

# Australia-New Zealand National Security Dialogue 2019

Meeting Papers for New Zealand Attendees

---

6 September 2019

0800 - 1400 hours

Pipitea House, 1-15 Pipitea Street, Wellington

[Page intentionally left blank]

Released under the Official Information Act 1982

## List of Meeting Papers

Tab	Documentation
A.	<b>Context</b> <ul style="list-style-type: none"> <li>• Memorandum - Australian Perspective</li> </ul>
B.	<b>Agenda</b> <ul style="list-style-type: none"> <li>• Annotated Agenda for New Zealand Attendees</li> <li>• Agenda</li> </ul>
C.	<b>New Zealand Interagency Briefing Pack</b> <ul style="list-style-type: none"> <li>• <b>Item 1</b>- Integration of National Security and Economic Decision Making</li> <li>• <b>Item 2</b> - Critical Infrastructure</li> <li>• <b>Item 3</b> - Emerging Technologies               <ul style="list-style-type: none"> <li>○ s6(a) [REDACTED]</li> <li>○ [REDACTED]</li> </ul> </li> <li>• <b>Item 4</b> - Counter Terrorism</li> <li>• <b>Item 5</b> - Foreign Interference</li> </ul>
D.	<b>Administration Documents</b> <ul style="list-style-type: none"> <li>• Administrative Instruction</li> <li>• Biographies - Australian attendees</li> </ul>
E.	<b>2018 Documentation</b> <ul style="list-style-type: none"> <li>• 2018 Joint Note to the Prime Ministers</li> <li>• 2018 Meeting Record (including outcomes)</li> </ul>

[Page intentionally left blank]

Released under the Official Information Act 1982

---

## Tab A: Context

- Memorandum - Australian Perspective

*Four pages withheld in full under sections 6(a) and 6(b)(i)*

*Ten pages removed and refused under section 18(d) as publicly available at [ministers.dese.gov.au/tehan/national-press-club](https://ministers.dese.gov.au/tehan/national-press-club)*

Released under the Official Information Act 1982

---

## Tab B: Agenda

- Annotated Agenda for New Zealand Attendees
- Agenda

Released under the Official Information Act 1982



---

# Australia-New Zealand National Security Dialogue Annotated Agenda for New Zealand Attendees

**Date** 6 September 2019

**Time** 0800 - 1400 hrs

**Venue** s6(a) Pipitea House, 1-15 Pipitea St, Wellington, New Zealand

**Clearance** s6(a) The venue is a SCIF so electronic devices will need to be stored at reception upon arrival.

**Contact** s6(a) or [nssd@dpmc.govt.nz](mailto:nssd@dpmc.govt.nz)

---

## Attendees - Australia

s6(a) Department of the Prime Minister and Cabinet

s6(a) Department of Foreign Affairs and Trade

s6(a) Department of Home Affairs

s6(a) Department of Defence

s6(a) Defence Force

s6(a) Office of National Intelligence

s6(a) Australian Security Intelligence Organisation

s6(a) Australian Secret Intelligence Service

s6(a) Australian Signals Directorate

s6(a) Australian Federal Police

s6(a) Department of the Prime Minister and Cabinet (note taker)

## Attendees - New Zealand

**Brook Barrington**, Chief Executive, Department of the Prime Minister and Cabinet

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

**Andrew Hampton**, Director-General Government Communications Security Bureau

**Carolyn Tremain**, Chief Executive, Ministry of Business, Innovation and Employment

**Andrew Bridgman**, Secretary of Defence

**Chris Seed**, Secretary, Ministry of Foreign Affairs and Trade

**Bill Perry**, Acting Comptroller, New Zealand Customs Service

**Air Marshal Kevin Short**, Chief of the Defence Force

**Hon Dame Annette King**, New Zealand High Commissioner to Australia

**Mike Bush**, Commissioner of New Zealand Police

**Rebecca Kitteridge**, Director-General New Zealand Security Intelligence Service

s9(2)(a) Senior Advisor, National Security Systems Directorate, Department of the Prime Minister and Cabinet (note taker)


#	TIME	DESCRIPTION	LEAD
	0800 - 0815	<b>WELCOME AND REFRESHMENTS</b>	New Zealand
1.	0815 - 0900	<b>INTEGRATION OF NATIONAL SECURITY AND ECONOMIC DECISION MAKING</b> <i>Focus:</i> Growing Economies and Managing Risk Discussion on what each country is doing to integrate and coordinate policies to achieve national security outcomes, while maximising opportunities for economic growth in an increasingly contested global economic and technological environment. <i>Outcomes sought from the session:</i> s6(a)	Australia <i>Lead:</i> PM&C <i>Lead responder:</i> MBIE <i>Support responders:</i> DPMC, MFAT, GCSB
2.	0900 - 1000	<b>CRITICAL INFRASTRUCTURE</b> <i>Focus:</i> Threats to Critical Infrastructure Discussion about the key threats to critical infrastructure that each country needs to manage, and possible methods for doing this. <i>Outcomes sought from the session:</i> s6(a)	New Zealand <i>Lead:</i> MBIE <i>Support presenters:</i> DPMC, MFAT, GCSB <i>Lead responder:</i> Home Affairs
	1000-1015	<b>MORNING TEA</b>	

Released under the Official Information Act 1982



3.	1015 - 1030  1030 - 1130	<b>EMERGING TECHNOLOGIES</b> s6(a) 	Australia <b>Lead:</b> Office of National Intelligence, Home Affairs, Australian Security Intelligence Organisation, Australian Secret Intelligence Service <b>Lead responders:</b> GCSB, MBIE, DPMC <b>Support presenters:</b> MFAT
----	--------------------------------------	--	---

Released under the Official Information Act 1982

4.	1130 - 1215	<p><b>COUNTER TERRORISM</b></p> <p><i>Focus:</i> Extreme Right Wing</p> <p>Discussion on the growing risk of right-wing extremism in New Zealand and Australia, and how each country is responding to this risk and how we can work together to respond to the risk.</p> <p>s6(a)</p> 	<p>New Zealand</p> <p><b>Lead:</b> DPMC, NZ Police, MFAT (Christchurch Call), NZSIS</p> <p><b>Support presenters:</b> MFAT</p> <p><b>Lead responders:</b> Home Affairs, Australian Security Intelligence Organisation</p>
1215- 1245		<b>LUNCH</b>	

