights. The refresh will certainly involve members of DEDIMAG – a key set of stakeholders.
- **CERT NZ:** CERT NZ is committed to engaging with the private and non-government sectors – and will continue to engage regularly with InternetNZ and the broader information security community.
- CERT NZ responded to InternetNZ feedback that they would like to see transparency in the Quarterly Reports. These reports now include the figures for referrals to all government departments.
- CERT NZ is benefiting from its current location in MBIE while it is still a small and relatively new organisation. Access to MBIE’s shared services is enabling it to spend more time focused on delivering to its mission.
- **WHOIS:** What impact has the GDPR had on your business? Is the Individual Registrant Privacy Option working well?
- What is the current situation in relation to Police access to the full New Zealand WHOIS information?
- **Telecommunications Amendment Bill:** We understand Internet New Zealand has a continued interest in the Government establishing a mid-market anchor service higher than the 100/20 Mbps.

s9(2)(f)(iv)



o s9(2)(f)(iv)

• s9(2)(f)(iv)

- The Internet New Zealand submission to Select Committee also provided a helpful suggestion that the Line of Business Restrictions relief concept be retained but that the Commerce Commission be given the opportunity to review future applications for such relief on the grounds that it may assist with innovation in the sector.
- We have adopted this helpful suggestion in the Bill that has now been reported back to the House.
- **Digital Inclusion:** Interested in InternetNZ's work on addressing the digital divide. How an InternetNZ and government agencies work together to bridge this divide?
- Interested in Jordan Carter's perspectives on the work of the Advisory Group? How is it progressing?

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

## Attachment A: Note provided by InternetNZ

# Hon Curran / InternetNZ meeting

Briefing note for meeting at 11.30am on 11 June 2018

IntNZ attendees: Jordan Carter (CE), Brent Carey (Domain Name Commissioner), Dr Ellen Strickland (Policy Director).

### Changes in approach to .nz domain name policymaking

We would like to introduce recent changes in InternetNZ Group with Brent Carey taking over as our new Domain Name Commissioner and Dr Ellen Strickland who is now leading our .nz (and public) policy efforts as Policy Director.

### Refresh of the Cybersecurity strategy

We would like to discuss the scope and goals of the strategy refresh and would like to provide input around domain name takedown policy and an Abuse Forum we are planning to host later this year to discuss dealing with cybersecurity abuse in the .nz domain space. We also ask that you consider taking advice from DEDIMAG on the strategy refresh to help align cybersecurity efforts with the wider goals of the Government's Digital Strategy.

### Telecommunications law

We have engaged constructively on the Telecommunications (New Regulatory Framework) Amendment Bill and would like to talk to you about anchor products. We have long advocated for ambitious, aspirational anchor products that will drive New Zealanders' Internet usage and help New Zealand make the most of the infrastructure we have invested in.

### Solving Digital Divides

We are engaging with your officials on digital divides issues and InternetNZ is working to support DEDIMAG to help make a meaningful contribution to collectively solving New Zealand's digital divides. Government investment is going to be critical in closing the digital divide and we would like to understand your intentions in this area.

### Future form of CERT NZ

We would like to discuss the future form of CERT NZ in light of both the extension of the Establishment Board's term, and Budget 2018's additional \$3.9m over the next four years. We believe that to be most effective, CERT is a collaboration between the public and private sectors, not a government service provider, and as such needs governance arrangements that keep it outside the core state sector.

We provide this note as a courtesy to give the Minister and officials an indication of the main points we will raise in the meeting.

