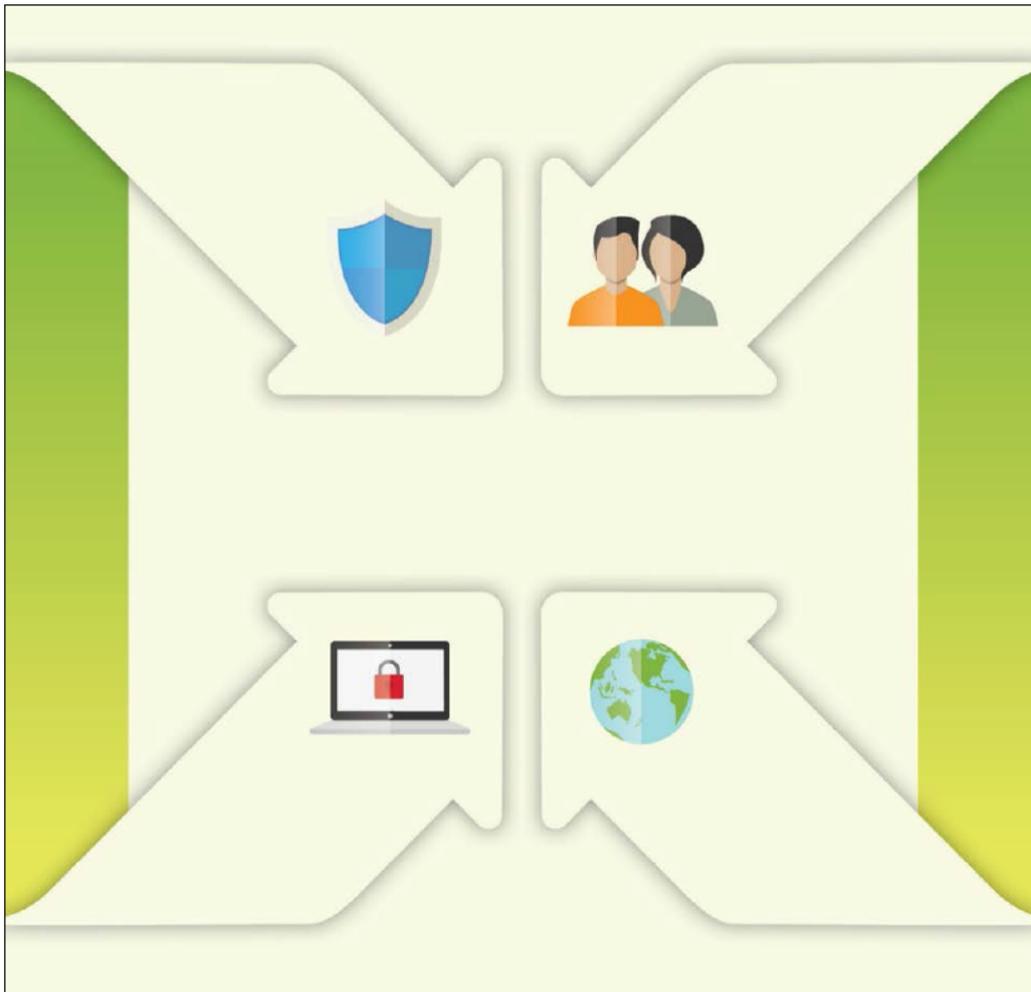




Briefing to Incoming Minister responsible for cyber security policy



Date

30 October 2017

Priority

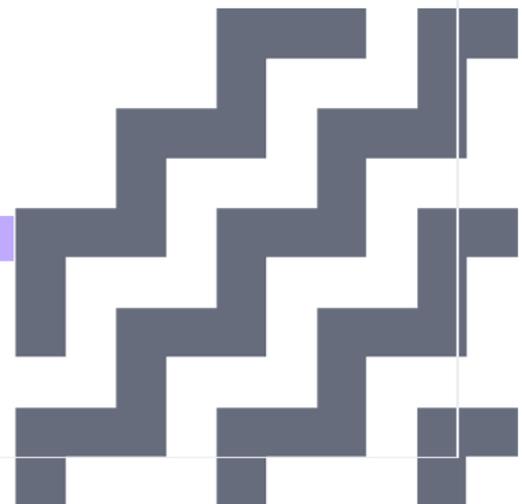
Routine

Security Classification

UNCLASSIFIED - previously Restricted

Tracking Number

3999201





Welcome and introduction

Welcome to your role as the Minister responsible for cyber security policy.

