Department of the Prime Minister and Cabinet

Minister of Broadcasting, Communications and Digital Media Weekly Reports 25 May – 29 June 2018

To increase transparency and open government, the Minister of 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 of weekly reports (25 May – 29 June 2018) 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.

Dates: 25 May 2018
1 June 2018
8 June 2018
15 June 2018
22 June 2018
29 June 2018

Title: National Cyber Policy Office: Weekly Reports.

Information withheld with relevant section(s) of the Act:
s 6(a) –security or defence of NZ or international relations
s 6(c) – maintenance of the law
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
s 9(2)(j) – carry on, without prejudice or disadvantage, negotiations.

~~RESTRICTED~~

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

Date:	25 May 2018	**Priority:**	Routine

National Cyber Policy Office: Weekly Report

Part 1: **Issues requiring your direction**

Part 2: **Action Plan update**

Part 3: **Cyber security news this week**

Part 4: **Briefs, Cabinet Papers, OIAs and Ministerials**

From:

Paul Ash
Director
National Cyber Policy Office
s9(2)(a) [redacted] (A/H)

Heather Ward
Principal Adviser and Acting Team Leader
National Cyber Policy Office
s9(2)(a) [redacted] A/H)

Recommendation:

1 **Agree** that, once this weekly report has been considered by you, the National Cyber Policy Office release the report in full at the end of June (aside from the contact details of officials which will be withheld under OIA 9 (2) (a)).

Yes../ No

Hon Clare Curran
Minister of Broadcasting,
Communications and Digital Media

.

... / 05 / 2018

Part 1: Cyber Security Strategy Refresh

1.1 Refresh of the Cyber Security Strategy and Action Plan

We are awaiting advice from the Chair of ERS regarding the proposed extension of the report back to Cabinet on the refresh of the Cyber Security Strategy to the end of October.

The Governance Group will meet on 29 May to provide feedback on the planning for the refresh of the Cyber Security Strategy. Following that, we will provide a full brief to you on the 31 May on the process, the engagement and outreach plan, and the proposed framework for engagement.

Part 2: Action Plan Update

Cyber Resilience:

NEW ZEALAND'S INFORMATION INFRASTRUCTURES CAN RESIST CYBER THREATS AND WE HAVE THE TOOLS TO PROTECT OUR NATIONAL INTERESTS.

2.1 Nil to report.

Cyber Capability:

NEW ZEALANDERS, BUSINESSES AND GOVERNMENT AGENCIES UNDERSTAND CYBER THREATS AND HAVE THE CAPABILITY TO PROTECT THEMSELVES.

2.2 Australia-New Zealand Cyber research and development collaboration

On 30 May the NCPO will participate in a workshop to design a research proposal for the Australia-New Zealand Cyber Security Research partnership, announced in February. The workshop will include leading New Zealand and Australian academics in the field of cyber security, officials from the MBIE's international science and innovation team, and Australia's main technology research body Data61. The research will cover two topics: the use of artificial intelligence in attacking and defending vulnerable networks, and the risks and opportunities of quantum computing. The workshop aims to produce a research proposal that will link New Zealand and Australian researchers together to undertake cutting edge research that takes advantage of each countries' unique research specialities. We will report back to you when the research proposal is completed, and next steps for the research are clear.

Addressing Cybercrime:

NEW ZEALAND IMPROVES ITS ABILITY TO PREVENT, INVESTIGATE AND RESPOND TO CYBERCRIME.

2.3 Microsoft Government Intelligence Community Innovation Day

NCPO attended a Microsoft-hosted Government Intelligence Community Innovation Day on 24 May. Microsoft demonstrated some of their Azure cloud based products to highlight the business opportunities that can be realised from the use of Artificial Intelligence solutions. The event focused on the rapid rate of data expansion, which was reported as doubling in size every year, and anticipated to reach 44 zetabytes by 2020. This data growth was the product of millions of deployed sensors. Their presentations demonstrated data was being used to prevent, predict and respond to law enforcement events through real-time analysis of computer aided despatch (CAD), data associated with caller location, number plate recognition, social media postings, tweets and existing case management details.

The morning sessions were concluded with a presentation from the Microsoft General Counsel around ethics and the societal concerns associated with automated collection and processing of big data. The presenter talked about AI liability, the impacts of new legislation such as GDPR, data usage and the need for visibility and transparency for consequential decision making. The goal for AI developers being to ensure their solutions are trustworthy by creating shared principles and an ethical framework. Microsoft has created 6 ethical principles: Treat everyone fairly and avoid biases; reliability of data; compliance with privacy laws; inclusiveness and recognition of the digital divide; and transparency and accountability. The afternoon sessions showcased a platform called Circadence, which provides cybersecurity teams with a platform to practice skills and hone tactics s6(c) [redacted]

International Cooperation:

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY.

Part 3: Cyber Security news this week (abridged clips)

3.1 Pakistan military accused of hacking Australian diplomats

Australian diplomatic security has been compromised after the Pakistani military allegedly hacked mobile phones using spyware developed by a software developer with links to a Sydney company. The hack allowed the military to track the movements of Pakistan-based

Australian diplomats travelling to Balochistan province and its capital, Quetta, according to US-based IT security company Lookout, which uncovered the breach. Both areas are considered high-risk travel zones for Australians, according to the Department of Foreign Affairs and Trade’s smarttraveller site. Lookout uncovered the hacking in January and yesterday warned there may be other data breaches involving the Australian diplomats because only a small amount of compromised material had been analysed. Lookout’s head of threat intelligence, Michael Flossman, a former Australian Defence Department employee, yesterday said Australian law enforcement authorities had been alerted to the breach that also involved diplomats from Britain and the US.

Source: The Australian - Online, 23 May

3.3 UK begins to formalise its legal approach to cyber war

International law wasn't developed with cyber space in mind, but the UK is setting out its legal approach amid tensions with Russia. Just as physically damaging attacks would be breaches of international law, so are cyber attacks which go beyond espionage according to the Attorney General, Jeremy Wright QC. Speaking to the Chatham House think tank, Mr Wright, who is a government minister and an MP for Kenilworth and Southam, emphasised that international law must keep pace with technological change to remain relevant. He said: "If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us." Although this is the first time a government minister has gone on the record about the UK's interpretation of international law in regards to cyber attacks, this interpretation is essentially in line with a UN declaration in 2013.

3.4 Britain 'must be ready to launch cyberattack'

A full-scale cyberattack could cripple a country within minutes, the head of military intelligence is warning. In a rare speech today, Air Marshal Phil Osborn will say that the risk from "very sophisticated" chemical weapons is also growing and that power stations, water supplies and other parts of critical national infrastructure are under threat from new, advanced missiles. Air Marshal Osborn, the chief of defence intelligence, says that Britain needs to be "much more aggressive and to take risks" to counter the range of threats, according to extracts released to The Times of his speech to the Royal United Services Institute. This could include launching cyberattacks. State-based threats, such as those from Russia, "have become more acute", he says, describing a "world that is more dangerous, uncertain and unpredictable". Air Marshal Osborn says that modern warfare is multilayered, with some forms of attack far harder to attribute. These combine the spectrum of non-conventional tactics, including cyber technology, state-sponsored assassinations, and information operations such as using multiple robotic accounts on social media to spread false messages designed to influence a population.

