



25 October 2022



Ref: OIA-2022/23-0151

Dear 

Official Information Act request relating to Australia's anti-encryption law

Thank you for your Official Information Act 1982 (the Act) request received on 14 September 2022. You requested:

"...I request from DPMC the following in fully searchable format:

- Official documents talk about the "...implications of Australia's controversial "anti-encryption" law... A copy of the most up to date, substantive report or doc or similar in whatever format that addresses these implications*
- A copy of the most up to date, substantive advice in whatever format, provided to agencies or to another party to disseminate, eg the GCDO or similar – bearing in mind as the advice may vary between agencies, that this request is for the advice that pertains to the largest number of the largest major agencies that interact with public data*
- The last two briefings or similar to any Minister about this..."*

The Department of the Prime Minister and Cabinet (DPMC) provided information relating to jurisdictional risk which informed part of a draft Cabinet Paper. This paper is currently expected to be considered by the Cabinet Government Administration and Expenditure Review Committee later this year. As such, this information is withheld in full under the following section of the Act:

- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials.

Additionally, DPMC provided advice regarding the use of Cloud Services for the Parliament Precinct in 'Briefing: Response to Letter from the Speaker of the House of Representatives on Cloud Services'. A copy of this briefing is released to you in part with some information withheld under the following grounds:

- section 6(a), to protect 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;
- section 9(2)(ba)(i), to protect the supply of similar information in the future;
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials; and
- section 9(2)(g)(i), as withholding the information is necessary to maintain the effective conduct of public affairs through the free and frank expression of opinions.

DPMC's Policy Advisory Group also prepared some briefings within scope of your request. These briefings are provided to the Prime Minister in confidence to support her in her role as leader of the Government and chair of Cabinet. The titles and dates of these briefings are withheld in full 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), to protect the entrusting of information to the Government of New Zealand on a basis of confidence;
- section 9(2)(f)(ii), to maintain collective and individual ministerial responsibility;
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by Ministers of the Crown and officials; and
- section 9(2)(g)(i), as withholding the information is necessary to maintain the effective conduct of public affairs through the free and frank expression of opinions.

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**



Briefing

RESPONSE TO LETTER FROM THE SPEAKER OF THE HOUSE OF REPRESENTATIVES ON CLOUD SERVICES

To

Minister of National Security and Intelligence (Rt Hon Jacinda Ardern)

Minister Responsible for the GCSB (Hon Andrew Little)

Minister for the Digital Economy and Communications (Hon Dr David Clark)

Date	30/09/2021	Priority	Routine
Deadline	15/10/2021	Briefing Number	2122NSP/011

Purpose

To provide a draft response to a letter from the Speaker of the House of Representatives on the potential use of Cloud services by the Parliamentary Service, including background and advice on several specific questions raised by the Speaker.

Recommendations

1. **Note** that the Speaker has sought Ministers' opinion on the potential rollout of Cloud-based tools for the Parliamentary Service, including that some Members' information may be stored in Australia before migrating to the onshore Microsoft data centre region.
2. **Note** that Cloud services offer increased functionality, security and cost-effectiveness, but carry some jurisdictional and sovereignty risks that cannot be fully mitigated.
3. In responding to the Speaker, **request** a briefing on the Parliamentary Service's risk assessment, including on risks relating to Ministerial data and proposed mitigations, prior to decisions on Cloud adoption. **YES / NO**
4. **Sign** the letter at Attachment A. **YES / NO**

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

29/09/2021

Rt Hon Jacinda Ardern
**Minister of National Security and
Intelligence**

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

Hon Andrew Little
Minister Responsible for the GCSB

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

Hon Dr David Clark
**Minister for the Digital Economy and
Communications**

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

Released under the Official Information Act 1982

Contact for telephone discussion if required:

Name	Position	Telephone		1st contact
Halia Haddad	Acting Manager, National Cyber Policy Office	DDI s9(2)(a)	Mobile	✓
s6(a)	Principal Policy Advisor, National Cyber Policy Office	DDI	Mobile s9(2)(a)	

Minister's office comments:

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

Released under the Official Information Act 1982

RESPONSE TO LETTER FROM THE SPEAKER OF THE HOUSE OF REPRESENTATIVES ON CLOUD SERVICES

Purpose

1. The Speaker of the House of Representatives has written to seek your views on a possible Parliamentary Service move to Cloud services (Attachment A). This paper provides considerations to inform Ministers' response to the letter. A draft response to the Speaker is included for your consideration (Attachment B).

