Document 1

~~IN CONFIDENCE~~

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

Briefing

NEW ZEALAND PARTICIPATION IN US-HOSTED INTERNATIONAL COUNTER-RANSOMWARE INITIATIVE, 13-14 OCTOBER 2021

To:
Prime Minister (Rt Hon Jacinda Ardern)
Minister for the Digital Economy and Communications (Hon Dr David Clark)
Copy to:
Minister of Foreign Affairs (Hon Nanaia Mahuta)

Date	20/09/2021	**Priority**	Routine
Deadline	20/09/2021	**Briefing Number**	2122NSP/029

Purpose

This briefing informs you of a virtual, plurilateral meeting: the International Counter-Ransomware Initiative, being hosted by the United States on 13-14 October 2021, and proposes New Zealand participation be led by the Prime Minister's Special Representative on Cyber and Digital, Paul Ash.

Recommendations

1. **Note** that New Zealand has been invited to participate in a US-hosted International Counter-Ransomware Initiative, for senior government officials on 13-14 October 2021 (14-15 October NZ time);

2. **Agree** that New Zealand's participation be led by the Prime Minister's Special Representative for Cyber and Digital, Paul Ash; and **YES / NO**

~~RESTRICTED~~

3. **Note** the United States has proposed that participating countries issue a joint statement, and that officials will revert with further advice on this and the other proposed outcomes, once we have further information.

s9(2)(a)

Tony Lynch
Deputy Chief Executive
National Security Group

27 / 9 / 2021

Rt Hon Jacinda Ardern
Prime Minister

/ 9 / 2021

Hon David Clark
Minister for the Digital Economy and Communications

/ 9 / 2021

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Paul Ash	Prime Minister's Special Representative on Cyber and Digital	s9(2)(a)	✓
s9(2)(a)	Senior Policy Advisor National Security Group		

Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

NEW ZEALAND PARTICIPATION IN US-HOSTED INTERNATIONAL COUNTER-RANSOMWARE INITIATIVE, 13-14 OCTOBER 2021

Purpose

1. This briefing informs you of a virtual, plurilateral meeting: the International Counter-Ransomware Initiative, being hosted by the United States on 13-14 October 2021, and proposes New Zealand participation be led by the Prime Minister's Special Representative on Cyber and Digital, Paul Ash.

New Zealand has been invited to participate in a plurilateral, senior officials counter-ransomware event

2. The United States Government is hosting a virtual, plurilateral event for senior government officials focussed on international efforts to counter ransomware and has invited New Zealand to participate, alongside 30 other countries[1]. The meeting will be held on 13-14 October 2021 (14-15 October NZ time).

3. The event's purpose is to reinvigorate existing efforts to counter ransomware through law enforcement and CERT networks, and identify new opportunities for international collaboration. It will involve a series of panel discussions that will examine efforts and generate ideas to improve resilience, prevent the abuse of virtual currencies to launder ransom payments, disrupt ransomware networks and strengthen diplomatic efforts.

s6(b)(i)

s6(a)

[redacted]

[1] The countries expected to participate are Australia, Brazil, Bulgaria, Canada, Czech Republic, Dominican Republic, Estonia, European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, Netherlands, New Zealand, Nigeria, Poland, Republic of Korea, Romania, Singapore, South Africa, Sweden, Switzerland, Ukraine, United Arab Emirates and the United Kingdom.

s6(a) [redacted]

We recommend New Zealand participate in the event

8. New Zealand's experience of ransomware has been similar to partner countries, with cybercrime affiliates targeting our public health, education and other sectors. Several high-profile New Zealand organisations have been affected by ransomware attacks, including the Waikato District Health Board, Fisher & Paykel, Lion and the Department of Conservation.

s9(2)(f)(iv) [redacted]

s6(a) [redacted]

Recommended approach for New Zealand's participation

11. The event will be chaired by the United States' Deputy National Security Adviser for Cyber and Emerging Technology (DNSA), Anne Neuberger, and the US has invited each participating country to be represented by one equivalent senior official.

12. We recommend New Zealand's participation be led by the Prime Minister's Special Representative on Cyber and Digital, Paul Ash, s6(a) [redacted]

Paul will have the opportunity to either speaking on or moderating a panel discussion.

Next steps

13. Officials will continue to engage with organisers on the proposed joint statement and other proposed outcomes noted in paragraph four, to ensure New Zealand perspectives and values are sufficiently reflected. A further briefing containing the draft joint statement will be provided to Ministers for approval, prior to the event.

Consultation

14. This paper has been consulted with the Ministry of Foreign Affairs and Trade (MFAT), who support the proposed approach for New Zealand's participation.