Source: The Times, Deborah Haynes, Friday, 18 May

3.5 North Korea’s Hackers—Many Living Abroad—Have Nabbed It $650 Million

North Korea has gradually become a hacking superpower, and has earned a pretty penny in the process. Agents acting on behalf of the ruling regime have stolen about $650 million through cyberattacks, according to research from Simon Choi, a consultant to South Korea's CIA-esque National Intelligence Service. In a lengthy feature, Winn explains how the North Korean government has rapidly become a world leader in hacking, despite its impoverishment and economic isolation. Since 2011, hackers from North Korea have been implicated in dozens of heists, including a theft of $81 million from Bangladesh's central bank via the Federal Reserve Bank. They are also suspected to have targeted a number of cryptocurrency exchanges in Japan and South Korea. Increasingly, along with North Korea's nuclear weapons prowess, these cyberattacks constitute a threat to international order.

Source: NextGov, 23 May

Part 4: Papers for the Minister (Briefs, Cabinet Papers, OIAs and Ministerials etc)

Status	Type/Title of paper	Comment or purpose	Deadline for Minister's sign-off
Drafting – due 28 May	Brief	Advice on possible visit to Singapore for International Cyber Week (18-20 September 2018)	25 May
Drafting.	OIA 2017/18 - 0500	OIA from Taxpayers' Union to the PM for details about the refresh of the Cyber Security Strategy (costs, number of officials, meetings etc) – one of 75 OIAs from the Taxpayers Union about various reviews.	4 June
✓ Response provided to MBIE for collation	OIA 18-25	OIA from Melissa Lee MP: Part of a broader request. Q12 relates to NCPO: any papers on Pyeongchang Cyber Attack: NIL response	7 June
✓ Response provided to MBIE by 11 May	Brief	Material to be provided to MBIE for Economic Development, Science and Innovation Committee 2018 Estimates Examination hearing on 7 June.	7 June
Drafting – in consultation with CERT NZ – due with Minister's office by 8 June	Brief	Meeting with Internet NZ on refresh of Cyber Strategy and CERT NZ	11.30am, 11 June

Drafting – response to be provided to MBIE for collation and to Minister's office by 11 May.	OIA 18-66	OIA from Melissa Lee for copy of weekly reports from 5 January to April 18	25 June

Committee and Date	**Date due in Minister's Office**	**Title of Paper**	**Comment or Purpose**
Govt Administrative and Expenditure Review Committee, 26 June		A New Approach to Digital Identity	Led by DIA. Considers a digital identity services for citizens and organisations
TBC		s9(2)(f)(iv), s9(2)(g)(i) [redacted]	[redacted]
ERS – 31 October		Refreshed Cyber Security Strategy and Action Plan	

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

Date:	01 June 2018	**Priority:**	Routine

National Cyber Policy Office: Weekly Report

Part 1: **Cyber Security Strategy Refresh**

Part 2: **Action Plan update**

Part 3: **Cyber security news this week**

Part 4: **Briefs, Cabinet Papers, OIAs and Ministerials**

From:

Paul Ash
Director
National Cyber Policy Office
s9(2)(a)
[redacted] (A/H)

Heather Ward
Principal Adviser and Acting Team Leader
National Cyber Policy Office
s9(2)(a)
[redacted] (A/H)

Recommendation:

2 **Agree** that, once this weekly report has been considered by you, the National Cyber Policy Office release the report in full at the end of June (aside from the contact details of officials which will be withheld under OIA 9 (2) (a)).

Yes../ No

Hon Clare Curran
Minister of Broadcasting,
Communications and Digital Media

.

... / 06 / 2018

Part 1: Cyber Security Strategy Refresh

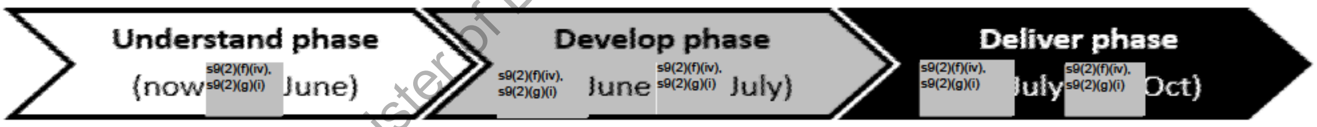
1.2 Refresh of the Cyber Security Strategy and Action Plan

The Chair of ERS has agreed to the extension of the report back to Cabinet to October 2018 [ERS-18-MIN-0010]. We are providing a brief to you today outlining the collaborative and multi-layered approach for the refresh of the Cyber Security Strategy.

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.

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 and resources 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; and the cyber security eco-system involving cyber security skills, research and development, growth of the cyber security sector and the challenges of emerging technology).


Understand phase
(now s9(2)(f)(iv), s9(2)(g)(i) June)
Develop phase
s9(2)(f)(iv), s9(2)(g)(i) June s9(2)(f)(iv), s9(2)(g)(i) July)
Deliver phase
s9(2)(f)(iv), s9(2)(g)(i) July s9(2)(f)(iv), s9(2)(g)(i) Oct)

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) s9(2)(f)(iv), s9(2)(g)(i) [redacted]	Report to Minister summarising insights from engagement and proposing a 'strawman' for the draft refreshed Strategy and Action Plan s9(2)(f)(iv), s9(2)(g)(i) [redacted]	1. Report to Minister summarising insights from engagement, and final draft of refreshed Strategy and Action Plan s9(2)(f)(iv), s9(2)(g)(i) [redacted] 2. Final Cabinet paper s9(2)(f)(iv), s9(2)(g)(i) [redacted]

The first joint engagement activity (workshops) in mid-June straddles the 'discover' and 'define' stages of the 'understand' phase. Workshops will be held in Wellington, Auckland and Christchurch. In the 'understand' phase, we are looking to get an understanding of the breadth of views, interests, experiences and insights into what stakeholders think should could be prioritised.

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 the week of 18 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. It would also be available on the Connect Smart website which will become a key vehicle for communicating progress on the Refresh.

Part 2: Action Plan Update

Cyber Resilience:

NEW ZEALAND'S INFORMATION INFRASTRUCTURES CAN RESIST CYBER THREATS AND WE HAVE THE TOOLS TO PROTECT OUR NATIONAL INTERESTS.

2.1 Nil to report.

Cyber Capability:

NEW ZEALANDERS, BUSINESSES AND GOVERNMENT AGENCIES UNDERSTAND CYBER THREATS AND HAVE THE CAPABILITY TO PROTECT THEMSELVES.

2.2 <u>Australia-New Zealand Cyber Security Research Partnership</u>

On 30 May, New Zealand hosted the first workshop involving cyber security researchers from both Australia and New Zealand. In February, during the Prime Minister's visit to Australia, both Prime Ministers announced Australia-New Zealand collaboration on cyber security research, focused on "post quantum cyber security" and "artificial intelligence for improved cyber security". The collaboration will include joint research projects, and provide for PhD and researcher exchanges. The workshop produced a draft research programme for these topics. This draft programme will be tested by a panel of experts selected by the MBIE international science partnerships team. s6(a) [redacted]

Addressing Cybercrime:

NEW ZEALAND IMPROVES ITS ABILITY TO PREVENT, INVESTIGATE AND RESPOND TO CYBERCRIME.

