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

12 February 2021

[redacted]

Reference: OIA-2020/21-0235

Dear [redacted]

Official Information Act request relating to reports or briefings received between 1 September 2020 – 16 November 2020 by the then Minister of Broadcasting, Communications and Digital Media

Thank you for your request made the Official Information Act 1982 (the Act), received as a transfer from the office of Hon Kris Faafoi by the Department of the Prime Minister and Cabinet (DPMC) on 26 November 2020. You requested:

> *"All reports or briefings received between 1 September 2020 and 16 November 2020 in [Minister Faafoi's] capacity as Minister of Broadcasting, Communications and Digital Media from ... the Department of the Prime Minister and Cabinet (DPMC)…"*

I note I last wrote to you on 23 December 2020, where I advised some documents had been withheld in full and extended the timeframe for responding to the remainder of your request by 20 working days. Following this, I am now in a position to further respond.

Please find enclosed the following documents:

	Title	**Date**
1.	Briefing: Draft international statement on end-to-end encryption and public safety: *[title partially withheld under section 6(a)]*	23 September 2020
2.	Briefing: Cyber Security Trades Pathway	2 October 2020
3.	Briefing: Attendance at Singapore International Cyber Week: New Zealand Statement	5 October 2020
4.	Communications Approach: International Statement: End-to-End Encryption and Public Safety	8 October 2020

Executive Wing, Parliament Buildings, Wellington, New Zealand 6011
☎ 64 4 817 9698 www.dpmc.govt.nz

I have decided to release the documents listed above, subject to information being withheld under the following sections of the Act, as applicable:

- Section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand;
- Section 6(b)(i), to protect the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government;
- Section 9(2)(a), to protect the privacy of individuals;
- Section 9(2)(b)(ii), to protect the commercial position of the person who supplied the information, or who is the subject of the information;
- Section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials; and
- Section 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinion.

In making my decision, I have taken the public interest considerations in section 9(1) of the Act into account.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on DPMC's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely

Tony Lynch
Deputy Chief Executive
National Security Group

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

Briefing

DRAFT INTERNATIONAL STATEMENT ON END-TO-END ENCRYPTION AND PUBLIC SAFETY: 6(a)

To

Prime Minister / Minister for National Security and Intelligence (Rt Hon Jacinda Ardern)
Minister of Foreign Affairs (Rt Hon Winston Peters)
Minister of Justice / Minister Responsible for the GCSB & NZSIS (Hon Andrew Little)
Minister of Police (Hon Stuart Nash)
Minister of Broadcasting, Communications and Digital Media (Hon Kris Faafoi)
Minister of Internal Affairs (Hon Tracey Martin)

Date	23/09/2020	**Priority**	Urgent
Deadline	28/09/2020	**Briefing Number**	2021NSP/012

Purpose

To recommend a course of action on 6(a) a draft international statement on end-to-end encryption and public safety. 6(a)

Recommendations

1. **Note** that New Zealand has been asked 6(a) to support an international statement on end-to-end encryption and public safety;
2. **Note** 6(a)
3. **Note** 6(a)
4. **Note** that, following ministerial direction, officials indicated New Zealand's agreement to support 6(a) ;

5. **Note** that at this stage 6(b)(i) [redacted]

6. **Note** that 6(b)(i) [redacted]

7. **Note** that officials have directly engaged with:

   a. 9(2)(b)(ii) [redacted]

   b. 6(b)(i) [redacted]

8. **Note** that officials recommend, on balance, signing the 6(a) [redacted]

9. **Agree** that New Zealand signs the statement 6(a) [redacted] **YES / NO**

   OR

10. **Agree** that Ministers meet (in person or via VTC) to discuss signature and timing of the statement and the extent of any supporting messaging. **YES / NO**

Tony Lynch **Deputy Chief Executive,** **National Security Group, DPMC** *…/…/..2020*	Rt Hon Jacinda Ardern **Prime Minister / Minister for National Security and Intelligence** …../…../….
	Rt Hon Winston Peters **Minister of Foreign Affairs** …../…../….

Hon Andrew Little **Minister of Justice** **Minister Responsible for the GCSB & NZSIS**
…../…../….
Hon Stuart Nash **Minister of Police**
…../…../….
Hon Kris Faafoi **Minister of Broadcasting, Communications and Digital Media**
…../…../….
Hon Tracey Martin **Minister of Internal Affairs**
…../…../….

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Tony Lynch	Deputy Chief Executive, National Security Group	Mobile: 9(2)(a)	
Sophie Vickers	Team Manager, National Cyber Policy Office	Mobile: 9(2)(a)	✓

Minister's office comments:

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

DRAFT INTERNATIONAL STATEMENT ON END-TO-END ENCRYPTION AND PUBLIC SAFETY: 6(a)

Purpose

1. This briefing recommends a course of action on 6(a) a draft international statement on end-to-end encryption and public safety. This advice follows 6(a) our own discussions with technology companies and other nations.