New Zealand's national security and economic growth depends on securing and protecting our most significant information assets. 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 cyber threats.

The National Cyber Policy Office (NCPO) within the Department of the Prime Minister and Cabinet (DPMC) leads the development of cyber security policy advice and provides advice to Government on investing in cyber security activities. It oversees the implementation of *New Zealand's Cyber Security Strategy* (the Strategy) and accompanying *Action Plan 2015* (the Action Plan).

Together, the Strategy and the Action Plan provide the current framework for the government and the private sector to improve the country's cyber security.

Good progress has been made, with the stand-up of CERT NZ, 'Connect Smart' public-private sector collaboration, work to build a cyber-security workforce, assistance to small businesses through a Cyber Credentials scheme, the roll-out of the Government Communications Security Bureau's malware detection and disruption services for organisations of national importance, protective security requirements for government agencies, and a range of international engagement.

But the threat trajectory is rapidly evolving and we will need to accelerate the pace of our response.

This briefing provides you with the key information you may require in your role as the Minister responsible for cyber security policy. It recommends a review of the Action Plan, and outlines three main priorities relating to the opportunities of a vibrant cyber security eco-system; ^{s6(a)} [REDACTED]; and the need to lift the government's capability to deal with cybercrime.

We look forward to working with you to advance a secure, resilient and prosperous online New Zealand.

Recommendation

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

- 1 Note the contents of this briefing.

NOTED



Andrew
Kibblewhite

Paul Ash

Chief Executive

**Director, National Cyber
Policy Office**

**Minister for
Communications**

Date: / /2017

Date: 30 / 10 /2017

Date: / /2017



Contents

- Briefing to Incoming Minister responsible for cyber security policy 1
- Welcome and introduction 2
- Recommendation** 3
 - 1. Overview 5
 - 2. Your responsibilities regarding cyber security policy 5
 - 3. The role of the National Cyber Policy Office 6
 - 4. New Zealand’s Cyber Security Strategy 2015 and Action Plan..... 7
 - 5. There is an upward trajectory of cyber threats 8
 - 6. It is timely to refresh the Action Plan 9
 - 7. Top three priorities 10
 - 8. The role of other government agencies..... 13
 - The cyber security landscape 14
- 9. Conclusion 14
- Appendix A: Additional actions 2017-2020 15



1. Overview

This briefing:

- a. explains how the National Cyber Policy Office (NCPO) within the Department of the Prime Minister and Cabinet (DPMC) can support you as Minister responsible for cyber security policy;
- b. sets out the New Zealand Cyber Security Strategy and Action Plan as the existing framework for government on cyber security;
- c. describes the increasing cyber threat trajectory;
- d. recommends the refresh of the Action Plan in the face of this increasing threat;
- e. outlines the most significant priorities;
- f. defines the cyber security roles of other government agencies; and
- g. signals a range of existing actions and initiatives for the 2017-20 period.

2. Your responsibilities regarding cyber security policy

Ministerial responsibility for cyber security policy

To date, the Minister for National Security and Intelligence has overall responsibility for cyber security policy. The previous Prime Minister allocated formal Ministerial responsibility for cyber security policy (and CERT NZ¹) to the Minister for Communications.

Other Ministers involved in cyber security issues

On cyber security, you will work closely with:

- the Minister of National Security and Intelligence;
- the Minister Responsible for the Government Communications Security Bureau (GCSB);
- the Minister Responsible for the NZ Security Intelligence Service (NZSIS); and
- the Minister of Foreign Affairs and Trade.

¹ CERT was once an acronym for “computer emergency response team”. Since 1997, CERT has been a registered trademark owned by Carnegie Mellon University and is no longer used as an acronym. CERT NZ was set up in April 2017 to receive reports of cyber incidents, analyse threats, share information and advice, coordinate incident responses and be a point of contact for the international CERT community.