2.3 International Engagement – Budapest Convention

As a part of NCPO's efforts to determine the requirements for accession to the Budapest Convention, we are engaging with our counterparts in the UK and Canada on their experiences and approach to the Convention. This includes a read-out on their views of the benefits of ratification; the usefulness of the Optional Protocol to the Convention, which covers racism & xenophobia; how mutual assistance to and from international partners changes after accession; and how the 24/7 contact capability required by the Convention works in practice.

International Cooperation:

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY.

Part 3: Cyber Security news this week (abridged clips)

3.1 The EU's Gift to Cybercriminals; Europe's new privacy rule, called the GDPR, already is thwarting security researchers and police.

The GDPR is intended to safeguard EU residents' privacy online. To that end, it effectively puts a wide range of "personal data" under cryptographic lock and key. The fundamental problem is that the regulation explicitly covers the kinds of information critical to law enforcement, such as data that could help investigators track down hackers and the devices they use to cause mayhem online. Take something as basic as the name, physical address and other contact information of the owner for a given website or domain name. Right now those details generally are publicly available in what is called the Whois database, which is maintained by the Internet Corporation for Assigned Names and Numbers, or ICANN. But the GDPR is being interpreted such that Whois data may not be shared without the owner's consent. Unless something is done, police will be robbed of ready access to vital data, drastically impeding their efforts to identify and shut down illicit activity. ICANN has proposed allowing law-enforcement officials to regain access to the information after they go through a lengthy accreditation program. But even that unwieldy plan is facing objections, including criticism from EU regulators that it would inadequately protect data guarded by the GDPR. As a result, the Whois database is likely to go dark for some time.

Source: The Wall Street Journal Online, 28 May

3.2 World News: Cyberattacks Target South Korean Firms --- Strikes began in the lead-up to the inter- Korean summit; Pyongyang suspected

When the North and South Korean leaders vowed on April 27 to cease all hostile acts against each other, many saw it as a turning point in cross-border relations. In the weeks since their agreement, the North ramped up its campaign of cyberattacks on South Korea, launching fresh assaults on financial companies and groups focused on North Korea, according to people familiar with the matter. Early indications, based on the malware and targets, strongly suggest North Korea was the culprit. Among the organizations affected were the Sejong Institute, an independent think tank, and the South-North Sharing Campaign, a left-leaning group that sends aid to North Korea. A spokeswoman for the latter group said South Korean officials had notified it that its website had been breached, but wasn't told who was behind the attack.

Source: The Wall Street Journal, 26 May

3.3 The Cybersecurity 202: The FBI is trying to thwart a massive Russia-linked hacking campaign

U.S. law enforcement is trying to seize control of a network of hundreds of thousands of wireless routers and other devices infected by malicious software and under the control of a Russian hacking group that typically targets government, military and security organizations. In a statement issued late Wednesday, the Justice Department said the FBI had received a court order to seize a domain at the core of the massive botnet, which would allow the government to protect victims by redirecting the malware to an FBI-controlled server. The DOJ attributed the hacking campaign to the group known as Sofacy, also known as Fancy Bear. While the statement did not explicitly name Russia, Fancy Bear is the Russian military-linked group that breached the Democratic National Committee in the presidential election.

Source: Washington Post.com, 24 May

3.4 Peter Dutton touts new cybersecurity powers being considered to protect banking network, power grid

Earlier this month, the Australian Government flatly denied reports that ASD — which operates as part of the Defence Department and primarily eavesdrops overseas — was going to be handed new powers to spy on Australians' electronic data and communications. It was claimed the Defence and Home Affairs departments had been canvassing changing the law to allow the ASD to access emails, banks records and text messages if their respective ministers gave their approval. But while the Government insists it does not plan to snoop on Australians, Mr Dutton has told the ABC's 7.30 that the idea of using ASD to protect critical infrastructure like the banking network, electricity grids or even the emergency triple-0 network is being debated. The Federal Government announced a couple of years ago that it now had both a strong defensive capability in cyberspace, but also an offensive one. That is, that it was able to go out into international networks and attack and disrupt cybercrime. But in the case of ASD, this only occurs in foreign networks.

Source: abc News, 29 May

3.5 The U.S. military combined cyber and kinetic operations to hunt down ISIS last year, general says

The military used cyber-operations alongside more conventional weaponry in an important battle against ISIS last year, a senior U.S. official revealed recently. U.S. Cyber Command, the country’s leading cyberwarfare force, was involved in secretly launching a series of cyberattacks against the terrorist group in 2017 that knocked out its computer systems in Iraq, said Gen. Stephen Townsend, the former commander of the Army’s anti-ISIS coalition. The tactic caused ISIS personnel to leave their heavy command posts, exposing them to attack with kinetic weapons such as missile strikes. The General discussed the covert operation in detail for the first time last week. It’s unclear how often the U.S. military or its allies use such a combination of tactics against enemy forces, and it’s rare for top officials to even discuss such operations.

Source: Cyberscoop, 29 May

3.6 US-CERT issued an alert on two malware associated with North Korea-linked APT Hidden Cobra

The Department of Homeland Security (DHS) and the FBI issued a joint Technical Alert on two strains of malware, the Joanap backdoor Trojan and Brambul Server Message Block worm, associated with the HIDDEN COBRA North Korea-linked APT group.

Source: Security Affairs – 30 May

Part 4: Papers for the Minister (Briefs, Cabinet Papers, OIAs and Ministerials etc)

Status	Type/Title of paper	Comment or purpose	Deadline for Minister's sign-off
Provided 1 June	Brief	Advice on possible visit to Singapore for International Cyber Week (18-20 September 2018)	11 June
Provided to Minister's office 1 June	OIA 2017/18 - 0500	OIA from Taxpayers' Union to the PM for details about the refresh of the Cyber Security Strategy (costs, number of officials, meetings etc) – one of 75 OIAs from the Taxpayers Union about various reviews.	4 June
✓ Response provided by MBIE to Minister's office	OIA 18-25	OIA from Melissa Lee MP: Part of a broader request. Q12 relates to NCPO: any papers on Pyeongchang Cyber Attack: NIL response	7 June
✓ Response provided to MBIE by 11 May	Brief	Material to be provided to MBIE for Economic Development, Science and Innovation Committee 2018 Estimates Examination hearing on 14 June.	7 June
Drafting – in consultation with CERT NZ – due with Minister's office by 8 June	Brief	Meeting with Internet NZ on refresh of Cyber Strategy and CERT NZ	11.30am, 11 June

Drafting – response to be provided to MBIE for collation and to Minister's office by 11 May.	OIA 18-66	OIA from Melissa Lee for copy of weekly reports from 5 January to April 18	25 June

Committee and Date	**Date due in Minister's Office**	**Title of Paper**	**Comment or Purpose**
Govt Administrative and Expenditure Review Committee, 26 June		A New Approach to Digital Identity	Led by DIA. Considers a digital identity services for citizens and organisations
TBC		s9(2)(f)(iv), s9(2)(g)(i) [redacted]	[redacted]
ERS – 31 October		Refreshed Cyber Security Strategy and Action Plan	

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

Date:	08 June 2018	**Priority:**	Routine

National Cyber Policy Office: Weekly Report

Part 1: **Cyber Security Strategy Refresh**

Part 2: **Action Plan update**

Part 3: **Cyber security news this week**

Part 4: **Briefs, Cabinet Papers, OIAs and Ministerials**

From:

Paul Ash
Director
National Cyber Policy Office
s9(2)(a) [redacted] (A/H)

Heather Ward
Principal Adviser and Acting Team Leader
National Cyber Policy Office
s9(2)(a) [redacted] A/H)

Recommendation:

3 **Agree** that, once this weekly report has been considered by you, the National Cyber Policy Office release the report in full at the end of June (aside from the contact details of officials which will be withheld under OIA 9 (2) (a)).