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



**BRIEFING: Meeting with Sai Honig, International Information System Security Certification Consortium, (ISC)<sup>2</sup>: cyber security skills**

<b>To:</b>	Hon Clare Curran Minister for Broadcasting, Communications and Digital Media
------------	---

<b>Date:</b>	22 June 2018	<b>Tracking number:</b>	DPMC-2017/18-1468
<b>Security classification:</b>	IN CONFIDENCE	<b>Priority:</b>	Routine
<b>Action sought:</b>	For Noting		
<b>Deadline:</b>	22 June 2018		

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
Paul Ash	Director, National Cyber Policy Office	s9(2)(a)	s9(2)(a)	✓
Heather Ward	Team Leader, National Cyber Policy Office	s9(2)(a)	s9(2)(a)	

<b>Agencies consulted</b>
N/A

**Minister's office to complete:**

<input type="checkbox"/> Approved	<input type="checkbox"/> Declined
<input type="checkbox"/> Noted	<input type="checkbox"/> Needs change
<input type="checkbox"/> Seen	<input type="checkbox"/> Overtaken by
<input type="checkbox"/> See Minister's Notes	<input type="checkbox"/> Withdrawn

<b>Comments</b>



**BRIEFING: Meeting with Sai Honig, International Information System Security Certification Consortium, (ISC)<sup>2</sup>: cyber security skills**

To:	<b>Hon. Clare Curran</b> Minister for Broadcasting, Communications and Digital Media
-----	---

**Purpose**

To brief you in preparation for your meeting with Sai Honig, board member of the International Information System Security Certification Consortium ((ISC)<sup>2</sup>), on 28 June at 11.30am.

**Recommendations**

The Department of the Prime Minister and Cabinet recommends that you:

1. **Note** the contents of this briefing

Yes / No



Paul Ash  
Director, National Cyber Policy Office  
Department of the Prime Minister and  
Cabinet

Date: 22 / 6 / 18

Hon. Clare Curran  
**Minister for Broadcasting,  
Communications and Digital Media**

Date: ..... / ..... / .....

## Sai Honig and Cyber Security Skills

---

1. You are meeting with Sai Honig at 11.30am on Thursday 28 June. Ms. Honig sits on the board of the **International Information System Security Certification Consortium, (ISC)<sup>2</sup>** – an international, non-profit membership association for information security professionals.
2. On the 15<sup>th</sup> of May, you spoke at the inaugural meeting of “Wahine in Tech”, an organisation aiming to “create a culture of success for women in the tech industry” and “to encourage discussions of the issues, attitudes, and tactics [women] face daily in the technology industry”.
3. Ms. Honig emailed after meeting you at this event. She expressed interest in meeting with you to discuss “how (ISC)<sup>2</sup> can help to create a more inclusive digital economy and increase awareness and understanding of information security.” Paul Ash, Director NCPO, Ginny Baddeley, Director of National Security Workforce (DPMC), and Amy Corkery, Advisor NCPO, will attend the meeting with you.
4. s9(2)(a)



## What is the International Information System Security Certification Consortium, (ISC)<sup>2</sup>?

---

5. (ISC)<sup>2</sup> stands for International Information System Security Certification Consortium. It is a non-profit organization which has over 130,000 members globally. It specialises in training and certifications for cyber security professionals. It has been described as the “world’s largest IT security organization”.
6. (ISC)<sup>2</sup> certifications require applicants to pass rigorous, in-person examinations, which are administered at licensed testing centres worldwide. Everyone who obtains a certification from (ISC)<sup>2</sup> automatically becomes a member. The most widely known certification offered by (ISC)<sup>2</sup> is the Certified Information Systems Security Professional (CISSP) certification, which is one of the most popular qualifications of its type.<sup>1</sup>
7. Members typically include enterprise information security professionals, such as: Chief Security Officers; Security Officers; Chief Technology Officers; Chief information Officers; security managers; systems engineers; systems integrators; chief risk officers; systems

<sup>1</sup> As of 1 January 2018, there are 122,289 (ISC)<sup>2</sup> members holding the CISSP certification worldwide, in 166 countries with the United States holding the highest member count at 79,617 members. From ISC website:  
<https://www.isc2.org/About/Member-Counts>



administrators; and network administrators. All certified (ISC)<sup>2</sup> professionals are required to support the (ISC)<sup>2</sup> Code of Ethics.

