



# Briefing

## STRENGTHENING NEW ZEALAND'S RESILIENCE TO MIS/DISINFORMATION

To: Prime Minister & Minister for National Security & Intelligence (Rt Hon Jacinda Ardern)

<b>Date</b>	20/12/2020	<b>Priority</b>	Routine
<b>Deadline</b>	29/01/2021	<b>Briefing Number</b>	2021NSP/031

### Purpose


1. To seek your agreement to coordination mechanisms for addressing mis/disinformation issues, and endorsement to develop a strategic framework to strengthen New Zealand's resilience to mis/disinformation.

### Recommendations

1. **Note** that while work has been done by agencies, academia and civil society to address COVID-19-related disinformation, this activity is currently not coordinated in pursuit of a common strategy;
2. **Agree** that, given the multiple equities for this issue, DPMC leads government efforts to strengthen resilience to disinformation, in close coordination with the proposed Interagency Coordination Group; YES / NO
3. **Note** that officials consider it is preferable for efforts to counter mis/disinformation to be primarily driven from outside of government, i.e. by civil society organisations, academia and the media;
4. **Agree** that DPMC and the Interagency Coordination Group develop a Strategic Framework for Strengthening New Zealand's Resilience to Mis/Disinformation for consideration by Ministers in Q1 2021; YES / NO

**RESTRICTED**

5. **Agree** that the following group of Ministers should be the first points of referral for work to strengthen New Zealand's resilience to mis/disinformation:
- i. Minister for National Security & Intelligence (Rt Hon Jacinda Ardern); **YES / NO**
  - ii. Minister of Education & Minister for COVID-19 Response (Hon Chris Hipkins);
  - iii. Minister of Health & Minister Responsible for the GCSB and NZSIS (Hon Andrew Little);
  - iv. Minister for Broadcasting and Media & Minister of Justice (Hon Kris Faafoi);
  - v. Minister of Internal Affairs (Hon Jan Tinetti);
  - vi. Minister for Digital Economy and Communications (Hon Dr David Clark).
6. **Agree** to refer this paper - for discussion around the proposed recommendations - to the Group of Ministers at Recommendation 5, and to the following Ministers whose agencies will be represented on the Interagency Coordination Group: **YES / NO**
- i. Minister of Arts, Culture and Heritage (Hon Carmel Sepuloni)
  - ii. Minister of Foreign Affairs (Hon Nanaia Mahuta)
  - iii. Minister of Police (Hon Poto Williams)
7. **Indicate** if you wish to discuss elements of the proposed strategy – including disinformation monitoring, working with civil society and engagement with Ministers – at the next available national security and intelligence briefing. **YES / NO**

  
Tony Lynch  
**Deputy Chief Executive**  
National Security Group  
DPMC

20/01/21  
...../...../.....

Rt Hon Jacinda Ardern  
**Minister for National Security & Intelligence**

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

**Minister's office comments:**

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

**Contact for telephone discussion if required:**

Name	Position	Telephone		1st contact
Dan Eaton	Director, National Security Policy Directorate, DPMC	9(2)(a)	9(2)(a)	
Greg Mitchell-Kouttab	Principal Policy Advisor, National Security Policy Directorate, DPMC	9(2)(a)	9(2)(a)	✓