Cloud services provide significant benefits

2. The usability of the current Parliamentary Information and Communications Technology (ICT) toolset is a source of frustration for users. This can hinder productivity and increase security risk, especially if staff use work arounds and turn to 'shadow Cloud' services.
3. COVID has shown the benefits of Cloud for the public service and New Zealanders more broadly, delivering resilience, continuity, and agility in enabling secure online working and collaboration from home. Our digital economy is increasingly turning to hyperscale Cloud to operate and sustain businesses, and as a platform for local and global growth.
4. Additionally, Cloud adoption is a way of improving government security swiftly and at scale and is a key cyber protection measure in the increasingly sophisticated threat landscape. Cloud adoption is therefore an important part of our digital economy, digital public service and cyber security plans.
5. Finally, the External Independent Review on Bullying and Harassment in the New Zealand Parliamentary Workplace recommended Parliamentary Service and the Department of Internal Affairs consider how best to provide staff with better tools to support flexible working, including ICT systems and devices. Officials assess that a move to Cloud-based tools would assist with meeting that recommendation.

There are risks associated with Cloud services

Security

6. Cloud services are designed to be highly secure and are routinely updated and improved by Cloud providers. The effective management of Cloud services requires specialist skills and knowledge. Where these are lacking, security issues may arise. Cloud security risks are most often realised due to misconfiguration or administrator inexperience with Cloud systems.
7. Officials would encourage the Parliamentary Service to use the New Zealand Information Security Manual (NZISM) Azure Blueprint for their relevant Microsoft Cloud infrastructure. This blueprint provides a means of easily and quickly implementing, and maintaining, NZISM-compliant Cloud infrastructure for Azure services. s6a

s6a

s9(2)(g)(i)

Jurisdictional risk

9. In the context of Cloud services, jurisdictional risks occur where data is subject to the laws of other countries in which Cloud service providers may store, process, or transmit data. Jurisdictional risks may lead to situations incompatible with New Zealand law or that prejudice our national interests. We have included in Attachment C a synopsis on jurisdictional risk.
10. At present, New Zealand does not have local hyperscale Cloud data centres for large data storage. Most Cloud services used by New Zealand agencies are currently based s6(a) . Microsoft and AWS are building data centres to host Cloud services in New Zealand. Microsoft's new data centre region is expected to be operational in early to mid-2023. AWS' facilities are expected to begin operations shortly after this. Other Cloud service providers (Spark/CCL, DCI, Canberra Data Centres, Datagrid) have also expanded, announced plans and/or begun construction of New Zealand facilities.
11. s9(2)(f)(iv) s9(2)(ba)(i)
12. If the Parliamentary Service implemented other Cloud tools, data could also be stored in other jurisdictions and subject to relevant laws in those jurisdictions. Engagement with the providers of such Cloud tools will be necessary to understand where data is transferred, stored, and processed, and to assess the relevant laws to understand jurisdictional risks.

What is special about data held by the Parliamentary Service?

s6a

14. The Parliamentary Service was invited by Cabinet to follow the NZISM and guidance on adoption of Cloud technologies. The NZISM notes that the majority of jurisdictional, sovereignty and privacy risks cannot be wholly and completely managed with controls available today. The agency head or Chief Executive must therefore carefully consider

those risks before adopting Cloud services as, ultimately, it is the responsibility of agencies to assess risks and determine whether they should accept them.