Yes../ No

Hon Clare Curran
Minister of Broadcasting,
Communications and Digital Media

.

... / 06 / 2018

Part 1: Cyber Security Strategy Refresh

1.3 Refresh of the Cyber Security Strategy and Action Plan

We have employed facilitators from KPMG and Thought Partners to assist with the first joint engagement activity during the “understand” phase of the refresh. The workshops will be held in the week of 25 June in Wellington (2 sessions on 26 June), Auckland (2 sessions on 28 June) and Christchurch (one session on 29 June). Invites to the workshops will be sent via our Connect Smart partnership mailing list. CERT NZ and the National Cyber Security Centre (within GCSB) will also forward the invitations to their stakeholders. We are also developing a broader list of stakeholders to be invited.

The aim of the workshops is to gather stakeholder experiences about cyber security, views on future challenges, and thoughts on the opportunities to improve New Zealand’s cyber security. It will enable us to appreciate the breadth of views and interests on the challenge of cyber security.

The Wellington workshops will be held at the Department of Internal Affairs’ Service Innovation Lab on Thornton Quay from 9.00am to midday and from 1.00pm to 4.00pm. If you are available, we recommend that you open the workshop(s) in Wellington. If you agreed, we could also record your opening message and use this in the Auckland and Christchurch workshops.

The ‘joint engagement activity’ workshops will be followed by a further workshop at the Service Innovation Lab to consolidate and analyse the outcomes.

Part 2: Action Plan Update

Cyber Resilience:

NEW ZEALAND'S INFORMATION INFRASTRUCTURES CAN RESIST CYBER THREATS AND WE HAVE THE TOOLS TO PROTECT OUR NATIONAL INTERESTS.

2.1 Nil to report.

Cyber Capability:

NEW ZEALANDERS, BUSINESSES AND GOVERNMENT AGENCIES UNDERSTAND CYBER THREATS AND HAVE THE CAPABILITY TO PROTECT THEMSELVES.

2.2

Addressing Cybercrime:

NEW ZEALAND IMPROVES ITS ABILITY TO PREVENT, INVESTIGATE AND RESPOND TO CYBERCRIME.

2.3 Government response to potential loss of WHOIS information

In the Weekly Report dated 18 May, we reported a potential loss of public access to databases containing WHOIS data, which contains owner registration details of global Top Level Domain (gTLD) names, due to conflict with the European Union's General Data Protection Regulation (GDPR).

Access to this data is an important tool for cyber security practitioners, including agencies responsible for elements of New Zealand's cyber security system such as the New Zealand Police, CERT NZ and Department of Internal affairs. s6(a), s6(c) [redacted]

The International Corporation for Assigned Names and Numbers (ICANN) has suspended enforcement of its model of uniform access to the WHOIS data and announced a "Temporary Specification for gTLC Registration Data". This will require government agencies to approach individual registry operators and registrars to request access for a "legitimate and proportionate purpose" under exceptions established in the GDPR. ICANN has given no indication of when it will restore a uniform system of access.

s6(a), s6(c), s9(2)(f)(iv), s9(2)(g)(i) [redacted]

[redacted]

International Cooperation:

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY.

2.4 US Cyber security developments

On 31 May the office of the Coordinator for Cyber Issues in the US State Department made two recommendations to the President on cyber security. The recommendations are entitled "*Deterring Adversaries and Better Protecting the American People from Cyber Threats*" and "*Protecting American Cyber Interest through International Engagement*".

The cyber deterrence document recommends imposing swift, costly, and transparent consequences on foreign governments responsible for significant malicious cyber activities aimed at harming US national interests. A policy will be created to provide criteria for the types of malicious activities that the US government will seek to deter. It will prepare a menu of options for swift, costly and transparent consequences below the threshold of the use of force. The US will work with partner states to ensure that deterrence activities have greater impact (e.g. intelligence sharing, supporting attribution, public statements etc).

The second document lays out the US vision for cyber space, and its objectives for international cyber diplomacy. The document sets out five objectives: increasing international stability, by promoting norms of acceptable state behaviour online; identifying, detecting, disrupting and responding to malicious cyber actors; upholding human rights and cross border data flows online; maintaining the role of non-government stakeholders in cyberspace, and; advancing an international regulatory environment that protects competition and intellectual property.

Part 3: Cyber Security news this week (abridged clips)

3.1 Long-Awaited Botnet Report Calls on Industry for Solutions

The US federal government should "lead by example" when it comes to ensuring its computers and internet-linked devices aren't hijacked by botnets, but industry should take the lead in determining just how those devices should be secured. The report from the Homeland Security and Commerce departments stops short of recommending specific new regulations to counter botnets or tasking the government with developing major counter-botnet strategies. Instead, government should play an instigating role, the report states. For example, government should urge industry to adopt security baselines for internet-connected devices, such as sensors and cameras, and then incentivize device builders to adopt those baselines by mandating them for federal agencies and in federal contracts. The government should similarly use federal contract requirements to incentivize more secure and resilient methods of software building, the report states.

Source: NextGov, 30 May

3.2 Facebook secretly shared data with dozens of companies

Facebook has confirmed it has data sharing partnerships with at least four Chinese companies, including Huawei, which has come under scrutiny from US intelligence agencies on security concerns. The social media company said Huawei, the world's third-largest smartphone maker, computer maker Lenovo Group, and smartphone makers OPPO and TCL Corp were among about 60 companies worldwide that received access to some user data after they signed contracts to re-create Facebook-like experiences for their users. Facebook denied that and said the data access was to allow its users to access account features on mobile devices. More than half of the partnerships have already been wound down, Facebook said. It would end the Huawei agreement later this week, it said on Tuesday, and is ending the other three partnerships with Chinese firms as well. Chinese telecommunications companies have come under scrutiny from US intelligence officials who argue they provide an opportunity for foreign espionage and threaten critical US infrastructure, something the Chinese have consistently denied.

Source: Newshub, 7 June

3.3 Qatar state news agency's hacking linked to Riyadh

The breach of Qatar News Agency (QNA) and the publication last year of fabricated statements attributed to the Emir of Qatar, Sheikh Tamim bin Hamad Al Thani, can be attributed to a Saudi piracy cell, an Al Jazeera investigation has revealed. According to the investigation, which was broadcast on Sunday, the piracy cell worked from within a leading Saudi ministry in the capital, Riyadh. The hacking of Qatar's state-run news agency and government social media accounts on May 24, 2017, set into motion a major diplomatic crisis in the region, which saw Saudi Arabia, the United Arab Emirates, Bahrain and Egypt sever diplomatic relations and cut off land, air and sea links with Qatar on June 5 last year. Saudi Arabia and its allies accused Qatar of supporting "terrorism" and advancing the agenda of their regional rival, Iran. Doha has strongly denied these allegations. Qatari writer Abdul Aziz al-Ishaq told Al Jazeera that the investigation proved Saudi King Salman bin Abdul Aziz was aware of the planned hacking of QNA's website during his visit to Doha in December 2016.