6(a) international statement on encryption and public safety

2. 6(a), 6(b)(i)

3. 6(a)

4. 6(a), 6(b)(i)

5. 6(a), 6(b)(i)

6(a)

6. 6(a), 6(b)(i)

7. 6(b)(i)

8. 6(b)(i) [redacted]

9. 6(b)(i) [redacted]

10. 6(b)(i) [redacted]

11. 6(b)(i) [redacted]

Progress on the text of the draft statement

12. 6(a), 6(b)(i) [redacted]

6(b)(i) [redacted]

Officials recommend signing the statement as part of managed communications on adapting to ubiquitous encryption

13. On balance officials favour signing the statement given the following considerations.

6(b)(i), 9(2)(g)(i) [redacted]

16. The statement usefully underlines that the wider industry should expect an upcoming policy dialogue on solutions for lawful access to the content of communications and for content moderation.

6(b)(i), 9(2)(g)(i) [redacted]

17. 6(b)(i), 9(2)(g)(i) [redacted]

18. 6(b)(i), 9(2)(g)(i) [redacted]

6(b)(i), 9(2)(g)(i) [redacted]

19. 6(b)(i), 9(2)(g)(i) [redacted]
The statement follows on from our previous support for Five Country Ministerial communications on cybercrime and public safety. New Zealand's cyber security strategy notes that we will continue to work with others on issues relating to encryption, including ensuring law enforcement can access the information it needs while balancing rights to privacy and security.

20. 6(b)(i), 9(2)(g)(i) [redacted] New Zealand will need to ensure that the statement, and our messaging around it, reflects and is consistent with New Zealand's longstanding support for an open, free and secure internet, as well as our commitment to proactively tackle cybercrime and the application of international human rights law online.

Conclusion

21. 6(a), 9(2)(g)(i) [redacted]

22. 9(2)(g)(i) [redacted]

6(a) [redacted]

Next steps

25. 9(2)(g)(i) [redacted]

26. 9(2)(f)(iv) [redacted]

Consultation

27. New Zealand Police, DIA, GCSB and NZSIS (Joint Director Generals' Office), MFAT, MBIE and MoJ were consulted on this paper.

Attachments:		
Attachment A:	In Confidence	Draft International Statement on Encryption

ATTACHMENT A

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

Briefing

CYBER SECURITY TRADES PATHWAY

To: **Minister of Broadcasting, Communications and Digital Media** (Hon Kris Faafoi)			
Date	2/10/2020	**Priority**	Routine
Deadline	16/10/2020	**Briefing Number**	2021NSP/011

Purpose

1. This note provides analysis of the proposals by 9(2)(a) [redacted] to expand the Targeted Training and Apprenticeships Fund to include the cybersecurity diploma and graduate diploma, 9(2)(f)(iv) [redacted] The proposal supports delivery of the workforce and ecosystem priority of the Cyber Security Strategy 2019.

Recommendations

1. **Agree** that NCPO continue to work with the Tertiary Education Commission to investigate options for cyber security to be added to the list of approved target areas for the Targeted Training and Apprenticeships Fund; **YES / NO**
2. **Agree** 9(2)(f)(iv) [redacted] **YES / NO**
3. **Agree** 9(2)(f)(iv) [redacted]; and **YES / NO**
4. **Sign** the letter at attachment A. **YES / NO**

By email Sophie Vickers **Team Manager, Cyber Policy**	Hon Kris Faafoi **Minister of Broadcasting, Communications and Digital Media**
2 October 2020	…../…../….

Contact for telephone discussion if required:

Name	Position	Telephone		1st contact
Sophie Vickers	Team Manager	9(2)(a)	9(2)(a)	✓
9(2)(a)	Principal Policy Advisor	9(2)(a)	9(2)(a)	

Minister's office comments:

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

CYBER SECURITY TRADES PATHWAY

Background

1. 9(2)(a) [redacted] wrote to you on 26 August 2020 on expanding the Trades Pathway to include the Level 6 cybersecurity diploma, 9(2)(f)(iv) [redacted]

Current cyber security qualification options

2. The number of study options for cyber security has grown over the 2019-20 time period. Currently the NZQA has five qualifications dedicated to cyber security:

    - a New Zealand Diploma in Cybersecurity (level 6)
    - three Graduate Diplomas in Cybersecurity (level 7)
    - a Master of Cyber Security (level 9)

3. Other Graduate and Postgraduate level study options in Computer Science and Information Technology have components that specialise in IT security. There also exist several industry-led professional qualifications. Some of which are curated by cyber security professional societies. Others are offered by large-scale technology companies, often drawing on or working with their proprietary technologies.

4. For the 2021 academic year there are four cyber security study offerings at NZQA levels 6 and 7, provided by three Institutes of Technology:

    - Unitec: offers a diploma in cyber security at their Mt Albert campus;
    - Toi Ohomai Institute of Technology: offers a graduate diploma in Rotorua; and
    - WelTec: offers both a graduate diploma and graduate certificate in cyber security in Petone.