15. Under the Government's Cloud First policy, to move to Cloud services agencies must:
- a) Make Cloud adoption decisions on a case-by-case basis following a risk assessment; and
 - b) Only store data classified at restricted or below in a Cloud service, whether it is hosted onshore or offshore.

s9(2)(f)(iv)

s9(2)(f)(iv)

Māori Data

18. Parliamentary Service holdings are likely to include Māori data. Members may wish to seek advice and assurance from the Parliamentary Service in respect of the implications of Cloud adoption for Māori data held by the Parliamentary Service.
19. We recommend the Parliamentary Service engages with its Te Tiriti partners to work through the specific risks and mitigations associated with Māori data. To support this engagement, the Parliamentary Service may wish to draw on existing frameworks and tools, for example:
- a) Archives New Zealand has produced guidance in setting its approach to management of data in its archival management system that references data location and specific data of interest to iwi/Māori;¹ and
 - b) Stats NZ applied a privacy impact assessment framework while assessing whether to migrate certain systems (excluding the Integrated Data Infrastructure - IDI) to Microsoft Office 365 hosted on infrastructure located in Australia, including drawing upon applicable dimensions of the Ngā Tikanga Paihere guidelines.²

Ecosystem capability vs vendor capture

20. In rolling out Cloud-based tools and services, it is important to consider vendor lock-in and dependency on specific software and updates.

21. s9(2)(g)(i)

¹ Refer to "Cloud Services: Information and records management considerations", available at <https://archives.govt.nz/manage-information/how-to-manage-your-information/digital/cloud-services>

² Available at <https://data.govt.nz/toolkit/data-ethics/nga-tikanga-paihere/>

22. For instance, if the Parliamentary Service decides to offer Microsoft 365, there would be significant benefits to users from collaboration tools beyond traditional productivity tools such as Word, PowerPoint and Excel. Microsoft 365 provides capabilities for collaboration, data analytics, process automation and more.

Conclusion

23. A draft response to the Speaker's letter is enclosed for your consideration reflecting the points discussed above.

Consultation

24. This briefing was prepared by DPMC with input from DIA, GCSB and a letter from Minister Little of 8 July 2021.

Attachments:	
Attachment A:	Letter from the Speaker
Attachment B:	Draft response to the Speaker
Attachment C:	Jurisdictional risk synopsis

Released under the Official Information Act 1982

ATTACHMENT A

Letter from the Speaker



IN CONFIDENCE

Office of the Speaker of the House of Representatives

Rt Hon Jacinda Ardern
Prime Minister

Hon Andrew Little
Minister for Government Communications Security Bureau, and the New Zealand Security Intelligence Service

Hon David Clark
Minister for Digital Economy and Communication

Cloud Services for Parliament

1. This paper sets out a possible Parliamentary Service approach to move to Cloud services and the impact and mitigating actions of members of Parliament and Minister's information as a result of it, and seeks your views.

Background

2. Cabinet endorsed the Government Cloud Acceleration Programme in 2016 (SEC-16-MIN-0026).
3. The Parliamentary Service cooperates with Government initiatives and guidance when it aligns with best practice and does not compromise Parliament's traditional independence from the Government.
4. Current guidance from the Government Chief Digital Officer (GCDO) for organisations requires use public cloud services in preference to traditional IT systems on a 'case-by-case basis, following risk assessments.' As a relatively small entity, the Parliamentary Service recognises there are many benefits that public cloud services provide its users, including ease-of-use, value for money, improved security, and improved choice.
5. In late 2018, the Parliamentary Service suspended its migration to cloud-based productivity tools (Microsoft 365) because of concerns about political and jurisdictional risk posed by the offshore hosting of member emails, as well as perceived limitations on Parliamentary Privilege. Following the decision to suspend that project, the Service also stopped or significantly slowed adoption of other cloud solutions for a time.
6. The Parliamentary Service IT group has continued to work with internal stakeholders, supported by the GCDO, to better quantify and understand the risks and benefits that cloud solutions pose for parliament. It has also met with senior members of other government agencies, including the Ministry of Defence, to understand their approach to managing the risks associated with cloud solutions. They have successfully applied the GCDO's Cloud Risk Assessment framework and information security patterns within Parliamentary Service.
7. Since mid-2018 the Service successfully implemented several cloud based solutions, including the successful roll out of Zoom videoconferencing for members and staff at the

1

RESPONSE TO LETTER FROM THE SPEAKER OF THE HOUSE OF REPRESENTATIVES
ON CLOUD SERVICES

Report No.
2122NSP/011

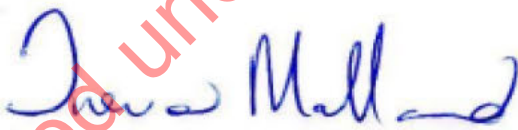
beginning of the COVID-19 lockdown. The cloud services adopted to date have focused primarily on non-Parliamentary or corporate use cases, such as health and safety reporting and customer service management, where risks to Members and Ministers is not a significant factor..

