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

24 March 2023

[redacted]

Ref: OIA-2022/23-0568

Dear [redacted]

Official Information Act request relating to Artificial intelligence

Thank you for your Official Information Act 1982 (the Act) request received on 11 February 2023. You requested:

> *These questions are directed to each of - the Ministry for Business, Innovation and Employment (MBIE)- Ministry of Foreign Affairs (MFAT)- the Department of Internal Affairs (DIA); and - the Department of Prime Minister and Cabinet (DPMC) each in their roles as part of the Digital Economy and Communications and in significant actors in the development of artificial intelligence policy and strategy in New Zealand. Please consider each question, though I have indicated where I think there is relevance for a particular department. I would welcome the opportunity to discuss the questions if needed.*
>
> *These questions are posed under the Official Information Act.*
>
> *1. What is New Zealand doing to implement and/or adopt domestically the UNESCO Recommendation on the Ethics of Artificial Intelligence, which was adopted by all member states in November 2021 at the 41st Session of the General Conference attended for New Zealand by Her Exc. Ms Nicola Reid.(Recommendation on the Ethics of Artificial Intelligence - UNESCO Digital Library)Please provide any briefings, reports, papers or filings on this UNESCO recommendation, its effect on New Zealand, and the path to greater domestic adoption. MFAT, MBIE*
>
> *2. Are the New Zealand government departments participating in any international instruments in artificial intelligence including bilateral or multilateral agreements, international guidance or international policies or strategy, whether by an international body or non-governmental organisation. Please provide any briefing papers or reports on those international instruments. MFAT, DPMC*
>
> *3. Does New Zealand have any domestic workstreams looking at what policies and ideas required for future New Zealand to succeed in a world with AI that has greater capabilities - proactive future-facing thinking, researching potential (extreme) effects and how New Zealand will need to adapt. Please send any research, reports or briefings on this work. MBIE, DIA, DPMC*
>
> *4. Are the New Zealand government departments researching the emerging fields of AI Ethics and AI Safety and how they are to be embedded in New Zealand AI policy? MBIE, DIA, DPMC*
>
> *5. What is the next step in AI policy development in New Zealand, please provide any policy briefing papers or reports regarding this. MBIE, DPMC, DIA*

> *6. Will the AI Charter become enforceable or be developed into more stringent regulation of AI? Please provide any policy development, briefing papers or reports that consider this. MBIE*
>
> *7. Does the New Zealand government have a position on responsibility for the safety of AI - for example is a developer responsible for all effects of the AI. DPMC, MBIE*
>
> *8. Please provide any reports or briefings on how is New Zealand considering the effect of quantum computing on encryption in New Zealand. If these do not cover it, please explain the government's roadmap towards the adoption of quantum-level encryption across government, the private sector and civil society.MBIE, DPMC*
>
> *9. May I have a copy of this document that was provided from DPMC to the then Minister holding the Digital Economy and Communications portfolio: 25 Jun 2021 Global Partnership on Artificial Intelligence - Mid-Year Council Meeting. DPMC*
>
> *10. Is there any other relevant information on the development of Artificial Intelligence policy in the department. MBIE, DIA, DPMC MFAT""*

On 21 February 2023 the Department of the Prime Minister and Cabinet (DPMC) sought to clarify part 2 of your request and, more broadly, a specific time period for the entire request. On 28 February 2023 you suggested a narrowed scope of the last 4 – 5 years and a discussion regarding part 2 of the request. As no further correspondence was received from you, DPMC has interpreted your request to be for information produced in the last 5 years and to include formal briefings, policy documents, and any other key documents held by DPMC.

Where questions have been directed to other agencies, I refer you to that agency's response; only material produced by DPMC is included in this response.

In regard to question 8, we hold one document, an assessment report produced by the National Assessments Bureau, entitled 'Quantum technologies: The weird world of tiny things'. The parts of that report relevant to your request are released in full via excerpt in attachment A. Where information has not been released it has been assessed as 'out of scope' of your request.

In regard to question 9 for the document titled 'Global Partnership on Artificial Intelligence – Mid-Year Council Meeting' this document is released in part. Where information is withheld it is done so under the following sections of the Act:

- Section 6(a), likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand
- Section 9(2)(a), to protect the privacy of individuals.