8. (ISC)<sup>2</sup> also offers general public education through its charitable trust, the Centre for Cyber Safety and Education, which provides educational resources, college scholarships and industry research.
9. (ISC)<sup>2</sup> has an Auckland chapter, formed in 2012, which organises (ISC)<sup>2</sup> professionals in the North Island. Waikato University's group *Cyber Security Researchers of Waikato* has been listed as a (ISC)<sup>2</sup> official training provider. There are 291 (ISC)<sup>2</sup> qualification holders in New Zealand, with 263 of those holding the CISSP.

## What is the government doing to support the cyber security workforce?

---

### Cyber security skills shortages

10. There is a worldwide shortage of cyber security workers—the 2017 Global Information Security Workforce Study, driven by (ISC)<sup>2</sup>, of over 19,000 information security professionals, found that by 2020 the global shortage would be around 1.8 million. According to a 2016 UK survey, the demand for cyber security professionals is growing 3.5 times faster than the overall IT job market, and 12 times faster than the total labour market.
11. The Greater Wellington Regional Council commissioned research from KMatrix in 2017 to understand the demand for cyber security roles across the Wellington region. Their projections show demand for cyber security roles across the board and predict a 14 percent growth in required cyber security roles over the next two years ending 2019 – translating to 265 positions. Extrapolating nationally, this would translate to a need for approximately 1500-1900 positions across New Zealand over the same time period.
12. s9(2)(g)(i)

### Setting up the Cyber Security Skills Taskforce

13. One of the actions in the Action Plan accompanying the 2015 Cyber Security Strategy was to build a cyber security professional workforce. To help achieve this, a public-private **Cyber Security Skills Taskforce** was established to stimulate new initiatives (such as scholarships, internships and training). The Taskforce is made up of eight private sector and academic representatives. The Taskforce has finished the bulk of the work that it set out to accomplish: s9(2)(g)(i)

14. The taskforce has focused on practical initiatives to help build a cyber security professional workforce, including:



- a. Establishing a Level 6 (sub-degree level) Diploma in Cyber Security. NZQA is currently refining the diploma following stakeholder feedback, and preparing the last parts of the documentation for the application to list the new qualification.
- b. Developing a secondary school pathway to enable early identification of year 13 students into the qualification.
- c. Working with industry to develop an internship framework for cyber security students and graduates.
- d. Developing programmes to address the lack of diversity within the cyber security workforce, so that we are drawing from the widest available talent pool;
- e. Working with training providers to progress other programmes to expand the pipeline of future talent.

### **Cyber skills shortages and diversity**

15. Solving the workforce shortfall in cyber security will require introducing more ethnic, age and cultural diversity. Good cyber security requires understanding computer users' behaviour, as well as promoting awareness and understanding of organisational risk in an effective, consumable way. A 2013 (ISC)<sup>2</sup> report revealed that, globally, only 11% of the cyber security workforce are women. More recently, reporting suggests that the number of women involved in cyber security has increased to 20%.<sup>2</sup>
16. The NCPO, together with DPMC's National Security Workforce team, is planning a women in cyber event to be held in August 2018. The Women in Cyber event will include "speed dating" sessions between mentors and mentees, and presentations from experienced professionals in the cyber security sector.

### **Cyber Security Skills and the Refresh of New Zealand's Cyber Security Strategy**

17. The NCPO is undertaking wide ranging stakeholder engagement as a part of the Refresh of the Cyber Security Strategy. A key topic for the refresh is increasing the supply of skilled cyber security workers. Increasing the supply of skilled cyber security professionals is an opportunity to not only contribute to improving New Zealand's ability to protect our information systems, but support economic growth, including potentially in the regions and through exports.<sup>s9(2)(a)</sup>

- a. career pathways into cyber security (Ms. Honig began her career as an auditor and has a degree from the University of Arizona in aerospace engineering); and
- b. the barriers and challenges for women to enter and participate in the cyber security workforce.