Source: Al Jazeera, 4 June

3.4 Senators demand Bolton reconsider eliminating top cyber post

The Trump administration’s decision to eliminate a top cybersecurity position at the White House is drawing more criticism from senators. A group of 19 senators, all of them Democrats, wrote to national security adviser John Bolton this week urging him to reconsider the move, calling it a “step in the wrong direction” and worrying that it would “lead to a lack of unified focus against cyber threats.” The role of White House cybersecurity coordinator was established under the Obama administration to coordinate cybersecurity policymaking efforts across the federal government. In mid-May, National Security Council officials disclosed that they would eliminate the position in order to streamline operations across the two senior directors who work on cybersecurity. The decision immediately drew criticism in Washington, particularly from Democrats who argued that it would represent a step backward and undermine U.S. efforts to secure cyberspace.

Source: The Hill, 30 May

3.5 The Cybersecurity 202: White House cybersecurity report shows federal agencies still struggling to get secure

The White House and the Department of Homeland Security have finished a government wide review examining the security of federal agencies, and the results aren’t pretty. Dozens of federal agencies have cybersecurity programs that aren't properly equipped to deal with cyber intrusions in their networks, according to a new report released by the White House Office of Management and Budget. Of the 96 federal agencies examined, a whopping 71 were relying on cybersecurity programs deemed "at risk or high risk." President Trump came to office promising cybersecurity would be a major priority — vowing on the campaign trail to order a review of U.S. cyber defences and to confront malicious cyber activity by foreign governments. Trump's relative prioritization of federal cybersecurity was welcomed by many experts in the wake of the massive Office of Personnel Management breach that exposed the personal information of some 22 million people in 2014, and in light of the intelligence community's fresh concerns about Russia's election interference during the 2016 presidential election.

Source: Washington Post, 30 May

Part 4: Papers for the Minister (Briefs, Cabinet Papers, OIAs and Ministerials etc)

Status	Type/Title of paper	Comment or purpose	Deadline for Minister's sign-off
✓ Provided to Minister's office 1 June	OIA 2017/18 - 0500	OIA from Taxpayers' Union to the PM for details about the refresh of the Cyber Security Strategy (costs, number of officials, meetings etc) – one of 75 OIAs from the Taxpayers Union about various reviews.	4 June
✓ Response provided by MBIE to Minister's office	OIA 18-25	OIA from Melissa Lee MP: Part of a broader request. Q12 relates to NCPO: any papers on Pyeongchang Cyber Attack: NIL response	7 June
✓ Response provided to MBIE by 11 May	Brief	Material to be provided to MBIE for Economic Development, Science and Innovation Committee 2018 Estimates Examination hearing on 14 June.	7 June
✓ Provided to Minister's office 8 June	Brief	Meeting with Internet NZ on refresh of Cyber Strategy and CERT NZ	11.30am, 11 June
Drafting – response to be provided to MBIE for collation and	OIA 18-66	OIA from Melissa Lee for copy of weekly reports from 5 January to April 18	25 June

to Minister's office.			

Committee and Date	Date due in Minister's Office	Title of Paper	Comment or Purpose
Govt Administrative and Expenditure Review Committee, 26 June		A New Approach to Digital Identity	Led by DIA. Considers a digital identity services for citizens and organisations
TBC		s9(2)(f)(iv), s9(2)(g)(i) [redacted]	[redacted]
ERS – 31 October		Refreshed Cyber Security Strategy and Action Plan	

~~RESTRICTED~~

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

Date:	15 June 2018	**Priority:**	Routine

National Cyber Policy Office: Weekly Report

Part 1: **Cyber Security Strategy Refresh**

Part 2: **Action Plan update**

Part 3: **Cyber security news this week**

Part 4: **Briefs, Cabinet Papers, OIAs and Ministerials**

From:

Paul Ash
Director
National Cyber Policy Office
s9(2)(a)
[redacted] A/H)

Heather Ward
Principal Adviser and Acting Team Leader
National Cyber Policy Office
s9(2)(a)
[redacted] A/H)

Recommendation:

4 **Agree** that, once this weekly report has been considered by you, the National Cyber Policy Office will review it alongside other weekly reports since 25 May for release at the end of June in consultation with your office.

Yes / No

Hon Clare Curran
Minister of Broadcasting,
Communications and Digital Media

.

... / 06 / 2018

Part 1: Cyber Security Strategy Refresh

1.1 Workshops in the "Understand" Phase

Invitations for the workshops in the "understand" phase of the Cyber Security Strategy refresh have been sent out through our Connect Smart partnership mailing list; CERT NZ and the National Cyber Security Centre (within GCSB) have also forwarded the invitations to their stakeholders. Information about the workshops is also available on the Connect Smart website. We have also provided a draft press release to your office.

The details of the workshops are as follows:

Wellington, Tuesday 26 June:
9.00am – 11.30am OR 12.30pm – 3.00pm
Venue: DIA Service Innovation Lab, Level 4, 191 Thorndon Quay, Wellington

Auckland**,** Thursday 28 June:
9.00am – 11.30am OR 12.30pm – 3.00pm, 28 June:
Venue: ANZ Centre, 23-29 Albert St, Auckland City

Christchurch, Friday 29 June,
9.00am – 11.30am
Venue: Canterbury Employers' Chamber of Commerce, 57 Kilmore St, Christchurch Central, Christchurch

The workshops will be facilitated by KPMG and Thought Partners. Your recorded video message will be shown at the beginning of each workshop. The workshops will focus on what is critical to New Zealand's cyber security; the principles or values that should underpin the Strategy; the priority areas; and a possible vision: what does New Zealand want to be known for in cyber security?

In addition to the workshops, we are engaging with key stakeholders, including on particular issues. An online survey will be available to enable those unable to attend the workshops to contribute. The Connect Smart website also encourages people to email their insights to us.

We will hold an officials' workshop with the facilitators at the Service Innovation Lab to consolidate and analyse the outcomes from the workshops on 3 July. We will provide a report to you by 5 July on the insights from these workshops and other outreach, including initial thinking about a possible framework for the refreshed Strategy. [Note this report is slightly delayed because of a delay in confirming venues for the workshops]. We will also prepare a summary of the insights from the workshops for release on the Connect Smart website.

1.2 Meeting with InternetNZ

In addition to the call on you by InternetNZ (Jordan Carter, Chief Executive) on 11 June, NCPO and other agency representatives from the Strategy Refresh Working Group and sub-Working

Groups had a session with the InternetNZ team on 13 June. Some of the key points from the meeting with InternetNZ included:

- Preference for a multi-stakeholder approach to the refresh of the Cyber Security Strategy to ensure that actions are owned by multiple agencies and non-government.
- A suggestion that the development of the Action Plan could involve co-designed deep-dives on particular issues. Feedback loops are important to ensure buy-in.
- Will the Strategy be accompanied by resources? How will this fit into the Budget cycle?
- Discussion about the role of the Domain Name Commissioner (Brent Carey) and the scope to help address cybercrime – this will be the subject of a more detailed conversation. InternetNZ are holding a forum in November on the abuse of domain names. InternetNZ have a good relationship with NZ Police and have recently signed an MoU with CERTNZ.
- InternetNZ are keen to see some way of measuring progress with cyber security – how do we know if we are making progress towards the desired state? We discussed cyber security maturity models.
- Agreement on the need to collaborate on international engagement. InternetNZ are keen to see government involved in the Internet Governance Forum. InternetNZ has some reservations about "deterrence" in the context of cyber security.
- InternetNZ suggested that CERT NZ could play an important role leading on cyber security innovation, alongside its role in service delivery. InternetNZ would like to see a hybrid governance arrangement. InternetNZ noted "noise" that the NZ Intelligence Community want to subsume CERT NZ – InternetNZ are absolutely opposed to this.
- A strong Strategy will help to address perceptions of institutional fragmentation. There should be a Minister with a portfolio responsibility for cyber security.
- InternetNZ supports accession to the Budapest Convention, including the requirement for data preservation. InternetNZ is opposed to data retention. Public engagement on this will be important to ensure public understanding of the distinction between preservation and retention.