Released under the Official Information Act 1982

# STRENGTHENING NEW ZEALAND'S RESILIENCE TO MIS/DISINFORMATION

## Executive Summary

---

1. While mis/disinformation is not a new phenomenon, its reach and veracity has increased exponentially in recent years via social media channels. Its impact on national security – through the potential erosion of trust in democratic institutions and the undermining of public health campaigns – became dramatically apparent through 2020.
2. Several of our closest international partners have witnessed unprecedented social and political polarisation driven in part by disinformation campaigns conducted by both state and non-state actors. Fuelled by fundamental distrust in the media and the political process, these countries face a significant challenge in trying to counter disinformation.
3. Mis/disinformation can create and amplify social divisions, challenge national values, foster extremist views, break down social cohesion and, in some cases, incite violence towards minority groups. Conspiracy theories can also have a corrosive effect, undermining trust in public institutions and the social contract, with attendant consequences for policy making and service delivery.
4. New Zealand still has relatively high levels of public trust in media and state institutions. This was positively demonstrated in 2020, as media outlets and civil society organisations successfully countered ('pre-bunked') a number of COVID-19 and elections-related disinformation campaigns before these could take hold in the population.
5. We cannot take this situation for granted, however, as we are unlikely to remain immune from these global trends. As a national security priority we need to focus our efforts on strengthening New Zealand's resilience to mis/disinformation. The attached National Security Policy Insights paper outlines the mis/disinformation problem, details efforts undertaken to date to combat mis/disinformation, and highlights the need for coordination, and the development of a strategic framework for a whole-of-society approach to mis/disinformation.
6. Ideally, efforts to counter mis/disinformation should be led from outside of government by the media, civil society, NGOs, academia and the private sector. Several leading academics, research organisations such as Te Pūnaha Matatini, other organisations such as Netsafe and InternetNZ have already been very active, and we are exploring how to support them and lift their capacity in this work.
7. Oversight of mis/disinformation is a sensitive issue, as any public commentary or perceived control of a "counter-disinformation effort" can reinforce conspiracy meta-narratives about state manipulation of information and give legitimacy to those claiming an erosion of free speech. For this reason, we would not recommend formal allocation of disinformation responsibilities or the identification of a government spokesperson. A group of relevant Ministers with whom significant issues can be highlighted and public

## ~~RESTRICTED~~

communications approaches approved will, however, be important to ensure appropriate proactive oversight of official activity in this area.

8. We propose that the Department of the Prime Minister and Cabinet (DPMC), working closely with an Interagency Coordination Group<sup>1</sup> that will report to a group of Ministers as required, should develop a strategic framework for a whole-of-society approach to building resilience to mis/disinformation in New Zealand.
9. Subject to approval of the strategic framework, the Interagency Group will subsequently become a coordination hub for the management of significant mis/disinformation issues, and will dock into a wider non-government led multi-stakeholder forum for addressing mis/disinformation more generally.
10. We propose to consult the draft strategic framework with a range of Ministers in early 2021, ahead of taking it to Cabinet for approval by April 2021. Our timeframes are informed by report-back commitments on the recommendations of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain report.
11. We would welcome a discussion with you on the policy proposals outlined in this paper and the attached report. In particular, we would welcome your views on:
  - how we engage with, and lift the capacity of, civil society, the media and academia to lead efforts to counter disinformation in New Zealand;
  - whether monitoring should be done by government agencies or by non-governmental partners (e.g. universities and/or private organisations); and
  - how you would envisage Ministerial engagement on this sensitive issue.

### **Purpose**

---

12. To seek your agreement to coordination mechanisms for addressing mis/disinformation issues, and endorsement to develop a strategic framework to strengthen New Zealand's resilience to mis/disinformation.

### **Background**

---

13. In October 2020, DPMC's National Security Policy Directorate took an earlier version of the attached Policy Insights paper to the Security and Intelligence Board (SIB)<sup>2</sup> to update them on work undertaken across the system to understand and counter the disinformation problem – particularly in relation to COVID-19 – and to highlight the gaps in New Zealand's ability to respond to disinformation.
14. SIB Chief Executives agreed that officials should seek guidance from Ministers on the proposed coordination of, and strategic framework for, strengthening New Zealand's resilience to mis/disinformation.

---

<sup>1</sup> That group will comprise: DIA, DPMC, MBIE, MFAT, MCH, MOE, MOH, MOJ, NZ Police, NZSIS and the GCSB.

<sup>2</sup> SIB is a governance board that brings together chief executives with national security responsibilities and focuses on external and internal security threats and intelligence issues.

## RESTRICTED

15. Given the complex crossover of mis/disinformation with a number of other significant national security issues, it should be noted that there will be some useful connections between this work and the development of a number of countering violent extremism (CVE) and social inclusion-based initiatives arising from recommendations of the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain.