<sup>2</sup> Report by Cyber security Ventures, due out in Q2 2018

## Annex 1

### Talking Points for your meeting with Sai Honig

#### *International Information System Security Certification Consortium (ISC)<sup>2</sup>*

- I'm interested in your experience with the (ISC)<sup>2</sup>. Is it playing an active role in New Zealand at present?
- Why is there a shortage of cyber security professionals? There is clearly demand – why is there not supply? Or are there issues matching supply and employer demand?
- The Cyber Security Skills Taskforce has focussed on building multiple pathways into the cyber security profession – such as a new Level 6 Diploma. What is your view on the varieties of cyber security qualifications in New Zealand? Are they fit for purpose?
- Do we have the right mix of qualifications and avenues into the cyber security profession in New Zealand? What more can be done?
- There is a lack of diversity in the information technology sector in general, and cyber security in particular. Some work is underway to attract more women to the cyber security industry. A 'Women in Cyber' event will be held in August 2018.
- Are there particular barriers for women in the cyber security sector?
- We are keen to focus on building cyber security skills – from general awareness and capability through to professional expertise. The Refresh of the Cyber Security Strategy and Action Plan provides an opportunity to consider new initiatives. We welcome your participation in the Refresh process.





## Aide memoire: Cyber Security Strategy Refresh Workshop, 26 June 2018

---

**To:** Hon Clare Curran, Minister of Broadcasting, Communications and Digital Media

**From:** Paul Ash, Director National Cyber Policy Office

**Date:** 25 June 2018

**Classification:** Unclassified

**Tracking No:** NCPO – x- 2018

---

### Cyber Security Strategy Refresh Workshop at DIA Service Innovation Lab

1. From 1.45pm to 2.45pm on Tuesday 26 June you are dropping into the second Wellington workshop on the refresh of the Cyber Security Strategy, at the Department of Internal Affairs' Service Innovation Lab.
2. You will be met by Grant Carpenter at the entrance to 191 Thorndon Quay at 1.45pm – the new premises for the Lab (you visited the Lab at its former location in December 2017). Grant will provide a brief tour of the new Lab and then bring you to the Cyber Security Strategy refresh workshop. Paul Ash, Director of the National Cyber Policy Office, will meet you at the workshop.
3. The **Service Innovation Lab** is a place where teams from different agencies, NGOs, private sector and New Zealanders can be co-located in a physical space conducive to collaboration and experimentation, supported by skilled lean and agile coaches who can help teams rapidly evolve their working methods.

### Details of the Cyber Security Strategy Refresh workshop

4. We have received around 50-60 RSVPs for each of the two Wellington workshops on 26 June. The list of attendees for this particular workshop is attached as Attachment A. The workshops are facilitated by KPMG s9(2)(a) James Greally) and Thought Partners (Meredith Osmond).
5. The workshops will focus on understanding:
  - what is important for cyber security at an individual, organisational and national level;



- what **principles** should we bear in mind for cyber security?
  - what **goals** should we focus on?
  - what do we want New Zealand to be known for in the cyber security space (**vision**)?
6. In addition to the facilitated discussion on principles, goals and vision, there will be posters around the room with detailed questions relating to the areas for possible attention highlighted in the Cabinet paper on the refresh of the Cyber Security Strategy (i.e. institutional issues, cybercrime, cyber diplomacy and deterrence, development of a cyber security sector, cyber skills and workforce, and cyber research and development). There will also be a poster setting out the priority areas of a selection of other countries' cyber security strategies (e.g. UK, Netherlands, Singapore, and Australia). Participants will be able to provide post-it comments on these posters at any point (e.g. before or after the workshop as they mingle in the room).