1.3 Presentation to Government Information Security Forum

NCPO (Heather Ward) presented to a session of the Government Information Security Forum (a meeting of government agency Chief Information Security Officers) on the Strategy refresh. As IT security professionals, the group are very enthusiastic about cyber security. The group have undertaken to email inputs and suggestions for the refresh. Some key points from the discussion:

- Importance of identity verification and assurance. Also that agencies/businesses/organisations should not collect more personal information than they need for business purposes.
- Importance of identifying and prioritising national information infrastructures (not just critical infrastructure) in order to ensure national information resilience.
- Suggestion that service providers can play a role in channelling cyber security to their small business customers.

Part 2: Action Plan Update

Cyber Resilience:

NEW ZEALAND'S INFORMATION INFRASTRUCTURES CAN RESIST CYBER THREATS AND WE HAVE THE TOOLS TO PROTECT OUR NATIONAL INTERESTS.

2.1 Nil to report.

Cyber Capability:

NEW ZEALANDERS, BUSINESSES AND GOVERNMENT AGENCIES UNDERSTAND CYBER THREATS AND HAVE THE CAPABILITY TO PROTECT THEMSELVES.

2.2 Nil to report

Addressing Cybercrime:

NEW ZEALAND IMPROVES ITS ABILITY TO PREVENT, INVESTIGATE AND RESPOND TO CYBERCRIME.

2.3 Commission on Crime Prevention and Criminal Justice (CCPCJ): Budapest Convention

Cybercrime was the focus of the 27th session of the Commission on Crime Prevention and Criminal Justice (CCPCJ), held from 14-18 May in Vienna. The Commission acts as the principal policy-making body of the United Nations in the field of crime prevention and criminal justice. It has 40 Member States (New Zealand is not currently a member). An MFAT representative in Vienna attended the meeting and reported by Formal Message (7 June 2018).

UN Secretary-General Guterres addressed the Commission for the first time and underscored the work of UN Office on Drugs and Crime in tackling the interlinked problems of drugs, organised crime, terrorism and corruption, and emphasised the role of the UN as a platform for all stakeholders to develop responses to cybercrime.

s6(a)

[redacted]

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

[redacted]

International Cooperation:

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY.

2.4 Nil to report.

Part 3: Cyber Security news this week (abridged clips)

3.1 Huawei to be banned from 5G

Chinese telco giant Huawei is all but certain to be excluded from providing equipment for Australia's soon-to-be-built 5G wireless networks, based on national security concerns, senior sources say. National security concerns have already resulted in Huawei being shut out of the national broadband network and yesterday Mr Turnbull and his Solomon Islands counterpart Rick Houenipwela met in Canberra to seal a deal in which Australian aid money will be used to fund a $200 million high-speed, undersea communications cable connecting the Solomons, Papua New Guinea and Australia. Again, motivated by national security concerns, Australia stepped in with the aid budget to head off a bid by Huawei to lay the cable. In an apparent effort to get ahead of any government decision, Huawei's Australian chairman John Lord went on national radio last week emphasising that the company was not state-owned. He said Huawei was 18 months ahead of its competitors on 5G technology and hinted there could be major job losses if it was excluded from building the new networks in Australia.

Source: The Australian Financial Review, 14 June

3.2 Chinese hackers stole plans for US submarine warfare

The US defence secretary has ordered a security review after Chinese government hackers stole data from an American military contractor, including plans for submarine-launched supersonic missiles. The hackers are said to have compromised the computers of a contractor working for the Naval Undersea Warfare Centre, in Rhode Island, to steal information on submarine warfare. Part of the stolen information was related to the US navy's Sea Dragon project, which has been given $300 million in funding but is cloaked in secrecy. The hack is thought to have been carried out by the Chinese Ministry of State Security, an elite spy agency. The Chinese have a long record of pilfering plans for advanced weapons. They are also believed to have stolen data on America's F-35 joint strike fighter, the Thaad anti-ballistic missile system and the new-generation littoral combat ship.

Source: The Times, 11 June

3.3 Federal government biggest target for cyber security attacks

A third of all cyber attacks investigated during the last financial year by Australia's cyber security agency were targeted at the federal government. Figures from the Australian Cyber Security Centre revealed that of the 671 cyber security incidents during 2016-17 that warranted an operational response, 33 per cent of those were aimed at federal parliament. According to the centre, almost 14 per cent of threats were aimed at state or territory governments, however the Australian Signals Directorate declined to comment on the statistics for specific jurisdictions. Of the remaining cyber security threats, more than 29 per cent were targeting industry, while all other attacks made up just less than 23 per cent.

Source: Sydney Morning Herald, 10 June

3.4 Major universities hit by data breach affecting thousands of job applicants at top firms

Leading universities including Melbourne and Macquarie have become the latest victims of a major data breach at human resources firm PageUp, forcing them to suspend their job boards and urge applicants to check their affairs for unusual activity. The breach is under investigation by the government-run Cyber Security Centre. The University of Melbourne, ranked number one in Australia by *Times Higher Education*, disabled its links to PageUp's systems and is only accepting job applications by direct email. It urged existing applicants to check their affairs for any "unusual activity concerning personal information supplied during the recruitment process". The Australian National University in Canberra was also hit by the breach. A spokeswoman said on Friday "we've been advised that our site is secure" and applicants could use site as normal, but they could also apply directly to the university if they wished.

Source: Sydney Morning Herald, 07 June

Part 4: Papers for the Minister (Briefs, Cabinet Papers, OIAs and Ministerials etc)

Status	Type/Title of paper	Comment or purpose	Deadline for Minister's sign-off
✓ Provided to Minister's office 1 June	OIA 2017/18 - 0500	OIA from Taxpayers' Union to the PM for details about the refresh of the Cyber Security Strategy (costs, number of officials, meetings etc) – one of 75 OIAs from the Taxpayers Union about various reviews.	4 June
✓ Response provided by MBIE to Minister's office	OIA 18-25	OIA from Melissa Lee MP: Part of a broader request. Q12 relates to NCPO: any papers on Pyeongchang Cyber Attack: NIL response	7 June
Drafting – response to be provided to MBIE for collation and to Minister's office.	OIA 18-66	OIA from Melissa Lee for copy of weekly reports from 5 January to April 18	25 June

Committee and Date	Date due in Minister's Office	Title of Paper	Comment or Purpose
Govt Administrative and Expenditure Review Committee, 26 June		A New Approach to Digital Identity	Led by DIA. Considers a digital identity service for citizens and organisations
TBC		s9(2)(f)(iv), s9(2)(g)(i) [redacted]	[redacted]

ERS – 31 October		Refreshed Cyber Security Strategy and Action Plan	

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

Date:	22 June 2018	**Priority:**	Routine

National Cyber Policy Office: Weekly Report

Part 1: **Cyber Security Strategy Refresh**

Part 2: **Action Plan update**

Part 3: **Cyber security news this week**

Part 4: **Briefs, Cabinet Papers, OIAs and Ministerials**

From:

Paul Ash	Heather Ward
Director	Principal Adviser and Acting Team Leader
National Cyber Policy Office	National Cyber Policy Office
s9(2)(a) [redacted] (A/H)	s9(2)(a) [redacted] A/H)

Recommendation:

5 **Agree** that, once this weekly report has been considered by you, the National Cyber Policy Office will review it alongside other weekly reports since 25 May for release at the end of June in consultation with your office.