***Disinformation** is false or misleading content (or the omission of content) designed to achieve a strategic purpose. Whether for ideological or commercial goals, the effort is designed to influence audience perceptions, opinions and/or behaviour (e.g. QAnon conspiracy theories).*

***Misinformation** is information that is false or misleading, but is not produced or disseminated in pursuit of an underlying ideological or commercial purpose (e.g. anti-fluoride information).*

### Building & Strengthening NZ's Resilience to Mis/Disinformation

16. Since the first COVID-19 lockdown in March, during which we witnessed the rapid spread of COVID-19-related disinformation, agencies have done a lot of work to understand and respond to the problem. Using academic and non-governmental research as the basis, agencies and media outlets have become more adept at proactive communications strategies to counter mis/disinformation narratives and, where possible, to get ahead of potential mis/disinformation campaigns (e.g. COVID-19 vaccines).
17. Despite this work, however, the overall system remains fragmented. Work to support the election highlighted a need for overarching leadership and coordination, as well as for a strategic framework to inform a whole-of-society approach. Without these we risk continued fragmentation, duplication of effort, lack of strategic direction or critical mass, and an inability to identify and act on threats before or as they emerge.
18. We recommend the following steps to support coordination of the issue:
- i) **DPMC to coordinate** the government's response to the mis/disinformation problem **and to lead an Interagency Coordination Group** comprising the following agencies:
    - Department of Internal Affairs (DIA);
    - Government Communications Security Bureau (GCSB);
    - Ministry for Culture and Heritage (MCH);
    - Ministry of Business, Innovation and Employment (MBIE);
    - Ministry of Foreign Affairs and Trade (MFAT);
    - Ministry of Education (MOE);
    - Ministry of Health (MOH);
    - Ministry of Justice (MOJ);
    - New Zealand Police; and
    - New Zealand Security Intelligence Service (NZSIS).

- ii) **The development, by DPMC and this Interagency Coordination Group, of a strategic framework for a whole-of-society approach to building resilience to mis/disinformation in New Zealand.** This process will include close consultation with academia, civil society organisations, the media council, and other key public stakeholders to ensure transparency and public buy-in. As outlined in Attachment A, the framework will involve:
- Guiding principles that including upholding freedom of expression, privacy, a free, secure and open internet, and New Zealand's human rights commitments;
  - The establishment of a broad civil society and academia-led multi-stakeholder approach to monitoring disinformation, engaging with tech platforms, and to building public awareness, critical thinking skills and online media literacy;
  - A strategy for public communications, detailing best practice in countering mis/disinformation and conspiracy theories; and
  - Referral policies, to enable relevant agencies to address instances when disinformation crosses certain thresholds into criminality, extremist behaviour or foreign interference.
- iii) **The identification of a group of relevant Ministers** that can be referred to in considering significant mis/disinformation issues as these arise, and to make decisions on critical policy and communications recommendations. It is not envisaged that these Ministers would necessarily meet on a formal basis, but given their portfolio responsibilities we would suggest the following Ministers receive regular updates from officials on the disinformation landscape:
- Minister for National Security & Intelligence (Rt Hon Jacinda Ardern)
  - Minister of Education (Hon Chris Hipkins)
  - Minister of Health & Minister Responsible for the GCSB and NZSIS (Hon Andrew Little)
  - Minister for Broadcasting and Media & Minister of Justice (Hon Kris Faafoi)
  - Minister of Internal Affairs (Hon Jan Tinetti)
  - Minister for Digital Economy and Communications (Hon Dr David Clark)

Other Ministers, such as Foreign Affairs and Trade, Police and Arts, Culture and Heritage may also need to be consulted on relevant mis/disinformation matters as appropriate to their portfolio responsibilities.

19. There is also an international dimension to mis/disinformation issues. As outlined in Appendix Two of Attachment A, New Zealand has received numerous bilateral and multilateral requests to share information about COVID-19-related mis/disinformation, and we expect that likeminded partners will increase offers to work together on further actions, statements, or attributions relating to disinformation. Developing a stronger domestic approach to mis/disinformation would effectively and credibly support these international engagements.

## **Next Steps**

---

20. Subject to your agreement, DPMC will commence work, in close consultation with the Interagency Coordination Group, on developing the proposed strategic framework. An outline of the potential elements of this framework is included in the attached paper. DPMC would look to have this ready for consultation with Ministers in Q1 2021.

## **Financial Implications**

---

21. Financial implications of this work are unclear at this point, though these are not expected to be significant in the short term. DPMC will be able to develop the Strategic Framework and conduct initial public engagement from within baselines. Funding may, however, be required depending on the longer-term resources required to undertake this work.
22. Funding will also be required for monitoring disinformation and conducting research activities to further understand the nature of the problem. MBIE currently funds disinformation research being undertaken by Te Pūnaha Matatini to help inform the COVID-19 communications strategy. Additional funding to engage NGOs such as the s9(2)(b)(ii) will be explored and outlined in future advice ahead of Budget 2022.