Given cyber security is a cross-cutting issue, you will also have close engagement with a range of other Ministers, including the:

- Minister of Justice;
- Minister of Police;
- Minister of Internal Affairs;
- Minister of Defence;
- Minister for Communications; and
- Minister for Economic Development.

Section 8, below, discusses the role of government agencies involved in cyber security.

3. The role of the National Cyber Policy Office

Since 2012, the NCPO, within DPMC, has led the development of cyber security policy advice for the government and advised the government on its investment of resources in cyber-security activities.

The NCPO formally reports to you on cyber security policy matters, in consultation with other Ministers as appropriate.

The NCPO works closely with counterpart policy teams in central agencies in Australia, Canada, the United Kingdom, and the United States – known collectively as the ‘Five Eyes’². It also conducts broader international engagement and outreach with the private sector on cyber security policy, particularly through the ‘Connect Smart’ public-private partnership³.

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

The NCPO chairs the monthly inter-agency Cyber Policy Group which involves agencies such as Government Communications Security Bureau; NZ Security Intelligence Service; NZ Police; CERT NZ; Ministry of Business, Innovation and Employment; Ministry of Justice; Ministry of Foreign Affairs and Trade; Department of Internal Affairs; Ministry of Defence; and New Zealand Defence Force.

² ‘Five Eyes’ refers to the intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

³ ‘Connect Smart’ is a public-private collaboration to drive cyber security improvement in New Zealand. It includes a growing network of banks, telecommunication companies and Internet Service Providers, ICT companies, software companies, social media, retail organisations, education institutions, non-government organisations, community groups, sectoral bodies, business associations and government agencies.

The Cyber Policy Group is the key 'clearing house' to track progress, discuss initiatives and assess the overall direction of the New Zealand cyber security eco-system. This inter-agency collaboration has been, and in our view, remains essential to cyber security efforts. Given New Zealand's size, our ability to collaborate should be a point of advantage for the country.

The NCPO oversees the implementation of the current *New Zealand Cyber Security Strategy* and accompanying *Action Plan 2015*.

4. New Zealand's Cyber Security Strategy 2015 and Action Plan

New Zealand's Cyber Security Strategy (the Strategy) and accompanying *Action Plan 2015* were approved by Cabinet in November 2015 [NSC-15-Min-0012]. The Strategy has provided the framework for coordinated cross-government efforts, in partnership with the private sector, to address cyber threats facing New Zealand.

The Strategy sets a **vision** of 'A Secure, Resilient and Prosperous Online New Zealand'. A range of government agencies contribute to each of the **four goals** of the Strategy (the goals are illustrated below).

The **Action Plan is a living document**, assessed annually as part of a strategic policy process. Flexibility has been built into the Action Plan to enable adaptation to the rapidly evolving threat environment and changes in technology. Actions can be dropped, amended or added, including to reflect learning about what works and what does not.



5. There is an upward trajectory of cyber threats

There is an upwards trajectory of cyber threats affecting New Zealand. An increasing number of New Zealand individuals, businesses and organisations are being affected by cyber incidents.

This year we have dealt with the implications for New Zealand ^{s6(a)} [REDACTED]
[REDACTED]
[REDACTED] the Wannacry ransomware (May 2017); and the notPetya ransomware (June 2017).

- **National Cyber Security Centre (NCSC):** 396 cyber incidents recorded in 2016-17 – an average of 33 per month.
- In the 2016-17, the NCSC worked with 33 public sector and 57 private sector organisations in relation to cyber incidents.
- **CERT NZ:** 364 cyber security incidents were recorded in its first three months (April – June 2017), involving direct financial losses of over \$730,000.

New Zealand's experience is not unique – it reflects a serious and growing international problem. Globally, there is growing use of cyber tools by state-sponsored cyber actors to pursue geo-political advantage. This might be aimed at strengthening influence, stealing commercially valuable information, undermining, or embarrassing other states, creating chaos and disruption, retaliating for the actions of other states, practicing techniques, or pre-positioning for future advantage.