#### Your role at the Workshop between 1.50pm – 2.45pm

7. From **1.50pm – 2.20pm**, the workshop will focus on **principles** (led by s9(2)(a) from KPMG). In groups of approximately ten, participants will set out up to five possible principles, with the current Strategy principles as a reference. Each group will report back one idea for a possible principle.
8. From **2.20pm – 2.50pm**, the workshop will focus on **goals** (led by s9(2)(a) from Thought Partners). Participants will self-select a station around the room, representing one of the existing four goals or a "blank" station. They will consider whether the goal is still relevant, and whether there are other areas or goals that we should focus on. Participants can wander around the stations and add their thoughts in different areas.
9. We have provided you with some talking points. **You may wish to speak at the juncture between the principles and goals exercises (around 2.20pm)**. During both the principles and goals discussions, you could wander around the room, mingling with the various work stations to get a sense of the discussion.
10. Attached is the PowerPoint presentation for the workshop (Attachment B) and the confirmation email sent to participants (Attachment C).

#### For those who can't attend the workshop.

11. In addition to the workshops, we are launching an **online survey this week on the Connect Smart website**. The survey will match the questions and areas of focus at the workshops and enable those unable to participate, or who prefer contributing in a written format, or need more time than is possible in a workshop, an opportunity to contribute to the refresh of the Cyber Security Strategy.

**Pulling it altogether**

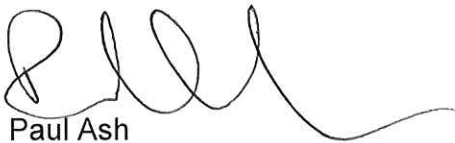
12. Following the workshops in Wellington, Auckland and Christchurch, we will have a facilitated **“pull it together” session** at the Service Innovation Lab on 3 July with NCPO and members of the Cyber Security Strategy Working Group (and sub-Working Groups) to analyse the outcomes from the workshops and research to date. We will present this to the Governance Group that afternoon. We will also prepare a public summary of the outcomes and key insights for circulation to participants and publication on the Connect Smart website. A report on the outcomes and key insights, and next steps, will be provided to you by 5 July.

**Recommendations**

---

The Department of the Prime Minister and Cabinet recommends you note the contents of this aide-memoire.

**Noted**



Paul Ash  
Director National Cyber Policy Office  
**Department of the Prime Minister and Cabinet**

Date: 25. / 06. / 2018.....

Hon Clare Curran  
**Minister of Broadcasting,  
Communications and Digital  
Media**

Date: ..... / ..... / .....

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

Attachment A: List of Participants for Wellington afternoon workshop

First Name	Last Name	Organisation	Position
s9(2)(a)		PwC	s9(2)(a)
		MBIE	
		I S Assurance Services	
		SSS - IT Security Specialists	
		GCSB	
		New Zealand Customs Service	
		GCSB	
		Victim Support	
		Police	
		NZDF	
		Aspeq	
		Ministry of Health	
		KPMG	
		MinterEllisonRuddWatts	
		DPMC	
		DPMC	
		Wellington Water	
		DIA	
		IR	
		Capital & Coast District Health Board	
		Internal Affairs	
		National Maritime Coordination Centre	
		(None - actively job-seeking)	
		IBM	
		Victoria University	
		Ministry of Health	
		MinterEllisonRuddWatts	
		Office of the Privacy Commissioner	
		Netsafe	
		Office of the Privacy Commissioner	

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



UNCLASSIFIED

Nicola	Brown	InternetNZ	
s9(2)(a)		GEOINT NZ	s9(2)(a)
		KPMG	
		Aspeq	
		NZDF	
		MFAT	
		Google	
		University of Waikato	
		Xero	
		Department of Corrections	
		GCDO	
		Department of Internal Affairs	
		Geeks On Wheels	
		Inland Revenue	
		Lateral Security	
		Aura Information Security	
		Department of Internal Affairs	
		University of Waikato	
		Pentech	
		Bank Of New Zealand	
		New Zealand Police	
		Defend	
		Geeks On Wheels	
		KPMG	

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

**Attachment B: PowerPoint presentation for Cyber Security Strategy refresh workshops**



DEPARTMENT OF THE  
PRIME MINISTER AND CABINET  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

## Refresh of the Cyber Security Strategy and Action Plan: Understand phase

NATIONAL CYBER POLICY OFFICE

June 2018

"We must protect the information and network systems that are vital to our economic growth, ensure the integrity and security of our increasingly digitalised government services and make sure Kiwis can interact online without suffering harm."