Also identified as relevant to your request are some briefings provided by the DPMC Policy Advisory Group to the Prime Minister. These briefings are provided to the Prime Minister in confidence to support them in their role as leader of the Government and chair of Cabinet. These briefings are withheld in their entirety under the following sections of the Act:

- Section 6(a), likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand
- Section 9(2)(f)(iv), maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials.

- Section 9(2)(g)(i), maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any public service agency or organisation in the course of their duty.

Finally, I have decided under section 15A of the Act to extend the time limits for deciding on question 2 of your request by an additional 10 working days. Consequently, the extended due date for your response will be 11 April 2023.

The extension is required because of the consultation needed to make a decision on your request. Despite the extension, a response will be sent to you as soon as possible.

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 may be published on the Department of the Prime Minister and Cabinet'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

[redacted]

Tony Lynch
Deputy Chief Executive
National Security Group

Briefing

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

GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE – MID-YEAR COUNCIL MEETING

To: Hon Dr David Clark, Minister for the Digital Economy and Communications

Date	25/06/2021	**Priority**	Urgent
Deadline	28/06/2021	**Briefing Number**	2021NSP/121

Purpose

1. To brief you on the upcoming Global Partnership on Artificial Intelligence (GPAI) virtual mid-year Council meeting, to be held from 12.00am - 2.00am on 1 July 2021 (NZT), and to seek your agreement on attendance and New Zealand's positions.

Recommendations

1. **Note** that the mid-year Council meeting for the GPAI is occurring virtually on 1 July 2021;

2. **Agree** to the New Zealand positions for the meeting outlined below; YES/NO

3. **Indicate** whether you prefer to:

a) **Attend** the live session; YES/NO

b) Deliver a **pre-recorded intervention**; or YES/NO

c) Have **officials** attend. YES/NO

Dan Eaton **Director, National Security Policy Directorate**		Hon Dr David Clark **Minister for the Digital Economy and Communications**
25../..6../2021		...../...../2021

Contact for telephone discussion if required:

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

Minister's office comments:

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

GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE – MID-YEAR COUNCIL MEETING

Purpose

2. To brief you on the upcoming Global Partnership on Artificial Intelligence (GPAI) virtual mid-year Council meeting, to be held from 12.00am - 2.00am on 1 July 2021 (NZT), and to seek your agreement on attendance and New Zealand's positions.

Background

3. The GPAI was formally launched in July 2020. New Zealand was one of the founding members, after endorsing its creation during the 2019 meeting of G7 Digital Ministers. It aims to be an international, multi-stakeholder initiative to guide the responsible development and use of artificial intelligence (AI), grounded in human rights, inclusion, diversity, innovation, and economic growth.

4. The GPAI is now fully established with expert working groups undertaking research on a range of topics.

5. Its activities support New Zealand government objectives, including addressing online extremism in support of the Christchurch Call, supporting international human rights law online, and using digital technologies in a way that generates confidence and trust.

6. The upcoming Council meeting provides an opportunity to review the initiative's first year and guide its future.

Your attendance at the mid-year Council meeting

7. The Council meeting will be held at ministerial level, with 'Deputy Minister-level'[1] delegates allowed in their place. You have the option of attending the live session, providing a pre-recorded intervention, or delegating to a senior official.

8. GPAI officials have indications that several ministers, in addition to the relevant Canadian and French ministers (Hon François-Philippe Champagne, Minister of Innovation, Science and Industry and Cédric O, Secretary of State for the Digital Sector, respectively) have confirmed their participation.

9. Attending the live session will be helpful for reinforcing New Zealand's positions on the GPAI's future direction. New Zealand's objectives include ensuring the principles of GPAI are reflected in membership decisions and aligning relevant GPAI workstreams with the Christchurch Call; these could be helpfully influenced by your attendance. Attending the live session is not, however, critical to New Zealand's ongoing participation in or influence on the GPAI.

[1] Deputy-Minister level equates to most senior relevant official in the New Zealand context.

10. Should you attend you will be supported by the Prime Minister's Special Representative on Cyber and Digital, Paul Ash, and an official from the National Cyber Policy Office. An annotated agenda will also be provided.

Decisions for the mid-year Council meeting

11. On 17 June (NZT) the GPAI Steering Committee agreed to make recommendations to the GPAI Council on substantive matters of membership, work planning, and administration. The Secretariat's paper on the key decisions for the Council is attached along with the draft agenda.