Cyber threat actors – state-sponsored or criminally-motivated – are acting in increasingly bold, brazen, and disruptive ways. Their intent may not always be evident but it is clear that these cyber threat actors are taking advantage of weaknesses in others' systems. It is often difficult to attribute responsibility for cyber incidents.

For example:

- October 2017: Yahoo reveals that 3 billion user accounts were breached back in 2013 (three times more than the 1 billion announced in December 2016).
- September 2017: Equifax (United States credit agency) suffers data breach affecting 145 million US customers.
- 2016: Foreign, likely state-sponsored, threat actors compromise the network of a New Zealand organisation and use its infrastructure to mount a significant cyber-attack on a foreign organisation.
- 2016: Reports of Russian interference in the United States 2016 elections.
- 2015: Theft of 21 million personnel details from the United States Office of Personnel Management (attributed in the media to Chinese espionage).

- 
- Mid-2017: compromises of national energy systems, including UK and Ireland, and US nuclear power plants.
 - December 2015 and December 2016: Ukraine power grid outages as a result of cyber incidents.

This 'new normal' is an environment where cyber threat actors take covert action against others that, while it may be an unfriendly and damaging act, often falls short of interpretation as an 'act of force' or 'intervention in a state's domestic affairs'. This 'grey area' activity poses an increasing challenge to the ability of governments to deliver security services to their economies and citizens.

Technological advances – in encryption, artificial intelligence, machine learning, and the Internet of Things⁴ – will make the threat environment more challenging.

For example:

- October 2016: Massive Distributed Denial of Service (DDoS)⁵ attack affected access to popular websites such as Twitter, Spotify, Amazon, Reddit, Tumblr, PayPal, Netflix, Airbnb, on the East Coast of the United States. The DDoS was spread by infected Internet of Things (IoT) devices, such as video cameras, CCTV cameras and digital video recorders.

6. It is timely to refresh the Action Plan

The Strategy has provided a clear framework for cross-government work on cyber security and raised the profile of collaboration with the private sector. Solid progress has been made towards implementation of the Action Plan.

The Strategy has emphasised the importance of enabling New Zealand's economic growth through cyber security. The intent of the Strategy is to position New Zealand as one of a small group of relatively cyber secure nations that are safe, attractive business destinations, and where New Zealand businesses can seize considerable opportunities, based on their cyber security capability.

We consider the Strategy remains a valuable and robust framework consistent with 'best practice' strategies developed by like-minded countries (Australia, Singapore,

⁴ The Internet of Things (IoT) is the inter-networking of devices – enabling devices to collect and exchange data, be controlled remotely, communicate between devices, and connect to the Internet. For example, it can include vehicles, wearable devices, smart electricity meters, smart homes with automated devices such as lighting or heating, industrial systems and sensors, and devices such as digital video recorders and Internet-connected cameras.

⁵ A 'Distributed Denial of Service' (DDoS) is when a perpetrator attempts to make an online system unavailable by overwhelming it with traffic from multiple sources. The targeted machine, website, or network resource is flooded with superfluous requests, which overloads the system, forcing it to slow down or even crash and shut down, thereby denying service to legitimate users of the system.

Netherlands, and United Kingdom). It would, however, be timely to take a fresh look at the Action Plan to test whether New Zealand is investing the right resources in the right ways across intelligence, protective security, military, law enforcement and civilian agencies to make the greatest difference (i.e. improvement) to our cyber security. It would also be useful to continue seeking ways to enable the public and private sectors to collaborate closely on this challenge.

Based upon recent experience, we consider there is a need to accelerate the tempo of our response to cyber threats; otherwise New Zealand could run the risk of becoming increasingly vulnerable to cyber intrusions at the expense of our security and economy. Our Five Eyes partners, and other like-minded states, have already intensified their cyber security efforts, and continue to do so.

We note that under the Electronic, Communications and Digital Defence section of the New Zealand Labour Party's Defence Policy, a 'comprehensive review of the integrity and efficiency of our electronic communications and digital infrastructure' is proposed. We look forward to engaging with you on your priorities for this review.