5. Uptake of cyber security study into the curricula of regional Institutes of Technology is proving challenging. This may be due to timing as Institutes of Technology and Polytechnics (ITPs) are amid the most significant changes to vocational learning in the last 25 years, which includes the bringing together of all 16 ITPs, under the recently established New Zealand Institute of Skills and Technology (NZIST)[1] along with sector wide reforms designed to create a strong, unified, sustainable vocational education system that is fit for the future of work, and that delivers the skills that learners, employers and communities need.

[1] New Zealand Institute of Skills and Technology (NZIST) is an interim name until a permanent name has been chosen.

Targeted Training and Apprenticeship Fund

6. The Targeted Training and Apprenticeship Fund[2] (TTAF; also known as free trades training) was announced as part of Budget 2020 and supports learners to undertake vocational education and training in high-demand areas, without fees. It is designed for both school leavers and people looking to reskill.

7. TTAF encompasses a range of training and apprenticeship programmes at sub-degree level free for learners from July 2020 until 31 December 2022. It is targeted towards industry skill needs where demand from employers for these skills is strong, or is expected to grow, during New Zealand's recovery period from the impacts of COVID-19.

8. Study currently covered by the TTAF includes:

    - all apprenticeships;
    - diploma and certificate programmes in targeted areas delivered by tertiary providers; and
    - industry training (outside of apprenticeships) in targeted areas that include: primary industries, construction, community support, manufacturing, mechanical and electrical engineering and road transport.

Potential to include cyber security training in the TTAF

9. Cyber security training is currently not included in the scheme. The process for including additional target areas is yet to be finalised. NCPO is in discussion with the Tertiary Education Commission (TEC) to include cyber security as a targeted area.

10. Including cyber security in the approved list will save students around $6,500 each and may attract people from a range of circumstances and stages of their lives to the cyber security workforce.

11. New Zealand's economic recovery from COVID provides an opportunity to address the gap in cyber security roles. Attracting career changers to the cyber security industry would provide a new pipeline of talent, bringing valuable associated skills to the profession.

9(2)(f)(iv) [redacted]

12. A key benefit of the vocational model of the cyber security diploma are the internships that it offers. Internship placement opportunities and assurance around appropriate mentoring of interns requires a significant amount of engagement and liaison with the cyber security industry. *9(2)(f)(iv), 9(2)(g)(i)* [redacted]

13. *9(2)(f)(iv)* [redacted]

[2] https://www.tec.govt.nz/funding/funding-and-performance/funding/fund-finder/targeted-training-and-apprenticeship-fund/

14. 9(2)(f)(iv) [redacted]

15. 9(2)(f)(iv), 9(2)(g)(i) [redacted]

9(2)(f)(iv) [redacted]

16. 9(2)(f)(iv) [redacted]

17.

18.

19.

ATTACHMENT A

Letter to 9(2)(a) regarding the inclusion of the Cybersecurity Diploma for the Trades Pathway – Attached below

Hon Kris Faafoi

MP for Mana

Minister of Broadcasting, Communications and Digital Media
Minister for Government Digital Services
Minister of Commerce and Consumer Affairs
Minister of Immigration

Associate Minister of Housing (Public Housing)

9(2)(a)
9(2)(a)
By email: 9(2)(a)
Copied to: 9(2)(a)

Ref: BCDM 2020-005

Dear 9(2)(a)

Thank you for your letter on 26 August 2020 regarding the inclusion of the Cybersecurity Diploma for the Trades Pathway.

I'm glad to hear that the New Zealand Diploma in Cybersecurity has been a success and has placed 30 students in cyber security roles, and that the second semester is fully subscribed. I'm also encouraged to see further cyber security Graduate Diploma options become available for the coming academic year.

A priority area in New Zealand's Cyber Security Strategy 2019 is to have a strong and capable cyber security workforce and ecosystem.

The National Cyber Policy Office (NCPO) is focused on cyber security workforce development in their forward work, and I have recently instructed the office to:

- investigate options to have cyber security added to the list of approved target areas for the Targeted Training and Apprenticeships Fund;
- 9(2)(f)(iv) ; and
- 9(2)(f)(iv)

I appreciate your interest and ongoing efforts in this space.

Yours sincerely

Hon Kris Faafoi
Minister of Broadcasting, Communications and Digital Media

Contact for telephone discussion if required:

Name	Position	Telephone		1st contact
Sophie Vickers	Team Manager	9(2)(a)	9(2)(a)	✓
9(2)(a)	Principal Advisor	9(2)(a)	9(2)(a)	

Minister's office comments:

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

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

BRIEFING

ATTENDANCE AT SINGAPORE INTERNATIONAL CYBER WEEK: NEW ZEALAND STATEMENT

To: Minister of Broadcasting, Communications and Digital Media (Hon Kris Faafoi)			
Date	5/10/2020	**Priority**	Routine
Deadline	7/10/2020	**Briefing Number**	2021NSP018

Purpose

This briefing provides information on Singapore International Cyber Week, ahead of your participation in the ASEAN Ministerial Conference on Cybersecurity Special Session with Dialogue Partners on 7 October. Attached to the brief is a statement to use at this event.