Yes / No

Hon Clare Curran
Minister of Broadcasting,
Communications and Digital Media

.

... / 06 / 2018

Part 1: Cyber Security Strategy Refresh

1.1 There has been a positive response to the workshops in Wellington, Auckland and Christchurch with almost 200 participants registered for the five events. We are analysing the RSVP lists to identify obvious gaps and to ensure that participation in the workshops is as broad as possible. We are sending additional targeted invitations, especially to boost participation in Auckland and Christchurch. Inevitably, however, there will be quite a few cyber security practitioners present.

You are popping into the Wellington afternoon workshop (1.45pm – 2.45pm on Tuesday 26 June at the DIA Service Innovation Lab). We have prepared a brief statement for you.

Cyber Resilience:

NEW ZEALAND'S INFORMATION INFRASTRUCTURES CAN RESIST CYBER THREATS AND WE HAVE THE TOOLS TO PROTECT OUR NATIONAL INTERESTS.

2.1 Nil to report

Cyber Capability:

NEW ZEALANDERS, BUSINESSES AND GOVERNMENT AGENCIES UNDERSTAND CYBER THREATS AND HAVE THE CAPABILITY TO PROTECT THEMSELVES.

2.2 Meeting with Sai Honig

You are meeting with Sai Honig at 11.30am on Thursday 28 June. NCPO has provided you with a separate briefing on this. Ms. Honig sits on the board of the International Information System Security Certification Consortium, (ISC)^2 – an international, nonprofit membership association for information security professionals.

Addressing Cybercrime:

NEW ZEALAND IMPROVES ITS ABILITY TO PREVENT, INVESTIGATE AND RESPOND TO CYBERCRIME.

2.3 Nil to report

International Cooperation:

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY.

2.4 <u>China FTA upgrade</u>

Ministry of Foreign Affairs and Trade officials have recently concluded a negotiation round with China on the FTA Upgrade. NCPO, alongside other agencies, is engaging with MFAT

s6(a), s9(2)(j)

[redacted]

[redacted]

[redacted]

s6(a)

[redacted]

s6(a)

[redacted]

Part 3: Cyber Security news this week (abridged clips)

3.1 Australia: Thousands of Treasury records breached

A data breach of Australia's Treasury records has exposed the personal details of thousands of people, including their addresses, birthdays, job history and phone numbers. The breach, which relates to the personal details of anyone who has applied or registered their interest for a job at Treasury, is being investigated by the Australian Cyber Security Centre. The breach relates to Treasury's use of the PageUp recruitment system that was infected by malware in May. But Treasury - the department responsible for the security of the federal budget - waited until Wednesday afternoon to alert thousands of staff and past applicants. Forensic experts that briefed Treasury revealed names, emails, addresses, phone numbers, gender, date of birth, nationality, employment status, and the personal details of all referees could have been caught up in the breach. The Treasury warning comes two weeks after the PageUp breach was first revealed and Australia Post warned job applicants that their bank details, tax file number and superannuation details and their license could also have been compromised. The Australian Cyber Security Centre recommends all PageUp users change their passwords.

Source: The Sydney Morning Herald, 22 June

3.2 Huawei, 5G, and Australia's China Debate

Australia is currently in the process of debating whether to allow the Chinese telecommunications company Huawei to participate in the role out of the forthcoming 5G network. The reality for Australia is that China's efforts are not benign. China's own law has much to say on the subject of Chinese firms being used for intelligence-gathering. Article 7 of China's 2017 National Intelligence Law declares: *All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of. The state will protect individuals and organizations that support, cooperate with, and collaborate in national* *intelligence work.* Huawei, being a Chinese company, must comply with Chinese law. Thus, China's own political realities are likely to have a critical impact on the level of trust other governments place on it. While China might want to leverage its technological capabilities to increase its capacity to engage in influence operations and intelligence gathering, this is likely to have a very real impact on the ability of these companies to engage in large-scale critical infrastructure engagements. By requiring Huawei's participation in these efforts, China is undercutting the ability of its companies to engage in certain markets.

Source: The Diplomat, 19 June

3.3 Singapore top cyber attack target during Trump-Kim talks: Report

Singapore was the top cyber attack target around the world during the Trump-Kim summit, with the country experiencing close to 40,000 attacks during the June 12 meeting, according to data collected by American technology company F5 Networks and its data partner Loryka. Data analysis by F5 Networks' Threat Research Intelligence team, which monitors global attacks, found that cyber attacks "skyrocketed" from June 11 and 12. Eighty-eight per cent of the 40,000 attacks were launched from Russia, followed by 8 per cent from Brazil, and 2 per cent from Germany. In addition, 97 per cent of all attacks from Russia during the two-day period were targeted at Singapore, said F5 Network's report which was published on June 14. The company could not verify if the attacks were state sponsored. Singapore also received up to 4.5 times more attacks than the United States or Canada on both days. Approximately 40,000 attacks were launched between 11pm on June 11, to 8pm on June 12 (Singapore time), peaking during the three-hour meeting between US President Donald Trump and North Korean leader Kim Jong-un at Capella Singapore in Sentosa.

Source: TODAYonline, 19 June

3.4 U.S. Easing Reins on Cyberattacks

The Pentagon has quietly empowered the United States Cyber Command to take a far more aggressive approach to defending the nation against cyberattacks, a shift in strategy that could increase the risk of conflict with the foreign states that sponsor malicious hacking groups. Until now, the Cyber Command has assumed a largely defensive posture, trying to counter attackers as they enter American networks. In the relatively few instances when it has gone on the offensive, particularly in trying to disrupt the online activities of the Islamic State and its recruiters in the past several years, the results have been mixed at best. But in the spring, as the Pentagon elevated the command's status, it opened the door to nearly daily raids on foreign networks, seeking to disable cyber weapons before they can be unleashed, according to strategy documents and military and intelligence officials. It reflects the greater authority given to military commanders by President Trump, as well as a widespread view that the United States has mounted an inadequate defence against the rising number of attacks aimed at America. It is unclear how carefully the administration has weighed the various risks involved if the plan is acted on in classified operations. Adversaries like Russia, China and North Korea, all nuclear-armed states, have been behind major cyberattacks, and the United States has struggled with the question of how to avoid an unforeseen escalation as it wields its growing cyber arsenal.