8. In November 2020, I gave approval for a small non-government party and its members to use cloud-based productivity tools (Microsoft 365).
9. In January 2021 the Parliamentary Service Chief Executive and the Clerk of the House of Representatives approved a new rollout of cloud-based productivity tools for core Service Corporate and Office of the Clerk staff respectively. Members, Ministers, and their support staff are currently out of scope of this initiative.
10. There are increasing requests from other parties and members for the rollout of these services to be made widely available.
11. The Parliamentary Service has found it increasingly difficult and costly to deliver required capabilities only on-premises over the past two years. Technology vendors are rapidly shifting investment to cloud products and retiring support for legacy on-premises versions.
12. The Service is currently developing a roadmap to align rollout of cloud-based tools to members, Ministers, and their support staff.
13. The Service will continue to implement public cloud services where they deliver features that Members, Ministers, and their staff need, where they deliver improved security and value for money, and where they do not introduce significant political, security, or jurisdictional risks to Parliament or its Members.
14. While initially some of the members' information would be stored in the offshore facility in Australia, the Service will migrate that information to the onshore Microsoft availability zone, which is currently under construction, as soon as it is launched.

Recommendations

I recommend that you:

1. **Provide your opinion** on the current development by the Service of a roadmap to align rollout of cloud-based tools to members, Ministers, and their support staff.
2. **Provide your opinion** about the fact that while initially some of the members' information may be stored in the offshore facility in Australia, the Service will migrate that information to the onshore Microsoft availability zone, which is currently under construction, as soon as it is launched.
3. **Note** that industry investment trends toward cloud-only solutions will, over time, increase the difficulty to identify new suitable on-premises solutions and increase the cost and risk of maintaining existing, legacy on-premises solutions.



Rt Hon Trevor Mallard
Speaker of the House of Representatives

ATTACHMENT B

Draft response to the Speaker

Dear Speaker,

Thank you for your letter of 21 June. We welcome the opportunity to make suggestions on the development of a roadmap for use of Cloud-based tools by the Parliamentary Service.

Capability considerations

It is important that the Parliamentary Service provides capable and secure ICT tools to Ministers, Members of Parliament and support staff.

The obsolescence of the non-Cloud Parliamentary toolset is a source of tremendous frustration for Members and staff (as encapsulated in Recommendation 58 of the Francis Review). Inadequate work tools hamper productivity but also introduce external security risks, for example when individuals have little choice but to use non-approved apps to get work done.

Better productivity, collaboration and mobility can only be achieved through adoption of Cloud services and should occur as soon as is safely possible.

Cloud security considerations

We agree that the decision to suspend the migration to Cloud-based productivity tools (specifically Microsoft 365) in 2018 was appropriate given the uncertainty around jurisdictional risks.

The Parliamentary Service was invited by Cabinet to follow the New Zealand Information Security Manual (NZISM) and guidance on adoption of Cloud technologies. The NZISM notes that jurisdictional, sovereignty, and privacy risks cannot be wholly and completely managed with the controls available today. Therefore, they should be carefully considered and accepted by the agency head or Chief Executive before the adoption of such Cloud services.

s9(2)(f)(iv)

s6(a) and s9(2)(f)(iv)

s6(a) and s9(2)(f)(iv)

Māori data governance

The Parliamentary Service holdings are likely to include Māori data. Members may wish to seek advice and assurance from the Parliamentary Service in respect of the implications of Cloud adoption for Māori data. We recommend that the Parliamentary Service engage with its Te Tiriti partners to work through the risks and mitigations and refer to existing frameworks and tools used by Stats NZ and Archives New Zealand.

s9(2)(f)(iv)

In summary

s9(2)(f)(iv)

Yours sincerely,

Rt Hon Jacinda Ardern

Minister of National Security and Intelligence

Hon Andrew Little

Minister Responsible for the GCSB

Hon Dr David Clark

Minister for the Digital Economy and Communications

Released under the Official Information Act 1982

Released under the Official Information Act 1982