Recommendations

We recommend that you:

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

Tony Lynch **Deputy Chief Executive, National Security Group**		Hon Kris Faafoi **Minister of Broadcasting, Communications and Digital Media**
…../…../2020		…../…../2020

ATTENDANCE AT SINGAPORE INTERNATIONAL CYBER WEEK: NEW ZEALAND STATEMENT

Background

1. Singapore has invited you to participate in Singapore International Cyber Week (SICW), which is being held from 5-9 October 2020. Singapore began hosting SICW in 2016. It has become a key feature of the international cyber calendar, and has bolstered Singapore's reputation as an active and influential player in international cyber issues.
2. You have agreed to participate in the ASEAN Ministerial Conference on Cybersecurity (AMCC) Special Session with Dialogue Partners[1], on 7 October.
3. This will be the first time New Zealand has been represented at Ministerial level at SICW. New Zealand has participated in SICW at officials' level in previous years.

Objectives for participation

4. The objectives for your participation in this session are to:
   - highlight New Zealand's support for ASEAN's cyber security initiatives and efforts;
   - highlight New Zealand's contribution to cyber security capacity-building in the region, including through the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE);
   - contribute to discussions on norms of responsible state behaviour online, 6(a) particularly in the context of COVID-19;
   - 6(a)
   - hear about other ASEAN member states' cyber security priorities; and
   - discuss opportunities for closer cooperation 6(a) on international cyber issues, particularly in the context of COVID-19.

Timing, format, and theme

5. The session is being held from 9.00pm – 10.30pm NZT on Wednesday 7 October. You have been invited to give a 3 minute intervention to share New Zealand's views on areas of cyber cooperation.
6. Interventions will be made in groups of 3-4, in alphabetical order, followed by a 10 minute discussion. The allocated timeslot for New Zealand's presentation is 10.10pm NZT.

[1] ASEAN Dialogue Partners are: Australia, Canada, China, India, Japan, Republic of Korea, New Zealand, Russia, United States, and the European Union.

7. Singapore has advised that the topic for discussion is "Enhancing Regional Cyber Cooperation in a New Normal". The focus will be on "identifying areas in which ASEAN Member States and Dialogue Partners can work together to build stronger regional cyber policy coordination and incident response, with lessons drawn from the current pandemic."

8. A statement for use in the session is included as Attachment A.

Participants

9. Supporting your participation in this session will be Tony Lynch, Deputy Chief Executive of the National Security Group in the Department of the Prime Minister and Cabinet (DPMC). DCE Lynch will be able to answer any questions you having during the event, and can be contacted on 9(2)(a) . DCE Lynch will also represent New Zealand in your place once you depart the event, as you have indicated you may need to leave before it has concluded.

10. An official from the Ministry of Foreign Affairs and Trade (MFAT) will also participate in the event, but will be listening in only.

11. At this stage other confirmed participants in this session include the ASEAN Secretary-General, and a range of Ministers and Senior Officials from ASEAN Member States and other Dialogue Partner countries. A draft list of participants is included as Attachment B.

12. Along with your participation in this session, officials from DPMC (NCPO) and MFAT will be participating in other sessions during the week.

Dial in instructions

13. All of Singapore International Cyber Week, including this session, is being held virtually.

14. This session is being held via Zoom. You can link to the Zoom session at: 9(2)(g)(i)

15. When entering your details for the Zoom profile for this session, 9(2)(g)(i)

16. Singapore has asked if you can dial in 15 minutes early, at 8.45pm, in order to do an audio and video check prior to the session formally commencing.

17. Singapore has provided a Participants' Guide for the session, which includes further details about connecting. This can be found at Attachment C. Please note that this Guide is for the full ASEAN Ministerial Conference on Cybersecurity (encompassing an ASEAN-only event, as well as the subsequent Special Session with Dialogue Partners) and therefore may include reference to times that are not applicable to your session.

6(a)

Attachments:	Classification:	
Attachment A:	UNCLASSIFIED	Statement for ASEAN Ministerial Conference on Cybersecurity Special Session with Dialogue Partners
Attachment B:	IN CONFIDENCE	Draft list of participants
Attachment C:	IN CONFIDENCE	ASEAN Ministerial Conference on Cybersecurity Special Session with Dialogue Partners Participants' Guide

Attachments B and C withheld under section 6(a)

Attachment A

ASEAN Ministerial Conference on Cybersecurity Special Session with Dialogue Partners

"Enhancing Regional Cyber Cooperation in a New Normal"

New Zealand Statement

[As appropriate/desired]
Ka nui te mihi ki a koutou.
Tena koutou, tena koutou, tena tatou katoa.