Membership engagement and accession

12. Membership is likely to be an ongoing tension for the GPAI. There is a need to balance broad international participation alongside ensuring the GPAI remains focussed on the ethical use of AI, based on human rights and democratic principles (this tension is common to many similar initiatives including, for example, the Christchurch Call) s6(a) [redacted]

13. The Steering Committee has recommended deferring all decisions on membership until the November Council meeting. NZ officials support this approach, as existing GPAI members need to clarify their collective view on the balance between broadening representation and maintaining underpinning values.

14. Given our objectives for the GPAI of establishing international norms for the ethical use of AI, we consider that membership should be restricted to countries that have a good human rights record and adhere to democratic principles. Holding the GPAI to this standard helps to reinforce these values with existing members and to promote human rights and democratic values to other nations.

15. At the working level, some nations' officials have indicated they are keen to broaden the geographic diversity of GPAI members. Geographic diversity provides credibility and can bring important perspectives to the discussion. In some instances, it may bring with it issues around the ability of new members to meet GPAI's standards.

16. Diversity notwithstanding, allowing membership to include nations that are not committed to the ethical use of AI will be unhelpful to the GPAI's goals. Allowing participation by independent experts from these nations, however, can enable diversity and input while maintaining the integrity of the GPAI. It may also assist in gaining civil society commitment within these nations to the ethical use of AI. It will be important in considering any such approaches to assess and manage the potential risk to any independent experts arising from participation.

17. We recommend New Zealand's position on future membership should be that:

    a) membership decisions be deferred until the November Council meeting;

    b) membership should be subject to nations having a good human rights record and adhering to democratic principles; and

c) the use of independent experts can expand geographic diversity without compromising GPAI's founding principles.

GPAI work planning for projects

18. The Steering Committee has proposed that the Council consider continuing the existing themes and adding some additional themes for 2021 projects. Expert working groups, including those involving New Zealand researchers, have already begun the process of standing up research teams for projects under the existing themes.

19. The existing themes for the GPAI's workplan are Responsible AI (including the AI and Pandemic Response subtheme); Data Governance; Future of Work; and, Commercialisation and Innovation. These themes are producing useful outcomes. The Responsible AI theme usefully supports our social media governance objectives under the Christchurch Call.

20. Future themes that appear to have strong support amongst the membership are: climate change; health and life sciences, including pandemics; and, the impact of AI on human rights. These themes are of interest to New Zealand researchers, support wider government priorities and are unlikely to detract from existing work.

21. We recommend that New Zealand agree with the Steering Committee's proposal on work planning.

New Zealand's intervention for the Council meeting

22. All members will be allowed a 2-3 minute intervention on matters relating to GPAI. Officials will draft a statement. We intend to reinforce the messages you conveyed at the previous Council meeting and reiterate the Prime Minister's positive comments about GPAI, made at the Christchurch Call second anniversary summit.

Next Steps

23. Dependant on your decision on attendance, officials will provide you a draft intervention and annotated agenda.

Attachments:	
	Key decisions for the mid-year Council 2021
	Draft agenda for the 2nd Session of the GPAI Council

Attachment A Excerpt

Quantum technologies: The weird world of tiny things

Page 1

A future quantum computer may pose a risk to keeping information and communications secure, especially if an adversary captures encrypted data today and stores it with a view to decrypting it in the future. The timeline to build a quantum computer capable of threatening common Internet encryption is highly uncertain. In anticipation, preparation of new quantum-resistant cryptographic standards is progressing at pace.

Page 3

If engineering, scientific and commercial challenges can be resolved and quantum computing advances towards large-scale quantum computers, the possibility of a future cryptographically-relevant quantum computer poses a national security risk. The primary risk is that information protected by current encryption could be collected by an adversary today and decrypted in the future using a quantum computer (see Annex 4: Secrets at risk in a quantum world). The types of encryption subject to this risk are among those in widespread use today – including those that secure most Internet communications (see sidebar: Keys to the kingdom).

KEYS TO THE KINGDOM

Asymmetric, or public-key, encryption is most at risk to a future quantum computer. This type of encryption is most notably embedded in the protocols intended to make today's Internet secure.

In Internet browsing, quantum-vulnerable encryption is used in two important steps: certifying that a website visited is genuine using a digital signature, and protecting the exchange of a shared secret key that then encrypts the remainder of the communication. In the event that encrypted data is intercepted and stored, a future quantum computer may be able to derive the private key from the corresponding public key and use that to decrypt the shared secret key exchange. Once in possession of these keys, a quantum computer user would be able to decrypt and read the content.

