DEPARTMENT *of the*
PRIME MINISTER *and* CABINET
Te Tari o Te Pirimia me Te Komiti Matua

Briefing to the Incoming Minister

Cyber Security Policy, Department of the Prime Minister and Cabinet

Date:	22 December 2016	**Priority:**	Routine
Security classification:	Restricted	**Tracking number:**	

Purpose

This briefing introduces you to your role as the Minister responsible for cyber security policy, and includes information on:

1. The current cyber security threat environment
2. The roles of New Zealand government agencies in dealing with cyber security threats; and
3. Current cyber security policy settings.

Recommendations

We recommend that you:

1. **Note** the information contained within this briefing;
2. **Note** that officials are available to meet to provide further information on New Zealand's cyber security policy and operational settings, and to seek your views on the cyber security policy work programme; and
3. **Note** that officials can also provide you with a classified briefing on request.

Paul Ash
Director
National Cyber Policy Office

..... / 12 / 2016

Hon Simon Bridges
Minister for Communications

..... / 12 / 2016

Cyber Security: Introductory Briefing

1. This introductory briefing is intended to provide you with an overview of New Zealand's current cyber security policy settings, the role of the National Cyber Policy Office (NCPO) in the Department of the Prime Minister and Cabinet (DPMC), and to support initial engagement on your priorities. Officials are available to provide further information and to meet with you to discuss the topics introduced in this briefing and seek your views on the NCPO's cyber security policy work programme.

The big picture: what's the problem that we're facing?

2. New Zealand's cyber security has become an increasingly critical element of our national security and economic well-being. The Internet is simultaneously the backbone of the world's economy and a major threat vector. New Zealand's geographic isolation is no protection from a wide array of threats, ranging from criminal activity to advanced threats from state-sponsored actors. New Zealand's national security depends on securing and protecting our most significant national assets.

3. The threats and threat actors are diverse. New high-profile data breaches emerge almost weekly. Recent international examples include the exposure of the private details from more than 412 million Friend Finder Networks accounts, and the leak of 68 million Dropbox passwords. In the last week, Yahoo has revealed that more than 1 billion user accounts may have been compromised by a breach in 2013. Ransomware attacks – where malicious software renders data or systems unusable until the victim makes a payment – have also become more common. The number of ransomware attacks targeting companies has increased threefold over 2016, affecting one in every five businesses worldwide.[1]

4. With an ever-growing number of everyday items connected to the Internet ('Internet of Things' (IoT) devices), the potential attack surface has also increased. A major distributed denial of service (DDoS) attack[2] using an IoT botnet[3] in October 2016 disrupted a range of the world's biggest websites (including Spotify, Twitter and Paypal) by flooding those sites with traffic. In August 2016, Australia's first-ever digital census was disrupted and forced offline after the census website was targeted by a series of DDoS attacks. Finally, public reporting now suggests that US intelligence agencies have concluded that Russia acted covertly to influence the recent Presidential election, using information gleaned by hacking the Democratic National Committee. This highlights the complex nature and array of cyber threats.

5. New Zealand is yet to experience a major cyberattack. However, New Zealanders and New Zealand businesses are affected by a range of cyber threats every day. The National Cyber Security Centre (NCSC) in the Government Communications Security Bureau (GCSB)

---

1 Lucian Constantin, "Ransomware attacks against businesses increased threefold in 2016", *Computerworld*, 10 December 2016.

2 A denial of service attack is when users are denied access to an Internet site or computer service because a malicious actor has overloaded the service with requests.

3 A botnet is a network of infected Internet-connected devices that are used to commit coordinated attacks without the device owners' knowledge.

recorded 338 cyber incidents in 2015/16 – an average of 28 incidents per month.[4] Research conducted in 2016 found that 20 percent of New Zealanders have been affected by cybercrime in the last year.[5] The global cost of cybercrime is estimated to be around $600 billion a year. New Zealand depends on connectivity for its economic future. It is estimated that $34 billion could be added to our economy if businesses made more effective use of the Internet.[6] The cost of cyber insecurity will have a real impact on our economy.

6. Improved cyber security also has the potential to deliver opportunities for New Zealand. It will enable New Zealanders and businesses to use information technology to its full potential - driving innovation, improving productivity, and enhancing quality of life. Ensuring New Zealand is secure, resilient and prosperous online is essential for building a more competitive and productive economy. Making the most of the digital economy is a key component of the innovation area of the Business Growth Agenda. Improved cyber security will mean New Zealand is a place where:

- New Zealanders and their businesses prosper;
- the harm from cyber threats and cybercrime is reduced;
- fundamental rights online are protected;
- significant national information infrastructures are defended; and
- New Zealand is respected internationally as a secure place to do business and store data.