*Minister Clare Curran*

**INTRODUCTION**



**Objectives**

To take a comprehensive look at New Zealand's cyber security framework and settings and gather from a breadth of views and interests:

- Your experiences about cyber security
- Your views on future challenges
- Your thoughts on the opportunities to improve New Zealand's cyber security.

**INTRODUCTION**



EMBEDDED VIDEO FROM  
THE MINISTER

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





CONTEXT

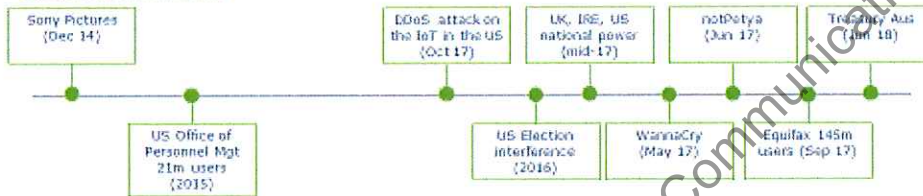
Global trends

"49% [of CEOs] say that becoming a victim of a cyber attack is now a case of 'when', and not 'if'. 51% believe they are well-prepared for a cyber attack."  
2018 Global CEO outlook, KPMG



- Lower trust and increasing public concern
- Increasing threat trajectory
- Emerging technology

Examples of recent cyber crime



CONTEXT

New Zealand

"One in five (20%) New Zealanders have been affected by cyber crime in the past year. This raises to 72% when spam and suspicious emails are factored in."  
Research into Cyber Security Behaviours 2016 National Cyber Policy Office



396 cyber incidents in 2017 (31 intensive incidents) (GCSB)



Highest ever number of vulnerabilities reported, and more than 2x as in previous quarter (CERT NZ)



67% Increase in incidents involving unauthorised access in 2018 to date (CERT NZ)



Phishing the top category of incidents in 2018 to date (CERT NZ)



Approx. \$3m in losses across 500 incidents of cyber crime in 2018 to date (CERT NZ)

## CONTEXT

### What we've done

We have started to make positive steps towards protecting New Zealand:

- Establishment of CERT NZ in 2017
- Delivery of CORTEX malware detection and disruption services
- Cyber Security Emergency Response Plan
- Cyber security awareness campaigns
- Protective Security Requirements for government agencies
- Work to improve cyber security of small businesses
- Building a cyber security workforce
- International engagement on cyber security issues
- Cyber Security Summit.
- Establishment of the NCSC in 2011
- Establishment of NCPO in 2012
- Cyber Security Strategies and Action Plans in 2011 and 2015

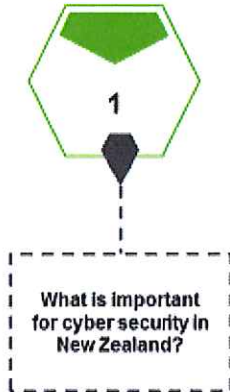
"It's timely for us to step up New Zealand's cyber security efforts so that we are not left vulnerable to cyber intrusion and to refresh the 2015 strategy so we can deal with increasingly bold, brazen and disruptive threats"