His Excellency the ASEAN Secretary General; Honourable Ministers; distinguished colleagues and delegates.

I am very pleased to represent New Zealand at this Special Session of the ASEAN Ministerial Conference on Cyber Security.

I would like to give special thanks to the government of Singapore for convening this discussion in these challenging global circumstances.

It is critical that we continue international cooperation on cybersecurity as we respond to COVID-19.

The pandemic has highlighted our increasing reliance on digital technologies. Lockdown periods and social distancing have accelerated and broadened use of, and dependence on, online communications and technology.

In New Zealand, we saw a significant increase in reporting of phishing, scams and frauds in the first half of this year. We believe this is in part due to cyber criminals taking advantage of more people being online and working from home.

In response to this, we have worked with partners across government, the private sector, and other stakeholder groups to build cyber awareness across New Zealand.

At the same time, globally, there have been multiple overseas reports of sophisticated actors targeting information, research, and infrastructure central to the COVID-19 response.

New Zealand has joined partners in condemning this sort of activity. The targeting of such systems in any country, at any time is unacceptable. It is particularly deplorable in the midst of the current global health crisis. New Zealand will continue to respond to such irresponsible activity where we see it.

It is because of this context that our continued cooperation on cybersecurity, and in particular responsible behaviour online, are so important.

I want to congratulate ASEAN Ministers for their ongoing leadership in this area, particularly through the endorsement and implementation of the norms of responsible state behaviour online.

I also wish to acknowledge ASEAN Members and Dialogue Partners' active contribution to multilateral processes, such as the United Nations Open Ended Working Group.

Our work together in this group is essential for strengthening the existing framework of responsible state behaviour online, and ultimately for ensuring all countries are able to benefit from a secure and stable online environment. We look forward to working with partners to deliver an OEWG report that brings about tangible, practical benefits for all states.

I would like to reiterate New Zealand's commitment to regional processes on cybersecurity cooperation, such as discussions at the ASEAN Regional Forum. A number of Ministers at the recent ARF Foreign Ministers' Meeting noted the heightened significance of cybersecurity risks at this time. It will be important to continue these meetings virtually, until we can meet again in person, as they are a key venue for building regional trust and confidence.

Finally, I wish to highlight the important role capacity-building plays in regional cyber security cooperation. It is critical that we each have the capacity to develop the kind of cyber resilience we need to harness the benefits of online connectivity, and to emerge from the current pandemic.

To this end, I was pleased to announce last year New Zealand's $10 million programme of cyber security capacity-building for our Pacific Island partners.

New Zealand also welcomes the ongoing work of Singapore's ASEAN Cyber Centre of Excellence, and we are committed to working together with the Centre to ensure we are taking a truly regional approach to building cyber capability. I am pleased that CERT NZ will work with the Centre to deliver a workshop next year.

We have already had a taste of what this type of collaboration can look like with CERT NZ, AP-CERT, and Malaysia CERT recently working together to deliver a remote training workshop as part of a wider remote capacity building series with the Pacific incident response community.

Cyber security issues are not easy. And we around this table do not always agree on how best to take forward international cooperation in this area. But we owe it to our collective security, prosperity and – in the current circumstances – health, to continue this conversation and find common ground and build trust wherever possible. New Zealand commits to this, and I look forward to working with you all as we confront this difficult issue.

6(a)

6(a)

6(a)

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

Communications Approach

INTERNATIONAL STATEMENT: END-TO-END ENCRYPTION AND PUBLIC SAFETY

To

Minister of Justice / Minister Responsible for the GCSB and NZSIS (Hon Andrew Little)

Cc:
Prime Minister / Minister for National Security and Intelligence (Rt Hon Jacinda Ardern)
Minister of Foreign Affairs (Rt Hon Winston Peters)
Minister of Police (Hon Stuart Nash)
Minister of Broadcasting, Communications and Digital Media (Hon Kris Faafoi)
Minister of Internal Affairs (Hon Tracey Martin)

Date	8/10/2020	**Priority**	Urgent
Deadline	9/10/2020	**Briefing Number**	2021NSP/019

Purpose

To recommend a communications approach to support New Zealand's signing of the *International Statement: End-to-End Encryption and Public Safety* (the statement) alongside Australia, Canada, India, Japan, the United Kingdom (UK) and the United States (US).