Cyber security and the New Zealand government

Your role as Minister for Communications and cyber security

7. The Minister for National Security and Intelligence has overall responsibility for cyber security policy. However, to date, the Prime Minister has allocated responsibility for cyber security policy to the Minister for Communications, given the strong links between the two policy areas. Cyber security policy is a national security issue that has close linkages to the broader Business Growth Agenda (BGA). Improved cyber security will enable New Zealanders and businesses to use information technology to its full potential – helping drive innovation and improve productivity – and develop New Zealand as a hub for high-value, knowledge-intensive businesses conducting research and development (R&D).

8. In this role, you are likely to work closely with the Minister in Charge of the NZ Security Intelligence Service and the Minister Responsible for the GCSB. Given cyber security is a cross-cutting issue, you are also likely to work with a range of other Ministers, including the Minister of Justice, the Minister of Police, the Minister of Foreign Affairs and the Minister of Defence.

---

4 Government Communications Security Bureau, *Annual Report 2016*. Available at http://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/GCSB-Annual-Report-2016.pdf.

5 Colmar Brunton, "Research into Cyber Security Behaviours 2016", November 2016. Available at https://www.connectsmart.govt.nz/assets/Uploads/Colmar-Brunton-post-Connect-Smart-Week-2016-research2.pdf

6 Hayden Glass et al, "The value of internet services to New Zealand businesses," 31 March 2014, Innovation Partnership. Available at http://www.innovationpartnership.co.nz/wp-content/uploads/2016/07/The-Value-of-Internet-Services-to-NZ-Businesses.pdf.

The roles of government agencies

9. The National Cyber Policy Office (NCPO) leads the provision of cyber security policy advice to the government, and supports you in your work in this area. In 2012 Cabinet agreed to establish the NCPO as a standalone unit within DPMC, transferring responsibility for cyber security policy from the then-Ministry of Economic Development [CAB Min (12) 8/2A]. The NCPO has counterpart policy teams with whom it works very closely in central agencies in Australia, Canada, the United Kingdom, and the USA.

10. The NCPO is currently headed by a Director, Paul Ash, and has a staff of seven. The NCPO sits within DPMC's Security and Intelligence Group, reporting to Howard Broad as DPMC's Deputy Chief Executive, Security and Intelligence.

11. Cyber security policy is a cross-portfolio issue. The NCPO:

- Leads the development of policy advice for the government on cyber-security and advises on investing government resources in cyber-security activities.
- Oversees the development, implementation and review of national strategies and policies on cyber-security.
- Leads international engagement on cyber policy.
- Facilitates engagement with the private sector on cyber-security issues.
- Manages the Connect Smart partnership and awareness programme (connectsmart.govt.nz).

12. The NCPO is responsible for leading and overseeing the implementation of *New Zealand's Cyber Security Strategy 2015,* and delivering the Government's cyber security priorities (discussed in more detail in the following section).

13. The NCPO works closely with a wide range of other government agencies, including the following:

- The *GCSB*, which provides advanced cyber-security services to organisations of national significance.
- *New Zealand Police*, in dealing with cybercrime (particularly the Police Cybercrime Unit).
- *New Zealand Security Intelligence Service,* including in its role delivering the Protective Security Requirements.
- The *Ministry of Justice* as the lead agency on justice-related policy.
- The *Ministry of Business, Innovation and Employment* (MBIE) as the lead on communications policy and the initial home of the forthcoming New Zealand CERT (discussed further below).
- The *Department of Internal Affairs* as the home of the Government Chief Information Officer, the Anti-Spam team (Electronic Messaging Compliance Unit) and Censorship Compliance Unit.
- The *Ministry of Foreign Affairs and Trade* in engaging on international cyber security policy issues.
- The *Ministry of Defence* and the *New Zealand Defence Force (NZDF)* on defence-related cyber policy issues.

New Zealand's Cyber Security Strategy 2015

14. New Zealand released its first national cyber security strategy in 2011. In November 2015, Cabinet approved a refreshed Cyber Security Strategy (the Strategy) which provides a framework for government agencies, working in partnership with the private sector, to address the cyber threats facing New Zealand. A short summary of the Strategy has been appended to this briefing.

15. The Strategy's vision is to achieve "a secure, resilient and prosperous online New Zealand". The Strategy sets out goals under four headings:

16. The Strategy also puts forward the following four principles for assessing existing actions and developing new ones.

- Partnerships are essential
- Economic growth is enabled
- National security is upheld
- Human rights are protected online

17. These principles – in particular the commitment to work in partnership - underpin all of the actions in the Strategy. The Strategy is accompanied by an Action Plan and a National Plan to Address Cybercrime. The Action Plan has seventeen actions across the four goals. These are whole-of-government actions, designed to protect the country's information technology systems and to ensure New Zealanders can make the most of being online.