*Minister Clare Curran*

## INTRODUCTION

### Aim of this session

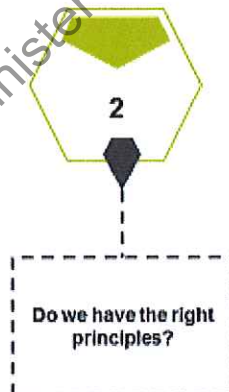
The aim of this session is to **understand** the principles, goals and vision by exploring the following questions:



## INTRODUCTION

### Aim of this session

The aim of this session is to **understand** the principles, goals and vision by exploring the following questions:

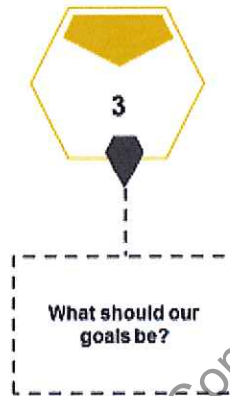




## INTRODUCTION

### Aim of this session

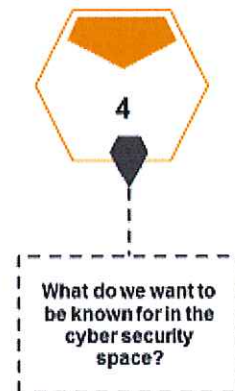
The aim of this session is to **understand** the principles, goals and vision by exploring the following questions:



## INTRODUCTION

### Aim of this session

The aim of this session is to **understand** the principles, goals and vision by exploring the following questions:

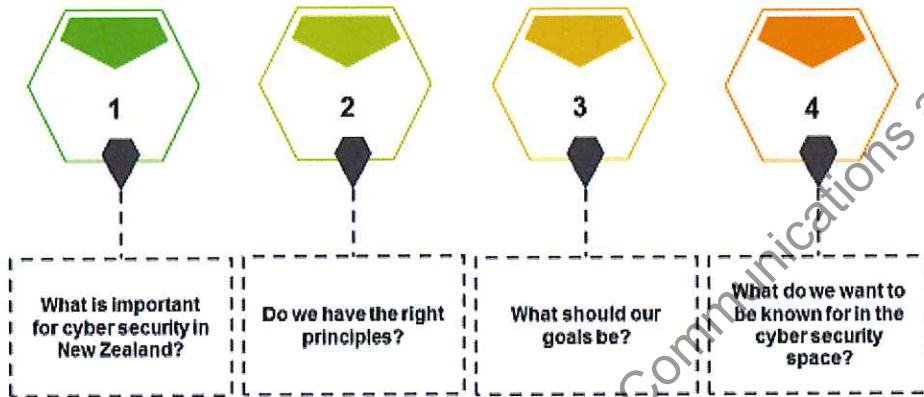




**INTRODUCTION**

**Aim of this session**

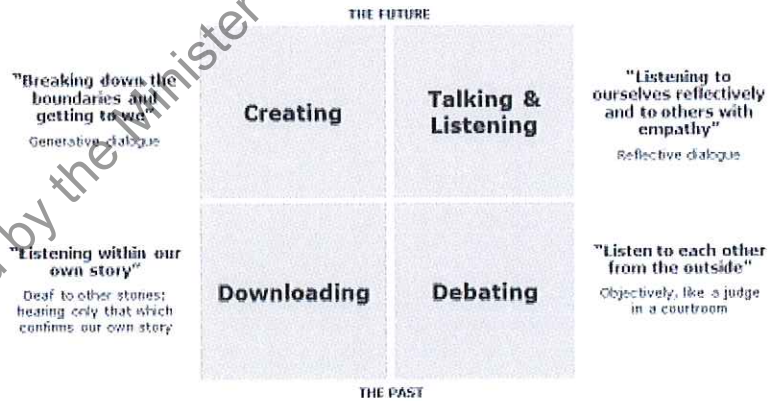
The aim of this session is to **understand** the principles, goals and vision by exploring the following questions:



**TODAY**

**How today will run**

**Four Ways of Talking and Listening**



From Adam Kahane, *Solving Tough Problems: A New Way of Talking, Listening, and Creating New Realities*

## 1. AREAS OF FOCUS

### Key questions

- 1 What is important for you about cyber security in New Zealand?
- 2 What is important for cyber security at an individual level, organisational level and national/international level?