Released under the Official Information Act 1982

5.	1245 - 1345	<b>FOREIGN INTERFERENCE RESPONSE</b> <i>Focus:</i> s6(a) Discussion about how Australia and New Zealand is responding to threats of foreign interference s6(a) s6(a) s6(a)	Australia <b>Lead:</b> Home Affairs, Office of National Intelligence, Australian Security Intelligence Organisation <b>Lead responders:</b> NZSIS, MFAT <b>Support responders:</b> DPMC (on behalf of DIA and MoJ)
6.	1345- 1400	<b>CONCLUDING ITEMS</b>	Australia & New Zealand (Co-chairs)
	1400	<b>END OF DIALOGUE</b>	

Released under the Official Information Act 1982

---

# Australia-New Zealand National Security Dialogue Agenda

**Date** 6 September 2019

**Time** 0800 - 1400 hrs

**Venue** s6(a) Pipitea House, 1-15 Pipitea St, Wellington, New Zealand

**Clearance** s6(a) The venue is a SCIF so electronic devices will need to be stored at reception upon arrival.

**Contact** s6(a) or [nssd@dpmc.govt.nz](mailto:nssd@dpmc.govt.nz)

---

## Attendees - Australia

s6(a) Department of the Prime Minister and Cabinet

s6(a) Department of Foreign Affairs and Trade

s6(a) Department of Home Affairs

s6(a) Department of Defence

s6(a) of the Defence Force

s6(a) Office of National Intelligence

s6(a) Australian Security Intelligence Organisation

s6(a) Australian Secret Intelligence Service

s6(a) Australian Signals Directorate

s6(a) Australian Federal Police

s6(a)

s6(a) Department of the Prime Minister and Cabinet (note taker)

## Attendees - New Zealand

**Brook Barrington**, Chief Executive, Department of the Prime Minister and Cabinet

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

**Andrew Hampton**, Director-General Government Communications Security Bureau

**Carolyn Tremain**, Chief Executive, Ministry of Business, Innovation and Employment

**Andrew Bridgman**, Secretary of Defence

**Chris Seed**, Secretary, Ministry of Foreign Affairs and Trade

**Bill Perry**, Acting Comptroller, New Zealand Customs Service

**Air Marshal Kevin Short**, Chief of the Defence Force


**Hon Dame Annette King**, New Zealand High Commissioner to Australia

**Mike Bush**, Commissioner of New Zealand Police

**Rebecca Kitteridge**, Director-General New Zealand Security Intelligence Service

s9(2)(a) Senior Advisor, National Security Systems Directorate, Department of the Prime Minister and Cabinet (note taker)



#	TIME	DESCRIPTION	LEAD
	0800 - 0815	<b>WELCOME AND REFRESHMENTS</b>	New Zealand
1.	0815 - 0900	<b>INTEGRATION OF NATIONAL SECURITY AND ECONOMIC DECISION MAKING</b> <i>Focus:</i> Growing Economies and Managing Risk Discussion on what each country is doing to integrate and coordinate policies to achieve national security outcomes, while maximising opportunities for economic growth in an increasingly contested global economic and technological environment.	Australia
2.	0900 - 1000	<b>CRITICAL INFRASTRUCTURE</b> <i>Focus:</i> Threats to Critical Infrastructure Discussion about the key threats to critical infrastructure that each country needs to manage, and possible methods for doing this.	New Zealand
	1000-1015	<b>MORNING TEA</b>	
3.	1015 - 1030  1030 - 1130	<b>EMERGING TECHNOLOGIES</b> s6(a) 	Australia
4.	1130 - 1215	<b>COUNTER TERRORISM</b> <i>Focus:</i> Extreme Right Wing Discussion on the growing risk of right-wing extremism in New Zealand and Australia, and how each country is responding to this risk and how we can work together to respond to the risk.	New Zealand
	1215-1245	<b>LUNCH</b>	

Released under the Official Information Act 1982

5.	1245 - 1345	<b>FOREIGN INTERFERENCE RESPONSE</b> <i>Focus:</i> s6(a) [REDACTED] Discussion about how Australia and New Zealand is responding to threats of foreign interference s6(a) [REDACTED] s6(a) [REDACTED]	Australia
6.	1345- 1400	<b>CONCLUDING ITEMS</b>	Australia & New Zealand (Co-chairs)
	1400	<b>END OF DIALOGUE</b>	

Released under the Official Information Act 1982



Released under the Official Information Act 1982

---

## Tab C: New Zealand Interagency Briefing Pack

- **Item 1:** Integration of National Security and Economic Decision Making
- **Item 2:** Critical Infrastructure
- **Item 3:** Emerging Technologies
  - s6(a) [Redacted]
  - s6(a) [Redacted]
- **Item 4:** Counter Terrorism
- **Item 5:** Foreign Interference

Released under the Official Information Act 1982

Released under the Official Information Act 1982

## Australia – New Zealand Security Dialogue 2019

### Cover-note

Attached are individual notes for each agenda item:

Agenda item 1: Integration of National Security and Economic Decision-Making

Agenda item 2: Critical infrastructure

Agenda item 3: Emerging technologies – s6(a)

s6(a)

Agenda item 4: Counter Terrorism (focus on Extreme Right-Wing)

Agenda item 5: Foreign Interference Response – s6(a)

s6(a)

There is a great deal of inter-connection and overlap between items 1, 2, 3 and 5.

s6(a)

In order to reduce duplication, the briefings are focussed on the specific issues likely to be covered within the particular agenda item; however the discussion is likely to cross over into other areas. Therefore we recommend the briefings are seen as a collective and read in their entirety.

The overlaps and inter-connections will need to be managed during the dialogue discussion.

Released under the Official Information Act 1982

### Agenda Item 1: Integration of National Security and Economic Decision-Making

Lead country:	<b>Australia</b>
Lead presenter:	• s6(a) Department of Prime Minister and Cabinet (PM&C)
Lead responder:	• Carolyn Tremain – MBIE
Support responders:	• Brook Barrington – DPMC • Chris Seed – MFAT, • Andrew Hampton – GCSB

#### Scope of item

*This item focuses on what each country is doing to integrate and coordinate policies to achieve national security outcomes, while maximising opportunities for economic growth in an increasingly contested global economic and technological environment.*

#### Outcomes sought from the session

Commitment to work together to share lessons-learned and knowledge of integrating economic and national security considerations into policy development; drawing in particular from New Zealand's experience.

#### Australian position

1. s6(a)

2.