7. Top three priorities

In refreshing the Action Plan, NCPO considers there are three areas for priority attention. Additional on-going actions and initiatives for the 2017-20 period under each of the four goals are listed in Annex A. We will engage with you at an early stage to seek your agreement on these priorities.

- i. Seizing the opportunities provided by a **vibrant cyber security eco-system**, which is an enabler of economic growth, a lucrative sector in its own right, and essential to building cyber resilience.
- ii. s6(a) [REDACTED]
- iii. Lifting the government's capability to **deal with cybercrime**, including through NZ Police resources and accession to the Council of Europe Convention on Cybercrime (known as the 'Budapest Convention').

Priority 1: A vibrant New Zealand cyber security eco-system

Cyber security is a **horizontal industry** in that it underpins economic activity across most sectors. It is essential in order for the economy to realise the estimated \$34 billion⁶ and \$2.2 billion⁷ potential gains from better embracing digital tools and the Internet of Things, respectively.

⁶ Sapere Research Group (commissioned by the Innovation Partnership), 'The Value of Internet Services to New Zealand Businesses', 31 March 2014:
<http://innovationpartnership.co.nz/app/uploads/2016/07/The-Value-of-Internet-Services-to-NZ-Businesses.pdf>

⁷ NZ Internet of Things Alliance, 'Accelerating a Connected New Zealand', April 2017:
<http://iotalliance.org.nz/report/>



Cyber security enables the delivery of more digitised government services, and it helps to make New Zealand a more attractive destination for doing business, collaborating on research, and storing and processing data.

Cyber security is also a **vertical industry** in that there is an opportunity for New Zealand cyber security businesses to export into a lucrative international market. The global cyber security market is worth US\$126 billion and is expected to double over the next 10 years⁸. New Zealand is well-placed to be a trusted exporter of cyber security services, with a number of companies already globally competitive.

We can learn from similar-sized states with which we work closely in other contexts (e.g. Digital 5⁹, Advanced Small Advanced Economies Initiative¹⁰), such as Israel and Singapore.

Possible opportunities include leading a delegation of New Zealand cyber businesses to the world's largest cyber conference in Silicon Valley in April 2018; developing a trans-Tasman cyber security research alliance; improving the seeding of cyber security and related start-ups by supporting incubators and accelerators; and working with New Zealand Trade and Enterprise to develop a compelling New Zealand Inc. narrative around promotion of digital security exports (a 'digital 100% Pure').

We also see merit in considering the possibility of a second national Cyber Security Summit to cement public and private sector collaboration in this area.

We will seek your guidance on these initiatives.

s6(a)



⁸Australian Cyber Security Growth Network, 'Cyber Security: Sector Competitiveness Plan', April 2017: <https://www.acsgn.com/cyber-security-sector-competitiveness-plan/global-outlook-cyber-security/>

⁹ The Digital Five is a network of leading digital governments involving Estonia, Israel, Republic of Korea, United Kingdom and New Zealand.

¹⁰ The Small Advanced Economies Initiative was established by New Zealand in 2012 to focus on the challenges and opportunities in an increasingly inter-connected and competitive global economy. It involves Denmark, Finland, Israel, Singapore and New Zealand.

s6(a)

Priority 3: Improved capability to deal with cybercrime

The third goal of the Strategy is about improving New Zealand's ability to prevent, investigate and respond to cybercrime. This is elaborated in the National Plan to Address Cybercrime. We can do more to address cybercrime by allocating resources and specialised training for law enforcement, ensuring that legislation is fit for the digital age and leveraging international relationships to fight cybercrime.

There is a talented Cybercrime Unit within NZ Police's High-Tech Group ^{s6(c)}

International cooperation between law enforcement agencies is essential for responding to cybercrime. NZ Police is active in the Five Eyes Law Enforcement Group. ^{s9(2)(f)(iv)} there would be value in considering NZ Police representation in key international cybercrime units such as the European Cybercrime Centre within Europol and the International Cybercrime Coordination Cell within the Federal Bureau of Investigation.