Document 2

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

NEW ZEALAND FOREIGN AFFAIRS & TRADE
Manatū Aorere

Briefing

CYBER SECURITY INTERNATIONAL ENGAGEMENT PLAN

To	**Minister of Foreign Affairs** (Hon Nanaia Mahuta) **Minister for the Digital Economy and Communications** (Hon Dr David Clark)		
Date	30/06/2021	**Priority**	Routine
Deadline	14/07/2021	**Briefing Number**	2021/NSP/130

Purpose

Officials across government agencies have developed a Cyber Security International Engagement Plan (IEP), in line with the "internationally active" priority in New Zealand's Cyber Security Strategy 2019. This briefing provides an overview of the IEP, including our vision, principles, and priorities for engagement.

Recommendations

It is recommended that you:

1. **Note** the Cyber Security International Engagement Plan.

Ben King **For Secretary of Foreign Affairs** Ministry of Foreign Affairs and Trade	Hon Nanaia Mahuta **Minister of Foreign Affairs**
...../...../2021	...../...../2021

Tony Lynch **Deputy Chief Executive, National Security** Department of the Prime Minister and Cabinet		Hon Dr David Clark **Minister for the Digital Economy and Communications**
…../…../2021		…../…../2021

Contact for telephone discussion if required:

Name	Position	Telephone
s9(2)(a)	Team Leader – International Cyber Policy, National Security Policy Directorate, DPMC	s9(2)(a)
s9(2)(a)	Lead Advisor, Cyber and Emerging Technology, International Security and Disarmament Division, MFAT	s9(2)(a)

Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

CYBER SECURITY INTERNATIONAL ENGAGEMENT PLAN

Purpose

1. Officials have developed a Cyber Security International Engagement Plan (IEP) to frame and prioritise our international cyber engagement. This briefing provides an overview of the IEP, and the priorities for engagement in the short to medium term. The IEP will be kept under review.

Background

2. In 2019, the New Zealand Government released a refreshed Cyber Security Strategy. This strategy highlights five Priority Areas, one of which is "Internationally Active":

> *New Zealand's interests will be advanced and protected through our international activity. We will continue to champion a free, open, secure internet. New Zealand's voice in international discussions related to cyber issues will support the international rules-based order and promote peace and stability in cyberspace.*
>
> *New Zealand considers that existing international law applies online as it does offline and supports the development and implementation of norms for responsible state behaviour to maintain a peaceful and stable online environment. Cooperation and dialogue on cyber issues is central to building confidence and understanding to reduce the risk of conflict. We will act bilaterally, regionally and globally to build trust in cyberspace.*
>
> *We will respond to unacceptable behaviour in cyberspace and we will cooperate with others to prevent and deter malicious activity that threatens peace and security.*
>
> *New Zealand's international engagement on cyber security issues will:*
>
> - *build clearly prioritised international partnerships and cooperation at policy and operational levels;*
> - *influence to support the rules-based international order and a free, open, multistakeholder internet;*
> - *prevent, detect, deter, and respond to malicious behaviour online'*
> - *secure our neighbourhood by strengthening regional capacity-building, confidence, and operational cooperation, including for law enforcement activities;*
> - *contribute to New Zealand's economic prosperity.*

3. Officials have developed the IEP to support delivery of this priority. Completion of the IEP was one of the commitments under the Cyber Security Strategy work programme for 2019/20. The IEP was approved by the Cyber Security Strategy Coordination Committee (the Strategy's governance group) in November 2020.

4. The IEP's vision, principles, priorities and focus relationships have been summarised in three A3s (in Attachment A).

Our vision and principles

5. The IEP sets out the principles for New Zealand's international engagement on cyber security as follows (these are consistent with the principles in the broader Cyber Security Strategy[1]):

- *We prioritise and support a robust, well-functioning rules-based order;*
- *We act independently, in our national interest;*
- *We acknowledge our close partners, and our place in the Pacific.*
- *We maximise our resources – and prioritise effectively;*
- *We coordinate across agencies – this is New Zealand's comparative advantage;*
- *We aim to find common ground, and build trust and confidence.*

6. The IEP also articulates the key outcomes that New Zealand is seeking from our international cyber security engagement, as follows:

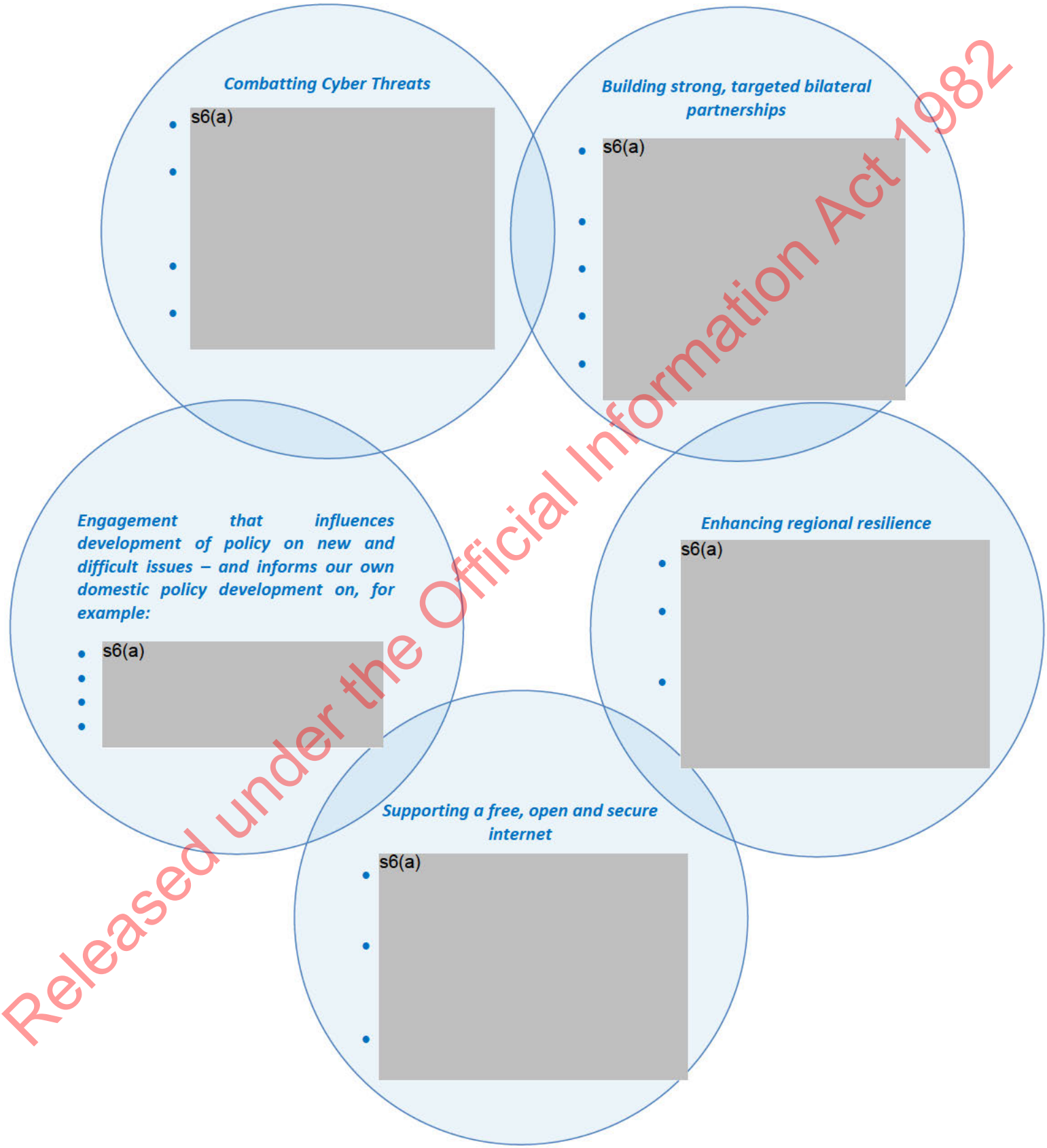
New Zealand wants:

- *A cyberspace that is safe, secure, free, open, and interoperable, with a multistakeholder approach to internet governance;*
- *To be a secure, advanced economy, well-equipped and positioned to address cyber threats – a risk that is heightened in a COVID-19 context.*
- *A well-functioning rules-based order that:*
  - *Provides a framework for responsible state behaviour online;*
  - *Enables effective international cooperation on cybercrime;*
  - *Allows for the further development of cyberspace and related technologies in a way that balances safety and security with innovation and economic development; and*
  - *Clearly prioritised, strong bilateral, regional and multilateral relationships that support our cybersecurity policy and operational objectives.*
- *To be recognised as a practical and constructive contributor to international cybersecurity discussions; and*
- *A Pacific region resilient to cyber risks.*

[1] These principles are also aligned with those articulated in our briefing on New Zealand's engagement in UN cyber processes ("Briefing: United Nations Cyber Processes", 2021NSP/064, dated 18/02/2021), which forms a subset of our international engagement on cybersecurity.

Our priorities for engagement

7. The IEP proposes that New Zealand will prioritise the following areas:



Priority countries and organisations for engagement

8. Alongside these priority areas, the IEP outlines engagement plans for specific countries, regional bodies, multilateral and multistakeholder organisations and processes. These include priority areas for engagement in those relationships, as well as the risks and opportunities of such engagement.

9. s6(a)

10.

11.

12.

13.

Next steps

14. This IEP is designed to provide a framework to guide our international engagement on cyber issues, it does not articulate specific new initiatives or resourcing/funding requirements. Work conducted under the auspices of the IEP will generally be absorbed within baselines. If there are specific new initiatives that require additional resourcing, it is possible that they could be funded from the Cyber Security Strategy implementation fund. Advice and recommendations on this will be developed as appropriate.