18. The Action Plan will be reported on annually by the NCPO, including recommendations on potential adaptations or changes to the Plan. The NCPO is currently developing the first annual report on the implementation of the Action Plan. The report was delayed by the Kaikoura earthquake in November 2016 but will be ready for Cabinet consideration in early 2017. It will provide a comprehensive update on progress against the items in the Action Plan,

measures of success, and outline next steps. We would be pleased to discuss the report with you.

Key initiatives

19. The Action Plan includes a wide-ranging suite of actions, with the following initiatives prioritised in 2016.

- Delivering New Zealand's first Cyber Security Summit. The Summit was held in Auckland on May 5 2016, with a theme of "Keeping New Zealand's Economy Cyber Secure". The Minister for Communications hosted the Prime Minister, chief executives, board chairs, and leaders from across the public and private sector in a day that included a series of keynote speakers and workshops. The workshops garnered meaningful input and feedback on key initiatives from the Action Plan.

- Funding of $22.2 million over four years was allocated in Budget 2016 to build a national CERT (a computer emergency response organisation). [redacted] It will initially be set up as a branded unit within MBIE, reporting to the Minister for Communications. Consideration by Cabinet of CERT NZ's longer-term organisational form, including how it can best be configured to work in partnership with the private sector, is scheduled for the end of 2017. The CERT will have the following functions: incident response and triage; situational awareness and information sharing; advice and outreach; international collaboration; coordination of serious cyber incidents.

  [redacted]

- A public-private sector taskforce has been set up to address the shortage of cyber security skills in New Zealand. A level 6 cyber security diploma will be developed, with a second year programme involving industry internships. A secondary school programme will position students for the diploma. The qualification should be developed in time for teaching in Semester 2, 2017. The taskforce has also been tasked with reporting back to you on other initiatives to grow the cybersecurity workforce.

- Work is underway to establish a "cyber credentials" scheme to help small businesses to improve their cyber security. A joint DPMC/MBIE/Westpac team is using a 12 Week Accelerator called Lightning Lab, working out of the Innovation Hub Creative HQ, to develop the cyber credentials platform and products. At Week 6, the team has developed a minimum viable product and is testing it with SMEs and ICT security firms in the market.

  [redacted] The team will bring an investable proposal back to the IaaS Fund (and to you) in March 2017.

Other elements of the Strategy

20. Addressing cybercrime is also a priority (and one of the Strategy's four goals). This will require resources to ensure Police have the operational capability to deal with cybercrime and to assess whether current legislative settings are fit-for-purpose in relation to cybercrime. It is proposed that New Zealand consider the requirements to accede to the Council of Europe Convention on Cybercrime.

[redacted]

21. Other elements of the Strategy include NZDF cyber defence capabilities; exercises to test preparedness to deal with a major cyber incident; the on-going Connect Smart partnership and cyber capability campaign;[7] improving the security of government information through the Protective Security Requirements and secure use of information communication technologies; and international collaboration, including with Five Eyes partners. The Strategy also includes a goal and actions to manage the international aspects of cyber security policy, working with MFAT.

22. At their February 2016 meeting, the Prime Ministers of Australia and New Zealand agreed to cooperation on cyber exercises, developing cyber skills, cyber security awareness campaigns and other practical initiatives to improve cyber security. Officials hold a six-monthly policy dialogue with Australian counterparts. A key focus of the December 2016 Australia-New Zealand Cyber Dialogue – held last week – was on ways to realise these commitments. Officials developed new initiatives for announcement in the joint Prime Ministerial statement in February 2017. A table top cyber security exercise was also held as part of the Dialogue.

Immediate priorities

23. We think your immediate priorities may include:

- taking the first annual report on the Action Plan to Cabinet in February 2017;
- considering a report-back on a roadmap of measures to build cyber-security skills before the end of March 2017;
- considering the outputs of the cyber credentials development process; and
- considering the NZDF's cyber capabilities;
- a report in the first quarter of 2017 by the NCPO that will provide initial policy work on cyber security issues raised by the Internet of Things.

24. The first annual report on the implementation of the Strategy– as envisaged when the Strategy was adopted - will also provide an initial opportunity to consider new and revised cyber security initiatives. We expect there will also be a range of opportunities to continue to connect cyber security policy with work programmes underway elsewhere in government, including in MBIE (for example on innovation and the digital economy).

---

7 Connect Smart is the government's cyber security awareness-raising and capability-building campaign. It is a public-private collaboration, relying in part on sponsorship from the private sector. See www.connectsmart.govt.nz