#### Talking points

3. New Zealand's economic policy is underpinned by a commitment to open and competitive markets, free flows of people, capital, technology and ideas, and low regulatory costs.
4. New Zealand's approach is based on the principle of risk management rather than risk elimination. As part of this, we weigh national security risks against



economic benefits. New Zealand has integrated national security into its economic decision-making, for example within the emerging space industry.

5. Careful consideration of risks and economic opportunity is important - national security is a broad concept, and can lead to an overreaction if the risks and their significance are not clearly defined.
6. In some cases, the national security risks will be so high that we would not take up the economic opportunity, but in other cases the analysis will point to risk taking, albeit coupled with measures to keep risks as low as possible. A first step is to assess the risk environment and the extent and adequacy of current mitigations.
7. We have been doing things this way for a while, and though our approach has not changed, new government objectives present a number of associated challenges. In particular, the well-being focus, which has driven decisions the government makes about policies and budget initiatives. This broadens the goal from GDP growth and requires economic policy to consider issues such as climate change, income disparities, and national security from an integrated and 'systems' perspective, rather than as standalone issues.
8. Using Foreign Interference as an example, New Zealand has developed a work programme that involves putting in place an ability to take national security into account in relation to foreign investment and science-funding decision making, developing access controls for critical infrastructure, and general awareness-raising in the research community, critical infrastructure sectors, and advanced technology firms. This allows us to make the most of economic opportunities without ignoring potential negative security consequences.
9. New Zealand's small size enables ease of access and collaboration – it is easy to get the right people from both the economic and national security sides around the table. This is an advantage as we map out problems, design policy interventions, and put our foreign interference mitigations into place.
10. New Zealand's State Services Commission is leading a significant programme of work to change the statutory framework governing New Zealand's public service. A key part of the reform programme focuses on improving agency integration and joined-up delivery of policy through:
  - joined up planning and budgeting for complex cross-cutting issues,
  - the ability to adopt new types of public service joint ventures to support joined-up, agile service delivery and joint resource management (including assets and staff); and
  - a more flexible departmental agency model.

## Key questions

s6(a)



## Background

*Australia*

s6(a)



*New Zealand*

13. Examples where there is active consideration of national security outcomes in New Zealand's economic decision-making process:

- **Our emerging space industry and launch site for satellites.** Satellites can have a range of purposes and provide services that are inherently dual use; for example, navigation services are useful for industry and military capabilities. The Outer Space and High Altitude Act (OSHAA 2017) was created to help enable the opportunity for a New Zealand launch industry while also managing associated safety and security risks.
- The Ministry for Primary Industries has a responsibility to protect the country's productive sectors from **unwanted pests and diseases** while promoting the movement of goods into and out of New Zealand. Import Health Standards issued under the Biosecurity Act set out the requirements that commodities must meet before goods can be safely imported into New Zealand. In developing standards, MPI must have regard to, among other things, national security considerations such as, possible impacts on human and animal health, the environment, and the wider economy.



- Treasury is leading work to enhance the ability of the **Overseas Investment Act screening regime** to manage national security and public order risks. It is considering both a new national interest test for investments already subject to screening, and the creation of new call-in powers for specific national security/public order risks outside the existing screening regime.

s6(a)



14. Key elements of the New Zealand Foreign Interference framework in an economic policy context are:

- Managing the risk of **economic coercion** that can arise if critical infrastructure is owned or controlled by a potentially hostile foreign state actor, or we are highly dependent on an overseas market in a potentially hostile foreign state.
- Managing the risk of **sabotage** that can arise if critical infrastructure is owned or controlled by a potentially hostile foreign state actor.
- Managing the risk of **espionage**, particularly if it is targeted at accessing knowhow that is important to New Zealand's economic prosperity or would advantage the military in a potentially hostile foreign state.

#### *Public service reform*

15. Changes to the statutory framework governing New Zealand's public service will include a focus on public service organisations. There will be more formalised and flexible options for organisational arrangements to support public service agencies taking a truly collaborative approach to tackle some of the big challenges facing the country. The new system-design allows for:

- Interdepartmental executive boards that support joined-up planning and budgeting and / policy alignment on complex cross-agency issues.
- Two different types of Public Service joint ventures – the interdepartmental venture, and the joint operational arrangement – that support joined-up, agile service delivery and joint resource management, including assets and staff.
- A more flexible departmental agency model.

16. Collaborating agencies will be able to align strategy and planning activities operating in overlapping policy areas. This will harness the capabilities of individual agencies to collectively plan for and respond to complex cross—agency problems or priorities. New Zealand's border security and natural resource sectors are examples of how this approach should work on an everyday basis.

17. The Public Service Bill is currently being drafted and is expected to be introduced to Parliament on 5 November 2019.

## Agenda item 2: Critical Infrastructure

Lead country:	New Zealand
Lead presenters:	<ul style="list-style-type: none"><li>• Carolyn Tremain - MBIE</li></ul>
Support presenters:	<ul style="list-style-type: none"><li>• Brook Barrington – DPMC</li><li>• Chris Seed - MFAT</li><li>• Andrew Hampton - GCSB</li></ul>
Lead responder:	<ul style="list-style-type: none"><li>• s6(a) – Home Affairs</li></ul>

### Scope of item

*Discussion about the key threats to critical infrastructure each country needs to manage, and possible methods for doing this.*

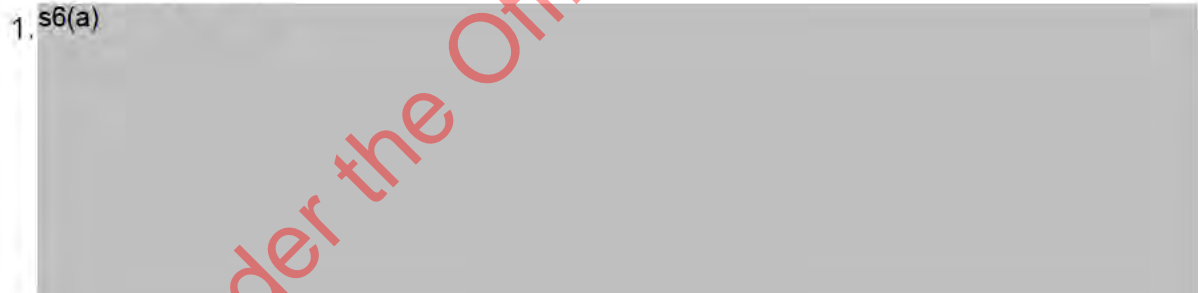
### Outcomes sought from the session

s6(a)



### Australian position

1. s6(a)




2.