15. The IEP will be revised as needed over time, including in response to any feedback from Ministers, as well as to changing circumstances internationally, changing cyber security dynamics, and New Zealand foreign policy and other priorities.

s6(a)

Consultation

16. The IEP has been developed jointly by the Ministry of Foreign Affairs and Trade (MFAT) and the Department of the Prime Minister and Cabinet (DPMC), in consultation with the Government Communications Security Bureau (GCSB), Ministry of Defence (MoD), New Zealand Defence Force (NZDF), CERT NZ, Ministry of Business, Innovation and Employment (MBIE), NZ Police, Department of Internal Affairs (DIA), Ministry of Justice, Crown Law, and New Zealand Security Intelligence Service (NZSIS).

17. This briefing has been jointly prepared by MFAT and DPMC.

Attachments

ATTACHMENT	CLASSIFICATION	TITLE
Attachment A:	RESTRICTED	Cyber Security International Engagement Plan A3s

Attachment A

CYBER SECURITY INTERNATIONAL ENGAGEMENT PLAN A3S

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

dpmc.govt.nz

Cyber security international engagement plan

We need to engage internationally to advance and protect New Zealand's interests, as cyber issues are inherently trans-boundary.

CYBERSPACE ISSUES

Threats

Rapidly evolving technology and increasing connectivity also increases our exposure to threats, like:

- s9(2)(g)(i)
-
-

Internet governance

Divergent views about how the internet should be governed:

- s9(2)(g)(i)
-

Other issues and harms

- Online harms including content issues such as: child sexual exploitation and terrorism content
- 5G network security risks
- The use of online channels to promote misinformation

our vision

- a secure, advanced economy, well-equipped for cyber threats
- a safe, secure, multi-stakeholder, free + open cyberspace
- a Pacific region resilient to cyber risks
- a rules-based order in cyberspace
- we are recognised as a practical + constructive contributor
- strong international relationships

our principles

- we will act **independently** in our national interest
- we will acknowledge our **close partners** + our place in the **Pacific**
- we will **maximise** our resources + **prioritise** effectively
- we will find **common ground** + build **confidence** + trust
- we will **coordinate** across agencies
- we will prioritise + support the **rules-based order**

OUR PRIORITIES

- Combating cyber threats
- Enhancing regional resilience in the Pacific and ASEAN
- Building strong, targeted bilateral partnerships
- Engagement that influences development of policy on new and difficult issues
- Supporting a free and open internet

s6(a)

s6(a)

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

Aide-Memoire

CYBER SECURITY STRATEGY APPROPRIATION

To	Minister for the Digital Economy and Communications (Hon Dr David Clark)	**Report No**	2021NSP/094
From	Tony Lynch, Deputy Chief Executive, National Security Group	**Date**	21/05/2021

Purpose

1. To provide information on expenditure to date on implementation of the Cyber Security Strategy 2019 and proposed future projects.

Background

2. Budget 2019 delivered $2 million per year on an ongoing basis for implementation of the Cyber Security Strategy.

3. This is in addition to other cyber security funding across government (such as the baseline funding for the GCSB's NCSC, CERT NZ, NZ Police's work against cyber criminals and departmental IT expenditure).

4. The funding is used for joint-agency projects to enhance national cyber security at a system level. Projects and initiatives funded through the strategy implementation are focused on parts of the strategy priority areas that are not well addressed by other government expenditure.

5. DPMC is the administering agency. Individual projects may be project managed by other agencies.

Comment

6. Due to the impacts of COVID-19, strategy implementation was delayed or deferred. This resulted in a rollover of the remaining 2019/20 budget to 2020/21. The current budget for 20/21 is $3.828m. The year to date spend is $841,104 (as at April 2021).

7. Approval in principle has been granted to roll over unspent funding at the end of this financial year to the 2021/22 financial year.

Projects funded under the strategy to date

8. The following items have been funded from the Cyber Security Strategy appropriation in 2020/21. Lead agencies are listed in brackets.

Project	Cost NZD (year to date Mar 21)
Trade Smart campaign contribution (CERT NZ)	200,000
Women in Cyber international workshop contribution (MFAT)	42,000
GPAI Secretariat contribution (DPMC)	85,390
Salaries and other operating costs (DPMC)	513,714
Total	**841,104**

9. The salaries currently funded under the appropriation are:

   a. Cyber Coordinator / Prime Minister's Special Representative on Cyber and Digital 1.0 FTE

   b. Principal Advisor (to deliver Budapest Convention) 1.0 FTE

   c. Principal Advisor (cyber security workforce) 0.4 FTE

   d. Senior Advisor (programme and project expertise) 1.0 FTE

Planned projects for 2020/21 and 2021/22

10. The following items are projected to be funded from the appropriation in 2020/21 and 2021/2022. Lead agencies are listed in brackets.