Public-key cryptography is critical to many activities on the Internet. Businesses and the public rely on online banking being safe, and using virtual private networks (VPNs) for secure remote access. Asymmetric encryption is also used in end-to-end encrypted messaging apps, although these use new keys for every message.

Digital signatures are used to prove that software updates are genuine and reliable, and are also a vital part of many cryptocurrency systems. A quantum computer may enable an attacker to steal cryptocurrency from wallets that are not managed according to best practice, or from some dormant wallets that contain large amounts

Quantum risk to encryption

The timeline to a quantum computer capable of solving the mathematics that underpin asymmetric encryption is highly uncertain. But developing encryption that would be resistant to a quantum computer does not depend on quantum computing, and the nature of the potential risk means the mitigation window begins well ahead of the arrival of a capable quantum computer. Developing and transitioning to new encryption schemes takes time and sensitive information may need to remain secure for decades. An open process began in 2016 to design quantum-resistant encryption and is expected to produce new standards in the next two years.

If a sufficiently large, fault-tolerant quantum computer were to be built, applying it to cryptanalysis would impose opportunity costs – it could be more valuable applied to other tasks. In addition, deriving individual keys to decrypt stored data is likely to be time-consuming and worthwhile for only the highest-value information, which may be challenging to identify while still encrypted.

Page 5

States are starting to raise awareness of the approaching need to transition to quantum-resistant cryptography. For consumer Internet security, New Zealand is likely to be highly reliant on Internet browser providers implementing new cryptographic standards in a timely manner. For government, the New Zealand Information Security Manual recognises the risk and notes that government agencies should be prepared to transition away from vulnerable cryptographic standards, possibly in the next two to three years.

Page 9

Annex 5: secrets at risk in a quantum world

The types of encryption in use today to secure Internet communications rely on mathematical difficulty as the means of security. In these encryption schemes the calculations required to find an encryption key would take so long on a classical computer that it is effectively impossible. As classical computing has improved, security has been maintained in most cases by increasing the length of encryption keys. Quantum computers work differently, and have been shown to be able to solve the mathematical problems that underpin public-key cryptography – albeit at a scale significantly smaller than would be needed to derive the keys used in today's cryptography.

The timeline to a cryptographically-relevant quantum computer is highly uncertain, and the qualities required cannot yet be specified. In 2021, research theorised that a single encryption key of one of the types commonly used today (2048-bit RSA) could be derived in around eight hours by a quantum computer with 20 million noisy qubits (more than 150,000 times the number in IBM's current largest device). However, the number of qubits may not be as important as reducing noise or further optimising algorithms. Among experts surveyed about the emergence of a quantum computer capable of breaking the kind of encryption key above, the majority felt it was 50 per cent likely or higher in the next 15 years.

Mitigating the potential risk posed by quantum computing means the mitigation window begins well ahead of the arrival of a capable quantum computer. Developing and transitioning to different encryption methods takes time, and may be difficult to implement where systems are not able to support quantum-resistant cryptography, which generally requires more computational resources than the algorithms they would replace. Some encryption embedded in hardware needs to remain secure over a long lifespan but cannot be updated.

In anticipation of the risk, efforts have begun to find new encryption methods that don't rely on the mathematical problems a quantum computer could easily solve. These new encryption methods are known as ‘post-quantum cryptography’ or ‘quantum-resistant cryptography’. An open process to identify and test new encryption algorithms has been led by the US National Institute for Standards and Technology (NIST) since 2016. In July 2022, the first four candidates for new quantum-resistant encryption algorithms were announced, and NIST is now working to create draft standards for these schemes, with an overall post-quantum cryptographic standard to be finalised in around two years. Testing continues on a further set of algorithms, in an attempt to ensure a diversity of mathematical approaches are available should further advancements in mathematics or computing render some obsolete for use in encryption.

The quantum computing risk to encryption has raised significant concern, but there are some important nuances to consider. If a sufficiently large, fault-tolerant quantum computer were to be produced, applying it to cryptanalytic tasks would impose opportunity costs – it could be more valuable applied to other tasks. Deriving individual keys to decrypt stored data is likely to be so time-consuming as to be worthwhile for only the highest-value information, which may be challenging to distinguish when in encrypted form. Instead of decrypting data, using a quantum computer to compromise or forge digital signatures may provide wide utility as a tool in offensive cyber operations.