### Talking points

3. New Zealanders' well-being is heavily reliant on the smooth and secure functioning and operation of critical infrastructure such as banking systems, electricity and communications networks, and health and governance systems. A disruption to any of these systems and their assets could have a range of serious implications for business, government, and the community more broadly.
4. Infrastructure failure may result from the failure of a physical asset or facility, caused by systemic mismanagement and underinvestment and/or foreign interference, or from a natural hazard event.



5. New Zealand has a lot of work underway to across government to address or build resilience to this risk. The devolved nature of our national security system means that responsibility for building resilience against infrastructure failure exists at multiple points across multiple agencies.
6. From a system perspective, the system governance board has recently adopted a new working definition to improve how we talk about and understand risks to and resilience of New Zealand's nationally significant critical infrastructure (para 29 refers).
7. s6(a)  

8. s6(a)  
s6(a) We have plans to develop a comprehensive national critical infrastructure framework over the next few years. This will include a national critical infrastructure strategy and associated work programme that will guide central and local government, as well as infrastructure owners. It will also likely result in new regulatory tools and instruments to make it easier to achieve infrastructure resilience across different sectors.
9. At a more targeted level our science and enterprise ministry, MBIE, is leading a considerable work programme to manage foreign interference risks in Critical National Infrastructure. We will talk more about this programme in Agenda Item 5, when we talk about managing the risks of Foreign Interference.
10. The New Zealand Treasury is also currently reviewing the overseas investment regime and some of the changes being considered would strengthen the regime's ability to manage foreign interference risks arising from overseas investment.
11. The GCSB is also delivering a range of work relating to the cyber security of New Zealand's critical infrastructure.

**Key questions**

- s6(a)  


## Background

### *Critical Infrastructure – system governance*

12. From a system-governance perspective, the Hazard Risk Board (HRB) has recently adopted the following working definition (developed through MBIE's Foreign Interference programme) to improve how we talk about and understand risks to and resilience of New Zealand's nationally significant critical infrastructure:

*Critical infrastructure is the systems, assets, facilities and networks and their related supply chains that underpin the wellbeing of New Zealanders now, and into the future, because they impact on:*

- i. New Zealand society and the day-to-day lives of New Zealanders*
- ii. the maintenance of public safety and security*
- iii. New Zealand's short and long term economic prosperity, and*
- iv. New Zealand's international reputation.*

13. s6(a)

14.

15.

16. To support this, HRB has agreed to the development of a comprehensive framework for critical infrastructure, which will ultimately produce a national critical infrastructure strategy and associated work programme for central and local government and private sectors to implement, and new regulatory tools and instruments. This framework will be delivered over the next three years, and will initially focus on increasing the visibility of critical infrastructure resilience work underway across government, and increasing the expectations on, and support for, critical infrastructure owners to consider national security outcomes in their business management processes.



*Foreign Interference in Critical Infrastructure*

17. MBIE is currently leading an approach to manage foreign interference risks in Critical National Infrastructure. The approach is risk-based, sector specific, and focuses specifically on the issue of access to critical national infrastructure. Critical infrastructure owners and operators have primary responsibility for managing risks to their operations, including those arising from malicious actors.
18. Each critical infrastructure sector has a “risk coordinating” agency within government, which is responsible for coordinating with central government, local government and private entities to ensure that appropriate strategies, plans, and protections are in place to mitigate relevant risks, including those arising from foreign threats.

19 s6(a)

20. The New Zealand Treasury is also currently reviewing the overseas investment regime, and some of the changes being considered (including extending a national interest test to the existing grounds in the Act and creating a national security and public order call in power) would strengthen the regime’s ability to manage foreign interference risks arising from overseas investment.

*Resilient cyber infrastructure*

21. The GCSB is delivering a range of work relating to the cyber security of New Zealand’s critical infrastructure. This includes:
  - Cyber Security Survey of New Zealand’s nationally significant organisations
    - The survey is the first of its kind in New Zealand and provides a useful benchmark for cyber security resilience across New Zealand’s nationally significant organisations. A range of resilience levels were found, reflecting that digital transformation is outpacing investment in cyber security. This highlights the need for more work to be done to improve cyber resilience across the board.
  - GCSB’s Annual Cyber Threat Assessment
    - The 2018 Annual Cyber Threat Assessment incorporates input from various partner agencies and found that malicious cyber operations continue to affect New Zealand entities.

- s6(a)

- s6(a)



- Malware Free Networks programme

- Our National Cyber Security Centre is continuing to scale the benefits of our CORTEX cyber defence capabilities through the roll out of our Malware Free Networks threat intelligence and disruption capability.

Released under the Official Information Act 1982

Released under the Official Information Act 1982

**Agenda Item 3: Emerging Technologies** – s6(a)  
s6(a)

Lead country:	<b>Australia</b>
Lead presenters:	<ul style="list-style-type: none"><li>• s6(a) Office of National Intelligence,</li><li>• s6(a) Home Affairs,</li><li>• s6(a) Australian Security Intelligence Organisation,</li><li>• s6(a) Australian Secret Intelligence Service</li></ul>
Lead responders	<ul style="list-style-type: none"><li>• Andrew Hampton – GCSB,</li><li>• Carolyn Tremain – MBIE,</li><li>• Brook Barrington – DPMC</li></ul>
Support presenters:	<ul style="list-style-type: none"><li>• Chris Seed – MFAT</li></ul>

**Scope of this item**

a) s6(a)

b) *Areas for collaboration around emerging and foundational technologies.*

**Outcomes sought from the session**

Commitment to further collaborate on managing the risks of emerging technologies, across the following topic areas:

- 'Internet of Things' security, including sharing information, collaboration on security principles and shared standards, and coordination in forums s6(a)
- s6(a)
- Sharing approaches to emerging and foundational technology.

**Australian position**

s6(a)

s6(a)



**Talking points**

4. Emerging technologies have the potential to radically change the social, economic, or political status quo. Many emerging technologies have the potential to upend existing national security dynamics, and will likely empower the states looking to change the existing rules-based international order.
5. Because these technologies are being developed simultaneously, it is important we take a holistic approach to understanding and responding to emerging technology. We must assess their impact and develop policy that considers the cumulative effect of many emerging or foundational technologies, rather than in isolation.

6. s6(a)



*Internet of Things*

7. Internet of Things (IoT) devices are already creating serious security vulnerabilities. s6(a)

s6(a)



8.