Proposed project	Estimated Cost NZD
s9(2)(f)(iv)	

s9(2)(f)(iv)

11. From 2021/22, the following salaries will be funded from the appropriation to better deliver the strategy:

s9(2)(f)(iv)

Future projects

13. DPMC has collated a prioritised list of ideas for projects. s9(2)(f)(iv)

Recommendations

14. It is recommended that you note the contents of this aide-memoire.

s9(2)(a)

Tony Lynch

Deputy Chief Executive
National Security Group

NOTED
Hon Dr David Clark Minister for the Digital Economy and Communications
Date: / /

Document 4

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

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

NEW ZEALAND FOREIGN AFFAIRS & TRADE
Manatū Aorere

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

BRIEFING

5G Security: Introduction

Date:	25 November 2020	**Priority:**	Low
Security classification:	**Restricted**	**Tracking number:**	2021-1429

Action sought		
	Action sought	**Deadline**
Hon Andrew Little Minister Responsible for the GCSB	**Note** the contents of this briefing.	No deadline
Hon Nanaia Mahuta Minister of Foreign Affairs	**Note** the contents of this briefing.	No deadline
Hon Damien O'Connor Minister for Trade and Export Growth	**Note** the contents of this briefing.	No deadline
Hon Dr David Clark Minister for the Digital Economy and Communications	**Note** the contents of this briefing.	No deadline

Name	**Position**	**Telephone**
James Hartley	General Manager, Commerce, Consumers and Communications, MBIE	S9(2)(a)
Sophie Vickers	Manager, NCPO, DPMC	
Cecile Hillyer	Divisional Manager, International Security and Disarmament Division, MFAT	
Andrew Hampton	Director-General of the GCSB	

The following departments/agencies have been consulted (if required)

Minister's office to complete:

- ☐ Approved
- ☐ Noted
- ☐ Seen
- ☐ See Minister's Notes
- ☐ Declined
- ☐ Needs change
- ☐ Overtaken by Events
- ☐ Withdrawn

BRIEFING

5G Security: Introduction

Purpose

To provide the attached document "Introductory Briefing on 5G Security". S6(a)

Background

The Minister for the Digital Economy and Communications has policy responsibility for the telecommunications network security regulatory system, including 5G network security. The Minister Responsible for the GCSB has decision making responsibilities under TICSA related to network security. The 5G network security (network security) also raises issues that fall within the Foreign Affairs and Trade and Export Growth portfolios.

For this reason the Ministry of Business, Innovation and Employment (MBIE), the Department of the Prime Minister and Cabinet (DPMC), the GCSB, and the Ministry of Foreign Affairs and Trade (MFAT) have prepared a briefing for Ministers with portfolio responsibilities for Digital Economy and Communications; Foreign Affairs; Trade and Export Growth, and Government Communications Security Bureau.

S6(a)

Officials are available at your earliest convenience to discuss this with you.

Recommended action

The Ministry of Business, Innovation and Employment, the Department of the Prime Minister and Cabinet, the GCSB and the Ministry of Foreign Affairs and Trade recommend that you:

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

Noted

S9(2)(a)

James Hartley
General Manager, Commerce, Consumers and Communications
Ministry of Business, Innovation and Employment

25 November 2020

Hon Andrew Little
Minister Responsible for the GCSB

..... / ..... / .....

S9(2)(a)

Andrew Hampton
Director-General of the GCSB

25/11/2020

Hon Nanaia Mahuta
Minister of Foreign Affairs

..... / ..... / .....

S9(2)(a)

Tony Lynch
Deputy Chief Executive, National Security Group
Department of the Prime Minister and Cabinet

.... / ..... / .....

Hon Damien O'Connor
Minister for Trade and Export Growth

..... / ..... / .....

S9(2)(a)

Ben King
For Secretary of Foreign Affairs and Trade

.... / ..... / .....

Hon Dr David Clark
Minister for the Digital Economy and Communications

..... / ..... / .....

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

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

NEW ZEALAND FOREIGN AFFAIRS & TRADE
Manatū Aorere

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Introductory Briefing on 5G Security

Briefing prepared for the Minister Responsible for the GCSB, Minister of Foreign Affairs, Minister of Trade and Export Growth and the Minister for the Digital Economy and Communications

November 2020

Purpose

1. S6(a)

2.

5G in context

What is 5G and why is it different to previous networks?

3. 5G is the next generation of mobile (wireless) technology. It will deliver faster mobile connections and data processing, better coverage, significantly increased capacity, and reductions in the delay between devices responding to each other over the wireless network (referred to as 'low latency').

4. While previous generations of wireless technology have largely focused on data and voice services, 5G represents a fundamental shift in how mobile technology is used. Access to massive amounts of data at significantly faster speeds will have numerous practical applications which are expected to lift productivity, enhance individuals' lives, and improve environmental quality.

5. 5G will enable further advances in artificial intelligence (AI) technology for a broad array of new business processes and applications and underpin the so-called 'Internet of Things' (IoT).[1] It will provide for applications such as enhanced augmented and virtual reality, autonomous vehicles, and remote surgical operations.