6(a) [redacted]

Recommendations

1. **Note** that Ministers have agreed to support 6(a) [redacted] *International Statement: End-to-End Encryption and Public Safety*;
2. **Note** 6(a) [redacted]
3. **Note** 6(a) [redacted]

4. **Agree** to sign the statement in your capacity as Minister of Justice and Minister responsible for the GCSB and NZSIS; **YES / NO**

5. **Agree** 9(2)(g)(i) ; and, **YES / NO**

6. **Forward** this brief to other Ministers with an interest in encryption. **YES / NO**

Tony Lynch **Deputy Chief Executive,** **National Security Group, DPMC**	Hon Andrew Little **Minister of Justice** **Minister Responsible for the GCSB and NZSIS**

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Tony Lynch	Deputy Chief Executive, National Security Group	Mobile: 9(2)(a)	
Sophie Vickers	Team Manager, National Cyber Policy Office	Mobile: 9(2)(a)	✓

Minister's office comments:

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

Background

1. In accordance with Ministerial agreement, 6(a) New Zealand will sign the *International Statement: End-to End Encryption and Public Safety* (attached as Appendix One). 6(a)

2. 6(a) 6(b)(i)

3. 6(a) 6(b)(i)

4. Officials recommend a low-key approach domestically so that the statement is not mischaracterised as a change in domestic policy.

New Zealand's communications approach

5. New Zealand's Cyber Security Strategy states that we will continue to work with others on issues related to encryption: ensuring that law enforcement can access the information it needs while balancing the rights of New Zealanders to protect their privacy and security. This is part of the Strategy's priority to "proactively address cybercrime". The Strategy also notes that strong encryption is a fundamental element of good cyber security, which is increasingly critical to New Zealand's national security and economic prosperity.

6. The Five Country Ministerial (FCM) June 2020 meeting's communiqué stated:

> *…we discussed the vital importance of collaboration between governments and the digital industry to address concerns with end-to-end encryption where it impacts public safety and the lawful access to information necessary to prevent or investigate serious crimes. We continue to urge technology companies to make real progress on this issue and work with governments in a meaningful way to resolve this challenge in ways that protect our citizens. We will continue to work with like-minded international partners and institutions to ensure complementary approaches to this issue.*

7. In line with these statements, it is proposed that New Zealand characterise our support for the statement as a continuation of current positions on law enforcement and collaboration with industry. Our reasoning for signing this new statement is to underline to the wider technology industry that we expect it to engage meaningfully on developing solutions for lawful enforcement to continue to investigate and prosecute serious crime in a changing technology landscape.

8. We also propose emphasising that our support for the statement is not about any individual firm. Most major firms have expressed a willingness to work on technical mitigations in support of public safety issues and we need this to continue and expand.

9. 9(2)(g)(i) [redacted]

Stakeholder engagement

10. Organisations with a potential interest in the statement may include those with an interest in privacy, civil liberties groups, and firms whose business depends on strong encryption and customer expectations of privacy and security, 6(a) [redacted]. Reactive talking points are attached as Appendix Three.

11. 9(2)(g)(i) [redacted]

12. Engagement with other NGOs and industry should be on a reactive basis as required. Proactive engagement with these groups may give a false impression that the statement represents a change in existing policy.

6(a) [redacted]

13. 6(b)(i) [redacted]

14. 6(b)(i) [redacted]

15. 6(b)(i) [redacted]

Consultation

16. The Ministry of Foreign Affairs and Trade, and the JDGO of the GCSB and NZSIS have been consulted on this brief.

Appendix One

INTERNATIONAL STATEMENT: END-TO-END ENCRYPTION AND PUBLIC SAFETY

We, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. It also serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people, as stated in the 2017 resolution of the UN Human Rights Council[1]. Encryption is an existential anchor of trust in the digital world and we do not support counter-productive and dangerous approaches that would materially weaken or limit security systems.

Particular implementations of encryption technology, however, pose significant challenges to public safety, including to highly vulnerable members of our societies like sexually exploited children. We urge industry to address our serious concerns where encryption is applied in a way that wholly precludes any legal access to content. We call on technology companies to work with governments to take the following steps, focused on reasonable, technically feasible solutions:

- Embed the safety of the public in system designs, thereby enabling companies to act against illegal content and activity effectively with no reduction to safety, and facilitating the investigation and prosecution of offences and safeguarding the vulnerable;
- Enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight; and
- Engage in consultation with governments and other stakeholders to facilitate legal access in a way that is substantive and genuinely influences design decisions.

IMPACT ON PUBLIC SAFETY

Law enforcement has a responsibility to protect citizens by investigating and prosecuting crime and safeguarding the vulnerable. Technology companies also have responsibilities and put in place terms of service for their users that provide them authority to act to protect the public. End-to-end encryption that precludes lawful access to the content of communications in any circumstances directly impacts these responsibilities, creating severe risks to public safety in two ways:

1. By severely undermining a company's own ability to identify and respond to violations of their terms of service. This includes responding to the most serious illegal content and activity on its platform, including child sexual exploitation and abuse, violent crime, terrorist propaganda and attack planning; and
2. By precluding the ability of law enforcement agencies to access content in limited circumstances where necessary and proportionate to investigate serious crimes and protect national security, where there is lawful authority to do so.