*5G and trusted markets*

9. New Zealand shares Australia's goal of secure future 5G networks. We also support the development of an open, trusted, and diverse international telecommunications equipment market.



10. New Zealand has had the Telecommunications (Interception Capability and Security) Act in place since 2013. It provides an independent, country and vendor agnostic way of mitigating network security risks on a case by case basis.
11. The TICSA regulatory framework has proven highly effective at securing New Zealand's public telecommunications networks.
12. New Zealand welcomes taking an international approach to creating secure networks and trusted technology markets. We are working with Australia through many forums, <sup>s6(a)</sup> on sharing information and aligning approaches on emerging security issues.

*Encryption*

13. The changing technology environment and increasing use of end to end encryption for communication are creating significant challenges for intelligence and law enforcement agencies.
14. However encryption is also fundamental to the development of the modern digital economy through the security of data, and protection of private, commercial and government information.
15. Modern digital services should, like any technology, be used to enhance prosperity and freedom, not used to harm others.
16. We agree with Australia that there are we must work constructively with industry to ensure lawful access to encrypted data by law enforcement agencies and our intelligence communities.

**Key questions**

- s6(a)



**Background**

s6(a)





s6(a)



*Internet of Things*

s6(a)



*5G and trusted markets*

s6(a)



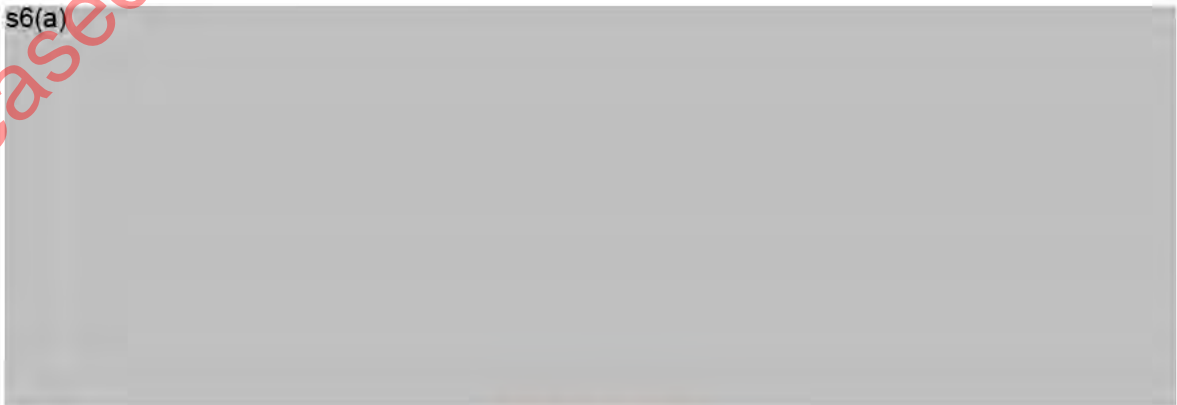
Released under the Official Information Act 1982

s6(a)



Encryption

s6(a)



Released under the Official Information Act 1982

33. New Zealand needs to have a domestic conversation on lawful access by law enforcement to encrypted data. Our position is that we must work constructively with the private sector to ensure law enforcement is able to effectively keep New Zealanders safe online without compromising the security of internet services. We have provisions in legislation (TICSA) that requires Internet Service Providers to provide access to encrypted communications.

34. s6(a)  
s6(a) [REDACTED] New Zealand  
previously emphasised the importance of working collaboratively with technology firms, which has been successful on other topics like the Christchurch Call.

*Access to and ownership of sensitive technologies*

35. As part of the MBIE-led Foreign Interference work programme, we are progressing a range of work aimed to protect New Zealand's sensitive technologies from foreign interference risks.

36. We now apply national security due diligence to decisions regarding Crown research funding of sensitive scientific research. We are also checking on whether existing safeguards on decisions on visa screening for individuals entering New Zealand who will have access to sensitive technology, are adequate.

Released under the Official Information Act 1982

### Agenda item 4: Counter Terrorism (focus on Extreme Right-Wing)

Lead country:	<b>New Zealand</b>
Lead presenters:	<ul style="list-style-type: none"><li>• Brook Barrington – DPMC,</li><li>• Commissioner Mike Bush – NZ Police,</li><li>• Chris Seed – MFAT (Christchurch Call),</li><li>• Rebecca Kitteridge – NZSIS</li></ul>
Support presenters:	<ul style="list-style-type: none"><li>• Chris Seed – MFAT</li></ul>
Lead responders:	<ul style="list-style-type: none"><li>• s6(a) Home Affairs</li><li>• s6(a) Australian Security Intelligence Organisation</li></ul>

#### Scope of item

*This item focuses on the growing risk of right-wing extremism in New Zealand and Australia, to support a discussion about how each country will respond to this risk and how we can work together to respond to the risk.*

#### Outcomes sought from the session

Commitment to further collaborate on countering terrorism, including across the following areas:

s6(a)



#### Australian Position

1. s6(a)





s6(a)

### Talking points

2. We have a broad programme of work underway to strengthen our counter terrorism system. This includes developing a national strategy to counter terrorism and violent extremism organised around the following focus areas:
  - Counter-Terrorism legislation
  - Building connections across society
  - Reducing racism and hate speech
  - Keeping places where people gather safe
  - Operational Counter-Terrorism work – responding to threats and leads
3. Another key piece of work, 'the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online' is a catalyst for driving meaningful change in eliminating terrorist and violent extremist content online.
4. Both countries are also taking a number of practical steps together to improve our understanding of the threat and sharing of information in specific cases of response.
5. Since March 15, New Zealand's cooperation with Australia on right-wing extremism has accelerated and New Zealand has noted real benefits from this closer collaboration.<sup>s6(a)</sup>

s6(a)

### Key questions

s6(a)

s6(a)

## Background

6. A detailed description of the Extreme Right-Wing threatscape is provided at Annex 1 at the end of this briefing note.
7. We have a broad programme of work underway to strengthen our counter terrorism system. This includes developing a national strategy to counter terrorism and violent extremism organised around the following focus areas:

### *Counter-Terrorism legislation*

8. Our counter-terrorism legislative settings have been developed based on international experience, particularly increased Islamist extremist terror events of the early 2000s. Changes were made at a rapid pace and focused on managing prominent terrorist entities and groups.
9. There is now recognition of a growing threat from lone actors who self-radicalise and have ambiguous networks. Our counter-terrorism legislative framework must continue to adapt to meet new challenges. Given the evolving terrorism environment, there is value in undertaking a more systematic and considered examination of our regime, aspects of which include-
  - The workability of the Terrorism Suppression Act 2002 and whether it is clear what conduct would constitute an offence under the Act.
  - New offences that might facilitate earlier intervention by law enforcement before individuals can undertake terrorist acts.
  - Considering criminalising travel by foreign terrorist fighters (required by UN resolution 2178).
  - Considering whether the terrorist financing offence is fit for purpose.
  - Consideration of a court-imposed civil order for people who present a terrorism concern through activities such as preparation/distribution of objectionable terrorist and violent extremist content.
10. This work is being informed by the legislative toolkits of our partner countries, including Australia.

s6(a)

11 s9(2)(g)(i)

### *Building connections across society*



12. Connection amongst members of society has been shown to reduce radicalisation and polarisation, and so in turn reduces the likelihood that an individual will conduct an act of terrorism. The Department of the Prime Minister and Cabinet has been leading some work with the Ministry of Social Development and other agencies to review the evidence on social inclusion, to identify the work already underway across government, and to provide some initial advice on potential further interventions to strengthen social inclusion.

*Reducing racism and hate speech*

13. The Ministry of Justice is working with the Human Rights Commission to consider how we might stop the spread of hate speech, including whether our existing laws adequately protect the right to equality, freedom from discrimination, and rights of minorities. This work will look at non-regulatory options that could help reduce levels of intolerance around racism and discrimination. This will build on existing priorities including the Child Wellbeing Strategy, which has as one of its six priorities that children are free from racism, discrimination, and stigma.

*Keeping places where people gather safe*

14. Security agencies will work alongside public and private sector entities who have a responsibility to protect the lives of people working in, using, and visiting crowded places, by making these places more resilient. This will be delivered through a Crowded Places Strategy, so that there are clear guidelines and tools for those who have responsibilities for sites where people gather.

*The Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online'*

We are also actively working on the 'Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online' (the Call)–

- The Call is at the centre of New Zealand's international response to the Christchurch attacks. Adopted in Paris on 15 May, the Call is a series of voluntary commitments for companies and online service providers, intended to reduce the harm from terrorist and violent extremist content online.
- Led by the Ministry of Foreign Affairs and Trade, New Zealand has been working collaboratively with the companies and country supporters to see what can be achieved as quickly as possible under the Call, in consultation with civil society.
- Since May, our focus has been on demonstrating progress across the Prime Minister's four priority areas ahead of the UN General Assembly in September:

- o Following extensive engagement with companies, we have agreement to reshaped Global Internet Forum to Counter Terrorism (GIFCT<sup>1</sup>) as a permanent organisation to take forward the Call commitment and to be a more effective collaborative venture between companies, countries and civil society, better enabling it to tackle some of the wider challenges of terrorism and violent extremist content. s6(a)

s6(a)

- o We are looking to launch a crisis response protocol to assist Call supporters in responding collaboratively and effectively to real-world crises with an online element, such as Christchurch.
- o We are funding a gap analysis of what additional research might be necessary to realise the Call's goals, including what additional data might be provided by companies to assist with efforts to prevent terrorist and violent extremist content, and to address the fundamental drivers and causes of radicalisation;
- o We are exploring with companies what concrete steps might be achieved on better understanding algorithmic outcomes, to better understand possible intervention points and thereby reduce the risk of radicalisation online. This will be the subject of one of the GIFCT's first working groups.

s6(a)

s6(a)

---

<sup>1</sup> The GIFCT is an existing industry body (set up in 2017 by Facebook, Google, Microsoft, and YouTube) with the objective of "substantially disrupting terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using [their] platforms". The GIFCT currently does this through: "employing and leveraging technology; sharing knowledge, information and best practices; and conducting and funding research".



s6(a)



*Operational Counter-Terrorism work – responding to threats and leads*

22. There has been an increase in hoaxes, threats, and other concerning behaviour and leads from the public. At 14 August 2019, over 2540 leads have been reported to or identified proactively by Police. While some are likely to pose little risk, initial assessments identified 89 high and 646 medium-level risk leads.
23. Police are undertaking significant operational activity in relation to these leads, including prosecutions, further inquiry, or ongoing monitoring.
24. This work has required new capabilities and capacity in Police, including an increasing intelligence and national security focus and resourcing, development of new leads case management systems; and work to enhance and support Districts.
25. Police continue to roll out Operation Whakahaumanu – Police engagement and proactive deployment across the country to ensure people feel safe in their communities, including advice on security and lockdown procedures at businesses and presence at public events.
26. Police continue to work on the prosecution of TARRANT and ongoing investigation of the 15 March terrorist attack. New Zealand appreciates the support of Australia in this case.

*The Royal Commission of Inquiry (RCOI) into the Attack on Christchurch Mosques*

27. The findings of the RCOI will be made public and there will likely be significant commentary and debate, including potential comparisons with the Australian operational approach to counter-terrorism. The Government is considering its process for responding to its findings and recommendations.

*Practical steps we are taking together to improve our understanding of the threat and sharing of information in specific cases of response*

28. Australia and New Zealand already collaborate on counter-terrorism through the Australia/New Zealand Counter Terrorism Committee (ANZCTC). This provides a forum for New Zealand to draw upon lessons learned and guidance for NZ-specific work.

29. Examples of Australia-New Zealand cooperation include the following:  
s6(a)



**Annex 1:** <sup>s9(2)(g)(i)</sup> [REDACTED]

*The scale of extreme right-wing terrorism*

1. <sup>s6(a)</sup> [REDACTED]

2. Right-wing extremism however, is thought to be increasing; we are aware that between 2013-2017, right-wing extremists were responsible for at least 66 deaths and 113 attacks of which 47 attacks were in 2017 alone (numbers from the Institute for Economics and Peace, Global Terrorism Index 2018). Large-scale attacks like in Oklahoma City, Norway and Christchurch are relatively rare.
3. Terrorist attacks aren't the only concern - hate crimes and extreme right-wing sentiments have a significant impact on national security and can have damaging effects on communities and community cohesion.
4. One major issue with quantifying the scale of extreme right-wing is difficulties involved in tracking numbers and trends because of patchy numbers and different definitions. Distinctions between crime, hate crime and terrorist incident blur, particularly where there is no hate crime offence (such as in New Zealand).
5. Another key issue is that real world behaviour can be very different to online behaviour. Many extreme right-wing adherents will have 'normal' jobs and do otherwise 'normal' things in the real world – while espousing extremist material online.