6. 5G will enable a diverse range of applications in part due to changes to the technological architecture of telecommunications networks. With previous mobile networks, the 'core' functions (i.e. where data is sorted and processed) and the 'edge' (i.e. the cellular radio functions) of the network have been largely separate. With 5G, these are effectively combined, with more processing functions at the 'edge' of the network, closer to the connected mobile devices.

New Zealand's roll out of 5G

7. As New Zealand's mobile market is primarily private sector-led, commercial decisions will affect the time it takes for the full range of 5G deployment cases to be realised. In New Zealand, Spark and Vodafone have commenced the roll out of their 5G networks in some regional towns (fixed wireless) and urban centres (mobile services) and 2degrees has announced it will commence the roll out of 5G in 2021. While 5G roll out will be led by the commercial sector, the Government has an interest in this technology due to the critical function it will play across the economy and society.

[1] Internet of Things refers to the network of devices and objects that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

5G security

5G and new security risks

8. As with previous mobile generations, 5G presents security risks. However, the risks 5G presents are not limited to just the configuration of the network, but also include the range and scale of interactions that 5G will enable. S6(a)

S6(a)

9. S6(a)

S6(a)

10. S6(a)

11.

New Zealand's approach to 5G security risk

12. The New Zealand Government has a range of legislative, policy and other programmes that contribute to mitigating and managing the risk associated with communications infrastructure, including 5G.

Addressing network security through the Telecommunications (Interception Capability and Security) Act 2013

13. Since 2014, New Zealand has managed its public telecommunication network security (including 5G) through the Telecommunications (Interception Capability and Security) Act 2013 (TICSA).

14. The purpose of Part 3 of TICSA is to prevent, sufficiently mitigate, or remove security risks arising from the design, build, or operation of public telecommunications networks, and from the interconnections of public telecommunications networks in New Zealand, or to networks overseas. MBIE is responsible for administering TICSA and associated policy. GCSB operationalises the network security provision of TICSA.

15. Under TICSA, network operators are required to notify the GCSB of planned changes to their networks within certain areas of specified security interest (notifiable changes could include the acquisition of equipment or services, changes to network architecture or changes in ownership or control). The GCSB assesses each notification for potential network security risk on a case-by-case basis (i.e. there are no 'bans' – TICSA is vendor and country agnostic). Only factors that impact on network security can be taken into account in these assessments.

16. If a network operator's proposal raises a significant network security risk, and the network operator is unable to prevent or sufficiently mitigate this risk, the Director-General of the GCSB may refer the matter to the Minister Responsible for the GCSB for a direction to prevent, reduce or mitigate the identified network security risk.

17. TICSA sets out a process for the Minister to make a direction that requires consideration of a range of factors in addition to network security, including the potential consequences of the direction on competition and innovation in the telecommunications market and the potential impact on the direction of trade. This process also includes consultation with the Minister for Communications (now the Digital Economy and Communications portfolio) and the Minister of Trade.

18. The majority of notifications raise minimal or no network security risk S6(a) S6(a)

19. S6(a) S6(a)

20. S6(a)

36. S6(a)

37.

38.

S6(a)

39. S6(a)

40.

Portfolio responsibilities

41. Telecommunications network security issues sits across several portfolios:

- Digital Economy and Communications
- Foreign Affairs
- Trade
- GCSB
- National Security and Intelligence.

42. The Minister for the Digital Economy and Communications has responsibility for administering TICSA.

43. The Minister Responsible for the GCSB has decision making responsibilities under TICSA related to network security. In making those decisions the Minister Responsible for the GCSB is required to take into account factors relating to the Digital Economy and Communications and the Trade portfolios.

S6(a)

44. S6(a)

S6(a)

45. S6(a)

46.

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

Briefing

BUDAPEST CONVENTION ON CYBERCRIME - INTRODUCTION AND NEXT STEPS

To: Minister for the Digital Economy and Communications (Hon Dr David Clark)			
Date	19/11/2020	**Priority**	Urgent
Deadline	23/11/2020	**Briefing Number**	2021NSP/028

Purpose

To provide you with information on the process for acceding to the Council of Europe Convention on Cybercrime (the Budapest Convention); outline the next steps and decisions that will need to be made: s9(2)(g)(i)

Recommendations

1. **Agree** to consult with the Minister of Justice on:
   a. the priority and timing of Cabinet decisions, and **YES / NO**
   b. the leadership of the Cabinet paper. **YES / NO**
2. **Note** Ministers will need to decide:
   a. on the scope of the data preservation scheme, which may have an impact on the proposed timeframe; and
   b. how to respond to feedback received from Māori submitters.
3. **Forward** this briefing to the Minister of Justice. **YES / NO**

s9(2)(a) [redacted] Tony Lynch **Deputy Chief Executive** **National Security Group** **Department of the Prime Minister and Cabinet**	Hon Dr David Clark **Minister for the Digital Economy and Communications**
19/11/20	...../...../....