### Layout

- Mixed groups of five in your semi-circles

## 2. PRINCIPLES

### Key question

- 1 What do we need to bear in mind when making our choices and decisions on cyber security?

### Layout

Mixed groups of 10 at each of the "Yellow" stations around the room





### 3. GOALS

#### Key questions

- 1 Are these goals still relevant?
- 2 Are there any other goals or areas you think we should focus on?

#### Layout

- Self-select the "Green" stations around the room



### 3. GOALS





## 4. VISION

### Key question

- 1 What do we want to be known for in the cyber security space?

### Layout

- Mixed groups of six to eight at each of the stations around the room



## NEXT STEPS

### Next steps

- Summarise insights and themes from all Understand sessions (complete by early July)
- Develop options for the vision, goals and principles that we can test in the develop phase
- Report back to participants on these by mid-July.



## NEXT STEPS

### Before you go...

- Feel free to stay behind and add your ideas to the more detailed questions
- If you wish to be involved going forward, please email us at [connectsmart@dpmc.govt.nz](mailto:connectsmart@dpmc.govt.nz)
- Please rate the session using the Board near the exit.

## THANK YOU

If you have any further thoughts or want to be involved in this project further, please email us at

[connectsmart@dpmc.govt.nz](mailto:connectsmart@dpmc.govt.nz)

For further information, please visit

[www.connectsmart.govt.nz](http://www.connectsmart.govt.nz)

**Attachment C: Confirmation email sent to participants**



[Click here](#) to view online

[newzealand.govt.nz](http://newzealand.govt.nz)



# Cyber Security Strategy Refresh Workshop Confirmation

Tēnā koe

We are pleased to confirm your participation in the **Wellington** workshop on the refresh of New Zealand's Cyber Security Strategy.

## Event Details

**Date:** Tuesday 26 June

**Time:** 12.30pm - 3.00pm

**Venue:** DIA Service Innovation Lab, Level 4, 191 Thorndon Quay, Wellington

## Overview

The Minister of Broadcasting, Communications, and Digital Media announced the refresh of New Zealand's Cyber Security Strategy in April. Cybercrime and cyber security threats continue to increase so it's important we review New Zealand's approach to cyber security.

The Refresh includes three phases, illustrated below:



**Purpose:** Research and analyse the possible vision, goals and principles.

**Purpose:** Research, develop and evaluate possible actions and initiatives to achieve the proposed vision and goals.

**Purpose:** Test and refine draft refreshed strategy and action plan.

In this first “understand” phase, we are keen to hear from a diverse range of stakeholders from the private sector, non-governmental organisations (NGOs), civil society and public sector entities.

We want to identify key themes to improve New Zealand’s cyber security, and develop the principles, goals and vision for a refreshed Cyber Security Strategy.

Ahead of the workshop, you might like to read this [one page summary](#) of the current Cyber Security Strategy. The workshop will focus on [four key questions](#) – you might like to think about these in advance too.

For more information about the refresh, visit the [Connect Smart website](#). Look forward to seeing you at the workshop.

Ngā mihi

The National Cyber Policy Office

### Contact us

Get in touch with a member of the team at Connect Smart

National Cyber Policy Office  
Phone: +64 (4) 819-8200  
Email: [connectsmart@dpmc.govt.nz](mailto:connectsmart@dpmc.govt.nz)

[www.connectsmart.govt.nz](http://www.connectsmart.govt.nz)

Connect with us



Brought to you by

**ubiquity**

LEADERS IN DATA-DRIVEN MARKETING

You are being sent this email as a valued partner in the Connect Smart programme.  
If you wish to unsubscribe please [click here](#).