*The nature of the extreme right-wing*

6. Understanding the threat posed by right-wing extremism is difficult. Numbers of extreme right-wing violence and groups are unclear and probably too conservative. There are a lot of extreme right wing groups – both formal and informal, however extreme right-wing terror attacks are probably more often perpetrated by lone actors.
7. Unlike other terrorist ideologies, the extreme right-wing does not have a unified or hierarchical leadership, and individuals hold a broad range of views and ideologies including, but not limited to, racism, anti-Semitism, homophobia, sexism, authoritarianism, and anti-democracy. The underpinning ideology is also not defined, and can be a combination unique to the adherent with much taken from mainstream politics and history.
8. Groups differ depending on national context (e.g. target groups, particular grievances) but the movement has an increasingly transnational flavour. Right wing extremist groups and individuals are fragmented and lack a unifying narrative or leadership. Some organised groups exist, but there is a wider pool of



individuals with extremist views across diffuse networks, often online. All known extreme right-wing terrorist attacks since 2011 have been by lone actors or small, self-directed cells. Those who act are often on the fringes of movements.

9. Much of movement exists on the fine line between legitimate views and dissent, and criminal behaviour. Many key thought leaders and groups publically distance themselves from violence.
10. All these factors are key obstacles to managing right-wing extremism.

*And what are the drivers?*

11. There is no single factor that drives the extreme right-wing, but the idea that one's culture, identity and place in the world are threatened is key, which is exacerbated by economic and political changes.
12. The internet has been a fundamental catalyst - regardless of ideology, the internet enables better connections between individuals globally, access to and sharing of ideas (often anonymously), and contributes to polarisation and recruitment.
30. Internet platforms host significant amounts of extremist and violent content, and their algorithms have been key in providing more content to users who show some interest in right-wing extremism. Aided by lax or non-existent service or community standards (and / or the difficulties that come with finding the content and enforcing these), the extreme right-wing is active across a range of s9(2)(j) and more underground (4chan and 8chan) platforms.
31. Extreme right-wing content moves between these platforms, exposing users worldwide. These platforms and forums function as echo-chambers, reinforcing and deepening ideological attachment and their users from alternative viewpoints and content. The extreme right-wing has appropriated internet and gaming culture, using coded language and hiding their content in irony and 'humour'.
32. A country's specific political and cultural settings complicate things further, and in all countries, the nature and activities of these groups shades over into legitimate forms of political discourse and activity. It can be difficult to determine the point at which political debate becomes hate speech.

*Key challenges of the extreme right-wing*

33. The extreme right-wing presents challenges from both an analytical and operational perspective. Analytically, the lack of common definition of what terrorism is, and the fluidity of individuals of adhering to different ideologies and picking up ideas from the internet makes it harder to draw distinct links between inspiration and action, which in turn may make it more difficult to legislate against attacks.



13 s6(a)



Released under the Official Information Act 1982

**Agenda Item 5: Foreign Interference Response:** s6(a)

s6(a)

Lead country:	<b>Australia</b>
Lead presenters:	<ul style="list-style-type: none"><li>• s6(a) Home Affairs,</li><li>• s6(a) Office of National Intelligence,</li><li>• s6(a) Australian Security Intelligence Organisation.</li></ul>
Lead responders:	<ul style="list-style-type: none"><li>• Rebecca Kitteridge – NZSIS</li><li>• Chris Seed – MFAT</li></ul>
Support responders:	<ul style="list-style-type: none"><li>• Brook Barrington – DPMC (On behalf of Department of Internal Affairs and Ministry of Justice),</li></ul>

**Scope of this item**

*This item focuses on how New Zealand and Australia are responding to threats of Foreign Interference,* s6(a)

**Outcomes sought from the session**

Commitment to further collaborate on managing the risks of foreign interference, across the following areas:

- Protecting the integrity of electoral systems from foreign interference.
- Examining the current foreign interference threatscape in the areas of democratic institutions, the economy, academia, and other levels of government; how to address it and how to prevent it.
- Sharing information on foreign direct investment cases (to the extent permitted under our respective regulatory regimes).
- Undertaking deeper cooperation on foreign ownership of and access to sensitive technology.

**Australian position**

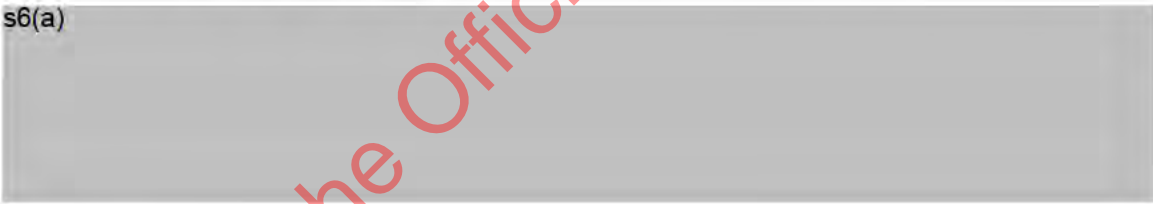
1. s6(a)



**Talking points**

2. New Zealand has a comprehensive and credible work programme to mitigate foreign interference with further Cabinet decisions to progress a number of mitigation measures likely to be taken in the coming months. This work is progressing in two streams: foreign interference in our economy, and foreign interference in our democracy.
3. Our approach intends to maximise the benefits of our open economy and society, while managing the risks at the margins in a proportionate way. As part of this, New Zealand will leverage our strengths, including high levels of transparency, trust in government, low levels of corruption and our robust media and academic communities.
4. Our approach is a product of our intelligence agencies, line departments with portfolio responsibilities (such as our science and enterprise ministry), and foreign ministry officials working together. It is not driven solely by the national security system, but developed with and delivered by our portfolio agencies.
5. This influences how we engage with various sectors of the economy and society. We can get the leaders of all our universities together in a room, to discuss risks and challenges they might face.

6. s6(a)



**Key questions**

s6(a)



s6(a)

- Foreign language media

s6(a)

- We are aware of foreign interference activity in New Zealand and overseas, but assessing the impact is difficult.
- Pressure, monitoring, and harassment of ethnic communities exercising their political and religious freedoms
  - Have Australian officials engaged with ethnic communities to discuss their experiences?
  - What efforts have been successful in disrupting this activity
  - How has diplomatic engagement on this subject gone?