Unlike our 'Five Eyes' partners, we have not yet acceded to the **Council of Europe Convention on Cybercrime (known as the Budapest Convention)**. The Convention addresses Internet and computer crime by harmonising national laws, improving investigative techniques and cooperation among nations. Accession would be an enabler for NZ Police's operational work with the European Cybercrime Centre (EC3) within Europol, and the International Cybercrime Coordination Cell (IC4) within the FBI.

The Convention requires States to adopt measures enabling law enforcement agencies to order preservation of computer data for up to 90 days. This is one of the main barriers to New Zealand acceding to the Convention. Work underway in the



context of the Ministry of Justice and Law Commission joint review of the Search and Surveillance Act 2012 may be relevant.

With your support we will continue to work closely with NZ Police on their prioritisation of resources for addressing cybercrime, s9(2)(f)(iv) and to work with the Ministry of Justice on considering accession to the Budapest Convention – which will require Cabinet consideration.

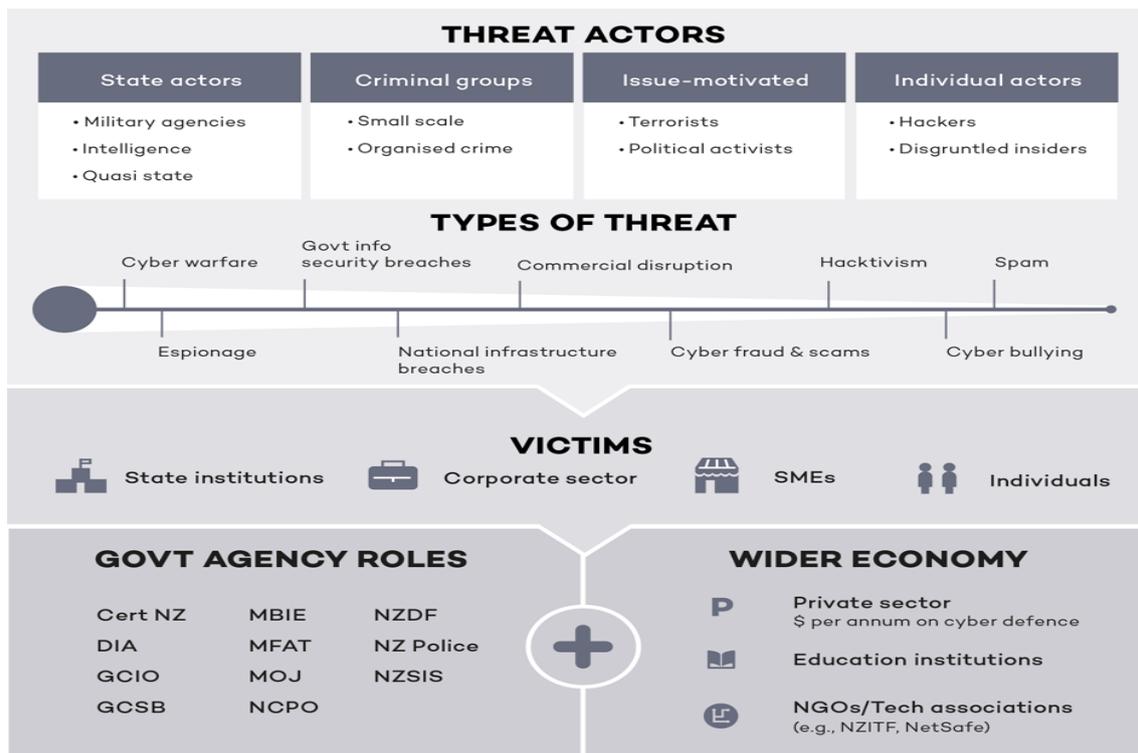
8. The role of other government agencies

Cyber security issues intersect with the work of a wide range of other government agencies including in the areas of national security and intelligence, defence, international relations, trade and economic development, criminal justice, government digitalisation, and public service delivery:

- The **GCSB**, through the **National Cyber Security Centre** (NCSC), responds to and mitigates cyber threats and provides defensive cyber threat services to public and private sector organisations of national significance. It delivers cyber threat intelligence to customers and partners. GCSB information assurance activities include providing high-grade encryption services to protect classified information and assessing proposed outer space and high altitude activity and changes to telecommunications networks for risks to national security. It also provides information assurance and security guidance to government agencies including through the Information Security Manual, which is an integral component of the Protective Security Requirements.
- The **New Zealand Security Intelligence Service** (NZSIS) delivers the Protective Security Requirements, which includes information security, for government agencies.
- **New Zealand Police** addresses cybercrime (particularly through the Police Cybercrime Unit within the High Tech Group), which is one of the four goals of the *Cyber Security Strategy*.
- The **Ministry of Justice** (MOJ) works on the rule of law and justice sector policy, including oversight of the *Harmful Digital Communications Act 2015* and the review of the *Privacy Act 1993* – the latter includes proposals on data breach reporting.
- The **Ministry of Business, Innovation and Employment** (MBIE) links with cyber security in the areas of communications policy, the Digital Economy Work Programme, research and innovation, consumer advice, and support for small businesses. MBIE advises the Minister for Communications on the implementation of the Telecommunications (Interception Capability and Security) Act 2013, which sets out the obligations of the communications industry in relation to legal interception and network security.
- **CERT NZ** receives reports of cyber incidents, analyses threats, shares information and advice, coordinates incident responses, and is a point of contact for the international CERT community. CERT NZ has been set up, initially, as a branded business unit within MBIE.

- The **Department of Internal Affairs (DIA)** is the home of the Government Chief Digital Officer – the functional lead for the government’s information communications technology strategy. The Department of Internal Affairs includes the Electronic Messaging Compliance Unit (anti-spam) and Censorship Compliance Unit.
- The **Ministry of Foreign Affairs and Trade (MFAT)** works jointly with NCPO on cyber security diplomacy, including cyber security dialogues with other countries, advancing norms of state behaviour online, and addressing barriers to trade arising from other countries’ cyber security regulations. International cooperation is one of the four goals of *New Zealand’s Cyber Security Strategy*.
- The **Ministry of Defence (MOD)** and the **New Zealand Defence Force (NZDF)** are focused on the cyber protection of the NZDF networks and deployed operations as well as the long term structure for raising, training and sustaining cyber capabilities. MOD and NZDF also work with NCPO on policy issues relating to the use of cyber operations in a military context.

The cyber security landscape



9. Conclusion

Our core message to you is that cyber security is critical to ensuring New Zealand can realise the benefits of connectivity and digital innovation. In the face of increasing cybercrime and malicious cyber activity, we propose to intensify New Zealand’s responses through a refreshed Action Plan. We look forward to engaging with, and supporting you on this proposed programme of work.

Appendix A: Additional actions 2017-2020

Under the existing Action Plan, some actions have been completed (notably the establishment of CERT NZ), some actions are underway, some actions may need amending or updating, and we may need to consider new actions. The following sets out on-going actions and initiatives in the 2017-20 period under each of the four goals.



Goal 1: Cyber Resilience: New Zealand's information infrastructures can resist cyber threats and we have the tools to protect our national interests.

- **CERT NZ** was established in April 2017 with funding of \$22.2 million over four years [EGI-16-Min-0086]. In order to be set up quickly with organisational support, CERT NZ was established as a branded business unit within the Ministry of Business, Innovation and Employment (MBIE).
 - Cabinet deferred decisions on the longer-term form until CERT NZ was operational and stakeholders were consulted. Cabinet is due to consider the future form of CERT NZ by December 2017.
 - CERT NZ is currently funded for 7am to 7pm Monday-Friday operations. It has indicated that future consideration of 24/7 operations may be necessary, in response to public expectations.
- GCSB's National Cyber Security Centre has completed the roll-out of **Project CORTEX**, delivering malware detection and disruption services to a select group of public and private sector organisations of national importance. It is now working to scale the benefits of operating these services to a larger pool of nationally significant organisations through direct customer engagement and wider dissemination of threat reporting via a customer portal and information security exchanges.
 - The GCSB is developing a **Malware Free Networks initiative**, following a 12 month pilot as part of the CORTEX project. Cabinet is expected to consider the scaling of Malware Free Networks in December 2017. This is an important technical initiative with the prospect of significantly improving the protection of a broader set of organisations of national significance.
- A **major cyber security exercise** is planned to test the *Cyber Security Emergency Response Plan* (as part of the National Exercise Programme within the National Security System). The aim is to ensure that our response systems are effective and ready in the event of a major cyber incident which disrupts

government organisations or other organisations of national significance. Current planning envisages that you will be involved in the exercise; we will follow up on this with your office.