Source: The New York Times, 18 June

Part 4: Papers for the Minister (Briefs, Cabinet Papers, OIAs and Ministerials etc)

Status	Type/Title of paper	Comment or purpose	Deadline for Minister's sign-off
✓ Provided to Minister's office 21 June.	OIA 18-66	OIA from Melissa Lee for copy of weekly reports from 5 January to April 18	25 June

Committee and Date	Date due in Minister's Office	Title of Paper	Comment or Purpose
Govt Administrative and Expenditure Review Committee, 26 June		A New Approach to Digital Identity	Led by DIA. Considers a digital identity service for citizens and organisations
TBC		s9(2)(f)(iv), s9(2)(g)(i) [redacted]	[redacted]
ERS – 31 October		Refreshed Cyber Security Strategy and Action Plan	

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

Date:	29 June 2018	**Priority:**	Routine

National Cyber Policy Office: Weekly Report

Part 1: **Cyber Security Strategy Refresh**

Part 2: **Action Plan update**

Part 3: **Cyber security news this week**

Part 4: **Briefs, Cabinet Papers, OIAs and Ministerials**

From:

Paul Ash Director National Cyber Policy Office s9(2)(a) [redacted] A/H)	Heather Ward Principal Adviser and Acting Team Leader National Cyber Policy Office s9(2)(a) [redacted] A/H)

Recommendation:

1 **Agree** that, once this weekly report has been considered by you, the National Cyber Policy Office will review it alongside other weekly reports since 25 May for release at the end of June in consultation with your office.

Yes / No

Hon Clare Curran
Minister of Broadcasting,
Communications and Digital Media

... / 06 / 2018

Part 1: Cyber Security Strategy Refresh

A series of five workshops were held in Wellington, Auckland and Christchurch this week. The two workshops in Wellington attracted around 50 participants each; the two in Auckland around 40 participants each; and the Christchurch workshop attracted 20 participants.

The workshops attracted a wide range of participants from across the economy, representing multinational organisations (e.g. Google, Microsoft), telecommunications (Vodafone, Spark), energy sector, banks and financial services, insurance sector, district health boards, a range of cyber security and IT providers (e.g. Datacom, Aura and individual service providers such as Geeks on Wheels and Need a Nerd), universities and other tertiary education providers, and non-government organisations (e.g. Netsafe, InternetNZ, Greypower). In Wellington, a range of government agencies, including the Director of the GCSB, participated.

The workshops focused on the possible vision, goals and principles for the Strategy as part of the “understand” phase. We received very positive feedback from all stakeholders and willingness to be involved in the next stages.

We will now focus on “pulling it together” – developing a possible framework vision, goals and principles) for the refreshed Strategy. This will be tested with stakeholders – and we will seek input again on how to populate the framework with actions and initiatives around late July.

Part 2: Action Plan Update

Cyber Resilience:

NEW ZEALAND'S INFORMATION INFRASTRUCTURES CAN RESIST CYBER THREATS AND WE HAVE THE TOOLS TO PROTECT OUR NATIONAL INTERESTS.

2.1 Nil to report

Cyber Capability:

NEW ZEALANDERS, BUSINESSES AND GOVERNMENT AGENCIES UNDERSTAND CYBER THREATS AND HAVE THE CAPABILITY TO PROTECT THEMSELVES.

2.2 <u>A New Approach to Digital Identity</u>

The Department of Internal Affairs has prepared a Cabinet paper outlining the case for setting a new strategic policy direction for digital identity management, one which actively supports the development of a 'healthy digital identity ecosystem' in New Zealand. The proposed new approach to digital identity backs government's priorities to share prosperity and to build a productive, sustainable, inclusive economy, and improve people's online experiences.

Addressing Cybercrime:

NEW ZEALAND IMPROVES ITS ABILITY TO PREVENT, INVESTIGATE AND RESPOND TO CYBERCRIME.

2.3 Nil to report

International Cooperation:

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY.

2.4 Nil to report

Part 3: Cyber Security news this week (abridged clips)

3.1 Australia backs Vanuatu's CERT

Australia put $400,000 towards supporting Vanuatu's newly launched Computer Emergency Response Team as well as helping the Pacific nation's work developing cyber policy and legislation. Prime Minister Malcolm Turnbull made the announcement today during a visit to Australia by his Vanuatu counterpart, Charlot Salwai. Vanuatu's CERT was launched last week. "This is a security infrastructure achievement which will see Vanuatu stepping up to cyber-threats and vulnerabilities and reporting them to a central point-of-management, control and mitigation team, who can analyse their findings, report with advisories and guides to help the government, business organisations and individuals who are using the internet in Vanuatu," acting director Gregoire Nimbtik said at the launch, according to a Vanuatu Daily Post report.

Source: Computerworld Australia, 25 June

3.2 United States: privacy advocates hail supreme court cellphone data ruling

Chief Justice John Roberts […] authored a majority opinion ruling in the United States Supreme Court that the government could no longer access an individual's cellphone location data without a warrant. The case, Carpenter v United States, is being hailed as a "groundbreaking victory for Americans' privacy rights in the digital age" by Nathan Freed Wessler, the ACLU attorney who argued the case before the supreme court in November. That is because, as Andrew Crocker of the Electronic Frontier Foundation explains, the ruling is "a crack in the edifice" of the "third-party doctrine" – a long-established legal theory that holds that if an individual shares information with a third party, they no longer enjoy constitutional privacy rights. In practical purposes, this means that the government needs only a subpoena or court order to obtain bank records or phone call history, rather than a search warrant – which is harder to get.

Source: The Guardian, 23 June

3.3 Z Energy security breach admitted as CEO fronts and apologises

Following an investigation by Stuff Circuit, fuel company Z Energy has admitted a major security fault that allowed access to business accounts and personal details. The extent of any unauthorised data access is unclear. Z was alerted to the "critical flaw" by a website user on 29 November last year. The problem hit the company's Z Card Online system, which allows people to manage fuel accounts, mostly for business fleets. There are around 45,000 Z fuel cards in the country. The Z Card Online vulnerability meant anyone could access accounts simply by changing the account number in the site's URL. Following initial unsuccessful remediation efforts, Z took the site offline in December but it did not disclose the potential data breach to customers whose data was affected. It appears that Z executives were not aware of the full extent of the problem until approached by Stuff. Chief Executive Mike Bennetts has now apologised and invited customers to contact the company. Z Card Online was a legacy system, initially built in the nineties, and has since been replaced.

Source: Stuff Circuit, 27 June

Part 4: Papers for the Minister (Briefs, Cabinet Papers, OIAs and Ministerials etc)

Status	Type/Title of paper	Comment or purpose	Deadline for Minister's sign-off
✓	BCDM1718-195 s9(2)(a) [redacted]	Email from s9(2)(a) [redacted] dated 5 June 2018, on cyber security & Huawei	TBD

Feedback provided on response 22 June	Ministerial: Fibre Rollout - Cybersecurity		

Committee and Date	Date due in Minister's Office	Title of Paper	Comment or Purpose
TBC		s9(2)(f)(iv), s9(2)(g)(i) [redacted]	[redacted]
Tbc		A New Approach to Digital Identity	This is an Internal Affairs led paper. The paper proposes a new strategic policy direction to develop a collaborative digital identity ecosystem that will create an architecture and marketplace model that will operate within an overarching government-set Identity Trust Framework.
ERS – 31 October		Refreshed Cyber Security Strategy and Action Plan	