## Background

### *Australia*

7. Australian federal Education Minister Dan Tehan has announced the establishment of a taskforce to help protect universities against foreign interference. The main areas of focus will be:
  - **Cyber security:** to ensure Australia's ecosystem is resilient to unauthorised access, manipulation, disruption, or damage.
  - **Research and intellectual property** – to deter and detect deception, undue influence, unauthorised disclosure or disruption to the Australian research, intellectual property and research community, while protecting academic freedom.
  - **Foreign collaboration** – to ensure collaboration with foreign entities will be transparent, undertaken with full knowledge and consent, and in a manner that avoids harm to Australia's interests.
  - **Culture and communication** – to foster a positive security culture through engagement with government and the broader community to educate, uplift awareness, and improve research and cyber resiliency.
8. Attention will also be paid to creating safe campus environments where students and staff can freely express views without interference and intimidation from foreign governments.



*New Zealand*

9. A cross-agency foreign interference work programme has been underway since late 2017; the existence of this programme has not yet been made public. Work is progressing in two streams: foreign interference in our economy, and in our democracy.
10. This work is guided by a number of over-arching concepts:
- Risk management, rather than elimination – a number of checks and balances will act in combination to bring the risk within tolerable limits.
  - These will be balanced against the significant opportunities and benefits New Zealand derives from open markets and investment flows, and our open and inclusive democracy and society.
  - We adopt a country-neutral approach proposed actions apply equally to any country, s6(a)
- s6(a)
11. In October 2018, Cabinet agreed that work should continue to further strengthen New Zealand's resilience against foreign interference risks in our economy and democracy.
12. The work focused on interference in our democracy seeks to address risks in our government, electoral, media, academia, and communities. The work focused on the economy seeks to address risks associated with sensitive technology, critical national infrastructure, and concentrated markets and investment. s6(a)
- s6(a)
- s6(a) we have identified various vectors of potential foreign interference and are working to strengthen our systems to mitigate the interference risk in each vector.
13. A feature of our approach has been the way government agencies have worked collaboratively to understand and address interference risks. Our small size has been an advantage in thinking about the problem, and it is proving to be an advantage as we put our mitigations into place. We can get almost all of the people who think about risks to our economy and our science system in one room, and have done so on an almost weekly basis over the last two years.
14. New Zealand has not undertaken any outreach to ethnic communities in the context of its foreign interference work programme. A stocktake found that a large number of government agencies undertake outreach to ethnic communities on a range of subjects. Some of it is relevant to foreign interference – such as building trust in New Zealand Police, and promoting democratic norms in an electoral context. But there is nothing focused on talking to ethnic communities about the degree they might be subject to improper pressure by or on behalf of foreign states. As discussed under Agenda Item 4 under Counter Terrorism, the government is considering a programme focused on social inclusion of ethnic communities, which may benefit communities subject to foreign interference.



---

## **Tab D: Administration Documents**

- Administrative Instruction (New Zealand version)
- Biographies - Australian Attendees

Released under the Official Information Act 1982



# Administrative Instruction for New Zealand Attendees

**TO:** New Zealand National Security Dialogue Attendees

**FROM:** Department of the Prime Minister and Cabinet

**DATE:** 29 August 2019

**SUBJECT:** Administrative Instruction for the Australia-New Zealand National Security Dialogue 2019

## Key Points

1. Participation at the Australia-New Zealand National Security Dialogue 2019 (Dialogue) is generally restricted to principals of agencies from relevant Australian and New Zealand government agencies, respective High Commissioners, and a note taker from each country.
2. A dinner for attendees will be held on the evening of Thursday, 5 September 2019 at the Members' Only Dining Room, Executive Wing (3<sup>rd</sup> floor), Parliament starting at 1830 hrs.
3. The Dialogue is being held at Pipitea House, 1-15 Pipitea Street, Wellington on Friday 6 September 2019, starting at 0800 hrs.

## Administrative Arrangements

### Dinner and Catering

4. The dinner for the Dialogue will be held at the Members' Only Dining Room, Executive Wing (3<sup>rd</sup> floor), Parliament. Those without access to Parliament will be met at reception in the Beehive and escorted to the Members' Only Dining Room.
5. During the Dialogue on 6 September, refreshments, morning tea and lunch will be provided at the venue to enable discussion time to be optimised.

### Dialogue Venue

6. The Dialogue is being held in the usual SIB meeting room s6(a) at Pipitea House, 1-15 Pipitea Street, Wellington, New Zealand.
7. As Pipitea House is a SCIF, electronic devices will need to be securely stored at reception.
8. The contact number for participants during the day is s6(a) Emails can be sent to [nssd@dpmc.govt.nz](mailto:nssd@dpmc.govt.nz).

### Timings and Agenda

Time	Activity	Comments
	Thursday 5 September 2019	

**IN-CONFIDENCE**

Afternoon	Australian attendees arrive in Wellington	
1830 for 1900	Dinner at Members' Only Dining Room, Executive Wing (3rd floor), Parliament	Dinner hosted by DPMC for principals in secure private room at the Beehive. Enter via the main Beehive entrance.
	<b>Friday 6 September</b>	
0800 for 0815	Arrive at Pipitea House	Refreshments available on arrival.
0815	Dialogue commences	Morning tea and lunch will be provided.
1400	Dialogue concludes	

**Attire**

9. Dress for the dinner on 5 September is smart casual and for the meeting on 6 September business attire.

**Contacts**

10. The Dialogue is being arranged by the National Security Systems Directorate, Department of the Prime Minister and Cabinet. Contacts are:

<b>Name</b>	<b>Catriona Robinson</b>	s9(2)(a)	<b>Sarah Holland</b>
<b>Role</b>	<b>Director, National Security Systems Directorate (NSSD), DPMC</b>	<b>Senior Advisor, NSSD, DPMC</b>	<b>Principal Advisor, NSSD, DPMC</b>
<b>Office</b>	s9(2)(a)	s9(2)(a)	s9(2)(a)
<b>Mobile (after hours)</b>	s9(2)(a)	s9(2)(a)	s9(2)(a)
<b>Email</b>	s9(2)(a)	s9(2)(a)	s9(2)(a)
	Or alternatively <a href="mailto:nssd@dpmc.govt.nz">nssd@dpmc.govt.nz</a>		

**14 additional pages are withheld in full under the following sections of the Act:**

- Section 6(a)**
- Section 6(b)(i)**
- Section 9(2)(a)**