- NCPO is working alongside the private sector-led Internet of Things Alliance to assess the security challenges arising from evolving technology, such as the **Internet of Things (IoT)**. We will work with you as we consider how to address the security challenges of the IoT and other emerging technologies.



Goal 2: Cyber Capability: New Zealanders, businesses and government agencies understand cyber threats and have the capability to protect themselves.

- Small businesses play a huge role in New Zealand's economic growth – but often do not have the skills or resources to protect their business information and remain cyber secure. We have developed a business model for a **Cyber Credentials scheme to assist small businesses** and are in the process of testing market interest and selecting a private sector provider(s) to deliver this programme. Once a provider is selected, we expect to see the scheme rolled out with benefit for the cyber security of New Zealand's small businesses.
- There is a shortage of **cyber security professional expertise in the workforce**, which means that businesses and organisations do not have the technical staff to carry out cyber security improvements. A Cyber Security Skills Taskforce (nine private sector and education sector representatives) was set up in November 2016 to take practical actions to address this shortage.
 - A new Level 6 cyber security qualification will be launched for uptake in 2018.
 - Work is underway on other initiatives to expand the cyber security skills pipeline to the workforce. We will seek your advice on priorities and next steps.
- Protective Security Requirements (PSR), incorporating information security, are mandated for 35 government agencies. At a system level, following two years of assurance reporting, there has been strong capability improvements in personnel and physical security – s6(a) [redacted]
[redacted] A process is underway to improve the settings for government information security.

s9(2)(f)(iv), s9(2)(g)(i) [redacted]

s9(2)(f)(iv), s9(2)(g)(i)

• s6(a), 9(2)(j)



Goal 3: Addressing Cybercrime: New Zealand improves its ability to prevent, investigate and respond to cybercrime.

- See Priority 3 above.



Goal 4: International Cooperation: New Zealand protects and advances its interests on cyberspace issues internationally.

- International work ensures New Zealand is able to advance its interest in a free, open and secure cyberspace; participate in the growing international debate about cyber security threats; and promote norms of acceptable state behaviour online. We foresee an increasingly fractious environment for this work, given recent developments. We may need to step up our effort in this area, working in conjunction with MFAT and other agencies. We will identify opportunities for you to participate in international cyber security events, and support you to engage on cyber security issues during your international travel and meetings with foreign counterparts.
- There is an opportunity for you to attend the **Global Conference on Cyberspace, New Delhi, 22-23 November 2017**. This is the primary international forum for engaging on Internet governance: it would provide an occasion for you to interact with your international counterparts on cyber security issues. The Conference is an avenue for New Zealand to underline its commitment to an open, free and more secure cyberspace, and to express strong support for the development of norms of acceptable state behaviour



online, based on the application of existing international law. The Minister for Communications led New Zealand's delegation to the Global Conference in Budapest in 2012, followed by the Minister for Commerce and Consumer Affairs in The Hague in 2015.

- New Zealand engages regularly with '**Five Eyes**' partners at the policy, intelligence, CERT, law enforcement and defence levels.
- We have close connections with **Australia** on cyber security. Prime Ministers have committed to cyber security cooperation in their Annual Joint Statements. s6(a)
[Redacted text block]
- There are regular dialogues with Singapore, India (to be held in November) and Japan (timing to be confirmed).
- The second New Zealand-**China** cyber security dialogue was held in September 2017. The dialogue builds bilateral policy and operational relationships s6(a)
[Redacted text block] We will continue to work with Chinese officials regarding China's new cyber security and cross-border data transfer regulations which affect New Zealand businesses.
- Further work is required to enable New Zealand exporters to meet increasingly onerous 'behind the border' cyber security requirements, as states and sector groups seek to regulate for security outcomes.