Concern about these risks has been brought into sharp focus by proposals to apply end-to-end encryption across major messaging services. UNICEF estimates that one in three internet users is a child. The WePROTECT Global Alliance – a coalition of 97 countries, 25 of the largest companies in the global technology industry, and 30 leading civil society organisations – set out

[1] https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement

clearly the severity of the risks posed to children online by inaccessible encrypted services in its 2019 Global Threat Assessment: "Publicly-accessible social media and communications platforms remain the most common methods for meeting and grooming children online. In 2018, Facebook Messenger was responsible for nearly 12 million of the 18.4 million worldwide reports of [child sexual abuse material to the US National Center for Missing and Exploited Children (NCMEC)]. These reports risk disappearing if end-to-end encryption is implemented by default, since current tools used to detect [child sexual abuse material] do not work in end-to-end encrypted environments."[2] On 3 October 2019 NCMEC published a statement on this issue, stating that: "If end-to-end encryption is implemented without a solution in place to safeguard children, NCMEC estimates that more than half of its CyberTipline reports will vanish."[3] And on 11 December 2019, the United States and European Union (EU) issued a joint statement making clear that while encryption is important for protecting cyber security and privacy: "the use of warrant-proof encryption by terrorists and other criminals – including those who engage in online child sexual exploitation – compromises the ability of law enforcement agencies to protect victims and the public at large."[4]

RESPONSE

In light of these threats, there is increasing consensus across governments and international institutions that action must be taken: while encryption is vital and privacy and cyber security must be protected, that should not come at the expense of wholly precluding law enforcement, and the tech industry itself, from being able to act against the most serious illegal content and activity online.

In July 2019, the governments of the United Kingdom, United States, Australia, New Zealand and Canada issued a communique, concluding that: "tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can gain access to data in a readable and usable format. Those companies should also embed the safety of their users in their system designs, enabling them to take action against illegal content."[5] On 8 October 2019, the Council of the EU adopted its conclusions on combating child sexual abuse, stating: "The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full respect of privacy and fair trial guarantees consistent with applicable law."[66]

The WePROTECT Global Alliance, NCMEC and a coalition of more than 100 child protection organisations and experts from around the world have all called for action to ensure that measures to increase privacy – including end-to-end encryption – should not come at the expense of children's safety[7].

---

2 WePROTECT Global Alliance, 2019 Global Threat Assessment, available online at: <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-+Global+Threat+Assessment.pdf>,

3 http://www.missingkids.org/blog/2019/post-update/end-to-end-encryption

4 https://www.consilium.europa.eu/en/press/press-releases/2019/12/11/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting/