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Sophie Vickers	Manager, National Cyber Policy Office	s9(2)(a)	✓
s9(2)(a)	Principal Policy Advisor, National Security Policy Directorate		

Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

BUDAPEST CONVENTION ON CYBERCRIME – INTRODUCTION AND NEXT STEPS

Purpose

1. This briefing provides you with further information on the process for acceding to the Council of Europe Convention on Cybercrime (the Convention), and outlines the next steps and decisions that will need to be made, in advance of an upcoming Cabinet report back.

Background

2. New Zealand's Cyber Security Strategy 2019 identified accession to the Budapest Convention as a key area of focus to proactively tackle cybercrime [CAB-18-MIN-0127]. In June 2020, Cabinet made an 'in principle' decision that New Zealand will accede to the Convention, with a final decision to be made following public consultation and the preparation of final advice on the legislative and financial implications. Cabinet agreed to receive a report back with full policy decisions in late 2020 [CAB-20-MIN-0252].

3. As the decision to accede to the Convention touches on cyber security and criminal justice policy, you co-lead this project with the Minister of Justice. Other interested Ministers include the Minister of Police, the Minister of Internal Affairs, the Minister Responsible for the GCSB, the Minister of Foreign Affairs, the Minister for Māori Crown Relations: Te Arawhiti, and the Attorney-General. These Ministers' agencies are responsible for enforcing cybercrime laws, managing relationships that may be affected by accession to international agreements, or in the case of the Attorney-General, considering requests from foreign jurisdictions for mutual legal assistance.

4. Work on accession to the Convention has been led by the Minister with the Communications portfolio due to the wide-ranging strategic benefits of accession, and because the telecommunications and cloud computing sectors will be directly affected by accession.

Overview of the Convention

The Budapest Convention is the only international treaty which seeks to address cybercrime

5. As the internet has become a normalised part of everyday life, it has also become a tool for criminal activity. Cybercrime is increasing in New Zealand every year and causes substantial financial and social harms.

6. Evidence of cybercrime and other serious crime is often held electronically by large internet service or cloud computing providers whose platforms are used by criminals.

7. The global nature of the internet means that an offender may be in one country, the victim in another, while the evidence of the offence is held by a company in a third country. Law enforcement therefore relies on international cooperation to prevent, investigate, and prosecute crimes committed wholly or in part online. This is simplified when countries have consistent laws for how crimes committed online are defined and how agencies can access recorded evidence of crime.

8. The Convention aims to prevent, deter, and detect crimes committed via the internet and other computer networks. It sets out a consistent basic framework for defining computer crimes, enabling lawful access to evidence, and outlining expectations on how relevant international agencies assist each other. Each country determines how to implement that framework in the context of its constitutional arrangements, privacy, and security policies.

9. The Convention came into force in 2004 and has 65 members, predominantly from Europe, but also from Asia, North and South America, Australia, and the Pacific. All members of the EU are parties to the Convention, as are the other Five Eyes countries.

Benefits of accession

Accession would enhance cooperation with other countries to address cybercrime

10. The legislative changes required to join would complement and enhance New Zealand's existing cooperation on cybercrime. Convention members share threat trends information, best practice technical advice, and capability-raising initiatives; accession would give New Zealand access to this. Parties benefit from a global network of points of contact available 24/7.

11. New Zealand would also be included in negotiations among the Parties on enhancements to the Convention to better address cybercrime. Accession would allow New Zealand to show legislative equivalency, should the Government decide to negotiate an Executive Agreement with the United States under the CLOUD Act (Clarifying Overseas Use of Data Act).[1] These and other bilateral agreements aim to provide a streamlined alternative to mutual legal assistance, which can be a lengthy process.

Accession would also have reputational value and support wider priorities

12. Accession supports New Zealand's objectives for a free, open and secure internet. Our absence from the Convention places us outside the developing norms for international governance of cyberspace. Joining would send a signal that we are committed to like-minded efforts to combat cybercrime, while at the same time protecting fundamental human rights and freedoms. This is important in the context of the recent adoption by the UN of a Russian resolution mandating the elaboration of a new global cybercrime treaty, which New Zealand and other like-minded countries voted against. We can provide further briefing on the context if you wish.

13. In addition, accession signals that our regulatory settings are up to date and consistent with best practice, enabling domestic and foreign investment in our digital economy to occur with confidence.

14. New Zealand's accession is a key deliverable of both the 2019 Cyber Security Strategy and the countering violent extremism work programme that was developed in response to the terror attack in Christchurch in 2019.

[1] The CLOUD Act was introduced to deal with issues raised in Microsoft Corp v United States where Microsoft argued it was not able to release information on a US citizen held on one of Microsoft's servers in Ireland.

The Convention does not address all the challenges of responding to cybercrime or securing electronic evidence in a digital age

15. The nature of technology and criminal activity has changed since the Convention was drafted. Further cybercrime-related policy issues will require consideration over time, outside of the accession process. s9(2)(g)(i)

16. Parties to the Convention are currently negotiating a 'Second Additional Protocol' to the Convention to address some of these broader policy issues. New Zealand is attending these negotiations as an observer. The next meeting is in December 2020. Any decision to accede to this protocol - or the existing Additional Protocol, which concerns racism and xenophobia online - would need to be subject to a separate Cabinet decision process.

Legislative changes required to accede

17. New Zealand already largely complies with the requirements of the Convention. Incremental changes would be required to the Search and Surveillance Act 2012, the Mutual Assistance in Criminal Matters Act 1992, the Crimes Act 1961 and the Customs and Excise Act 2018. The three notable changes are:

    a) introducing preservation orders into the Search and Surveillance Act (these would require a person or company to preserve, or refrain from deleting or modifying specific information for a specified period of time);

    b) introducing a new provision into the Search and Surveillance Act that requires third parties to keep confidential the fact that they have assisted law enforcement in executing a preservation order or a surveillance device warrant; and

    c) extending the availability of surveillance device warrants into the Mutual Assistance in Criminal Matters Act, so these could be used in New Zealand to obtain information relevant to overseas investigations, and vice versa.

Actions since our last report to Cabinet

Public consultation

18. Following the June 2020 Cabinet decision, officials have consulted the public. Consultation focused on the proposal that New Zealand accede to the Convention, and the details of a preservation order scheme to be included within the Search and Surveillance Act 2012. This is the most significant legislative change required for accession.

19. In additional to publishing a consultation document, officials held several virtual meetings with stakeholder groups. s9(2)(g)(i)

20. The consultation period ended in September. Many submitters dedicated significant resource and attention into considering the proposals, despite competing priorities.

s9(2)(g)(i)

[redacted]

[2] Article 10 of the Convention requires countries criminalise the intentional breach of copyright on a commercial scale. New Zealand law already complies with this requirement.

Ongoing work with operational agencies

27. Since consultation ended officials have been working to finalise the details of policy advice on a data preservation order scheme.

28. s9(2)(g)(i)

29. s9(2)(g)(i) The scheme that was consulted on is closely aligned with recommendations made by the Law Commission and the Ministry of Justice in a joint review of the Search and Surveillance Act, completed in 2018. Those recommendations provide a scheme that is useful for preserving evidence that is subject to a mutual assistance request as required by the Convention (which can take months or years to complete, during which time evidence could be lost before a production order is sought), but is not intended to have a wider domestic use.

30. s9(2)(g)(i)

31.

32.

33.

34.

35. s9(2)(g)(i) [redacted]

Upcoming Cabinet report back and next steps

36. In June 2020, Cabinet agreed that a second paper with full policy decisions be submitted for a final decision on accession to the Convention in December 2020. We propose that this paper would seek decisions from Cabinet on the following main issues:

    a) confirmation of the decision to accede;

    b) the design of the data preservation scheme;

    c) the arrangements for making surveillance device warrants available through mutual assistance;

    d) the arrangements for third party confidentiality orders; and

    e) confirmation of any reservations to the Convention that should be invoked.

37. Two options on the timing for the remaining work and a Cabinet report back are set out in the table below:

Step	Timeline A	Timeline B
Policy advice— • to the Minister for the Digital Economy and Communications and the Minister of Justice on accession to the Budapest Convention, and • to the Minister of Justice on legislative changes required to ratify the Convention	26 November 2020	mid-December 2020
Draft Cabinet paper and Extended National Interest Analysis to Ministers	26 November	early-February 2021
Revised Cabinet paper to Ministers, incorporating feedback	1 December	mid-February 2021
MFAT review of Extended National Interest analysis	1 - 8 December	mid-February 2021
Ministerial consultation on Cabinet paper	2 - 8 December	late-February 2021
Final paper lodged	10 December	early-March 2021
Cabinet discussion	16 December (CBC)	March 2021

Parliamentary Treaty Examination (Treaty text + NIA presented to the House)	February – March 2021	April – May 2021
Legislative drafting	March – May 2021	May – July 2021
Introduction and passage of legislation	TBC subject to Cabinet's priorities for legislation	TBC subject to Cabinet's priorities for legislation
Instrument of Accession deposited with the Council of Europe	TBC	TBC

38. Timeline A would deliver a Cabinet report back by December s9(2)(g)(i)

39. Timeline B would deliver policy advice to Ministers in December for decisions, to support a Cabinet report back early next year. s9(2)(g)(i)

Next Steps

40. s9(2)(g)(i)

41.

s9(2)(g)(i)

42. s9(2)(g)(i)

s9(2)(a), s9(2)(b)(i)