5 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf

6 https://data.consilium.europa.eu/doc/document/ST-12862-2019-INIT/en/pdf

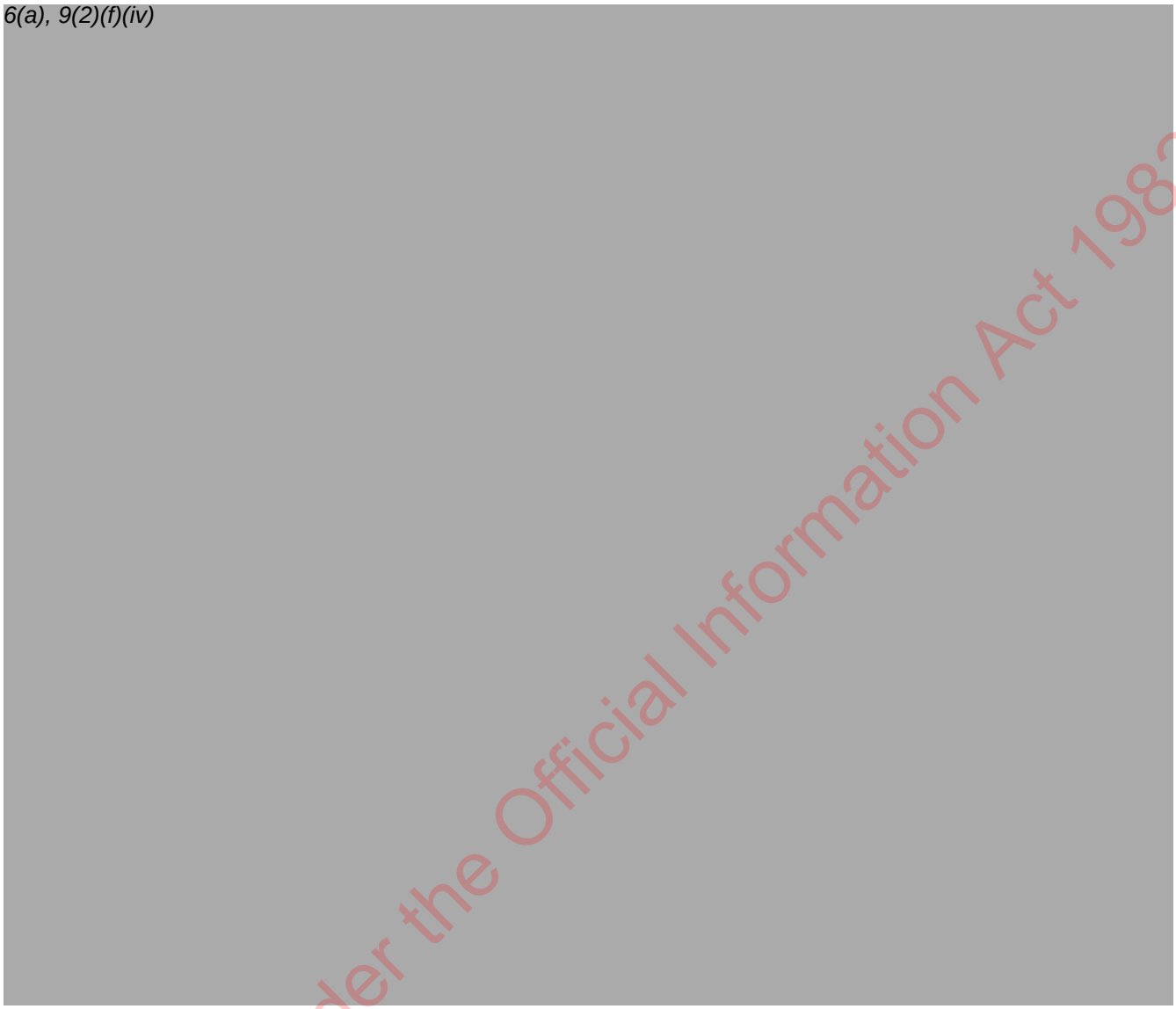
7 http://www2.paconsulting.com/rs/526-HZE-833/images/WePROTECT%202019%20Global%20Threat%20Assessment%20%28FINAL%29.pdf?_ga=2.109176709.1865852339.1591953966-1877278557.1591953966, http://www.missingkids.org/blog/2019/post-update/end-to-end-encryption, https://www.nspcc.org.uk/globalassets/documents/policy/letter-to-mark-zuckerberg-february-2020.pdf

CONCLUSION

We are committed to working with industry to develop reasonable proposals that will allow technology companies and governments to protect the public and their privacy, defend cyber security and human rights and support technological innovation. While this statement focuses on the challenges posed by end-to-end encryption, that commitment applies across the range of encrypted services available, including device encryption, custom encrypted applications and encryption across integrated platforms. We reiterate that data protection, respect for privacy and the importance of encryption as technology changes and global Internet standards are developed remain at the forefront of each state's legal framework. However, we challenge the assertion that public safety cannot be protected without compromising privacy or cyber security. We strongly believe that approaches protecting each of these important values are possible and strive to work with industry to collaborate on mutually agreeable solutions.

Appendix Two

6(a), 9(2)(f)(iv)



9(2)(f)(iv), 9(2)(g)(i)

Appendix Three

Reactive Q&A

How is this announcement going to affect New Zealanders and New Zealand companies?

New Zealand's position on encryption has not changed.

The international statement is entirely consistent with New Zealand's previous statements including the Cyber Security Strategy and Five Country Ministerial communiqués.

The announcement reiterates the need for the wider technology industry to work with governments and civil society on ways to enhance the safety and security of New Zealanders.

Will my privacy be protected if we weaken end-to-end encryption?

We're committed to protecting the personal rights and privacy of New Zealanders and support the role encryption has in protecting those rights.

As part of New Zealand's Cyber Security Strategy. we will continue to work with others on issues relating to encryption, including ensuring law enforcement can access the information it needs while balancing rights to privacy and security.

Any steps law enforcement and intelligence agencies take to access encrypted information needs to be in accordance with the law, i.e. under the appropriate warrant.

Are we seeking to create back-door access to communication technology?

New Zealand's position on encryption has not changed. New Zealand's approach to access for law enforcement purposes is set out in legislation and this statement does not propose changes to our legislative settings.

Encryption is vital to security and privacy online. We will continue working with civil society and industry to maintain the safety and security of New Zealanders.

Have we been compelled to sign up to this statement by our Five Eyes partners?

New Zealand's position on encryption has not changed. New Zealand maintains its own policy on encryption. The drafting of the international statement was a collaborative effort and is consistent with New Zealand's existing policy.

Is the statement asking technology firms to breach users' privacy?

The Government is asking the technology industry to uphold existing commitments to work with governments and, where appropriate, civil society on ways to enhance the safety and security of their users.

Current New Zealand legislation, including the Telecommunications (Interception Capability and Security) Act, and the Search and Surveillance Act, provides for lawful access to information, with checks and balances to ensure rights to privacy and due process are upheld. This includes an existing requirement for industry to assist in decrypting telecommunications where it has provided the encryption.