## **Consultation**

---

23. This paper was consulted with the nascent Interagency Coordination Group comprising: DIA, DPMC, GCSB, MBIE, MFAT, Ministry for Culture and Heritage, Ministry of Education, Ministry of Health, Ministry of Justice, NZ Police and NZSIS.
24. While agencies agree on the need for a Strategic Framework and the proposed elements, there remain some differences in views as to the financial implications on agencies of developing this workstream. These will be worked through alongside the development of the Framework.

## **Communications**

---

25. As part of the process to develop a Strategic Framework, we will work with non-government partners to establish the most appropriate and effective communications approach.
26. International experience shows that it is best not to directly address mis/disinformation, particularly through an official spokesperson, as this can lend legitimacy to the message/messenger or reinforce government conspiracy narratives.

<b>Attachments:</b>		
<b>Attachment A:</b>	Restricted	Strengthening New Zealand's Resilience to Mis/Disinformation





## ATTACHMENT A

### National Security Policy Insights Series

*Policy Insights papers apply a policy lens to emerging national security challenges to develop a better understanding of cross cutting risks and opportunities, support risk identification and management, and build national security agility and future focus. Their aim is to offer high-level policy insights that are useful to agencies and advance a more strategic approach to national security. The Policy Insights series is prepared by DPMC's National Security Policy Directorate, in consultation with sector agencies.*

## Strengthening New Zealand's Resilience to Mis/ Disinformation

### Understanding and countering the COVID-19 'infodemic'...

1. Since the first COVID-19 lockdown in March 2020, during which we witnessed the rapid spread of COVID-19-related disinformation, agencies have done a lot of work to understand and respond to the problem:

s6(a)

- The National Assessments Bureau (NAB) produced a number of assessments on COVID-19 and elections-related disinformation.
  - Since July 2020, the AOG Response Group Insights and Reporting Team has continued to monitor and report on disinformation trends. During the Auckland lockdown in August, this helped to inform targeted communications campaigns within affected communities.
  - The Ministry of Business, Innovation and Employment (MBIE) provided funding to Auckland University for research into New Zealand's epidemic model, including a data project by Te Pūnaha Matatini on social media-based COVID-19 related disinformation.
2. The major social media tech platforms, reacting to the reputation problem that disinformation poses for them, also took some steps through this period:
    - Facebook and Twitter removed some of the thousands of QAnon accounts and clamped down on COVID-19-related and US election-related disinformation;

## RESTRICTED

- Google released a new COVID-19 information policy for YouTube;
- Twitter has implemented new policies for flagging disinformation content – including COVID-19 and elections-related disinformation – and makes available disinformation and accounts it has removed available for research; and
- Microsoft has launched new technologies targeting disinformation – NewsGuard and Video Authenticator, as part of its Defending Democracy programme.

### ...and mis/disinformation more generally

3. Meanwhile, mis/disinformation more generally also gained a lot of public attention in New Zealand during the past few months with media organisations such as Stuff, Newsroom NZ, and The Spinoff, and independent organisations such as Netsafe<sup>3</sup> and InternetNZ drawing attention to the problem via public campaigns. These independent narratives are especially welcome and helpful, as they are less likely to be associated with conspiracy theories about state control than if they came from a government agency.
4. Major platforms have also reached out to New Zealand on disinformation issues, through Ministers and senior officials. This has included engagement as part of Christchurch Call implementation, in relation to the October General Election, and material relating to the COVID-19 pandemic. s9(2)(ba)(i)

5. Similarly, a range of civil society organisations and social enterprises specialising in disinformation issues has reached out to New Zealand officials to offer engagement and support on disinformation and related issues. s6(b)(ii)

Meanwhile, the Classification Office is currently developing an in-depth survey to help inform a better understanding of public attitudes towards and perceptions of disinformation.

6. In respect of central government activity, processes were put in place by DPMC, the Ministry of Justice (MOJ) and the intelligence agencies for addressing elections-related disinformation. And looking ahead DIA, with the Ministry for Culture and Heritage (MCH), is scoping a potential review of media content regulation, which may provide an opportunity to address policy issues relating to mis/disinformation. However, DIA and MCH are still at the early stages of this work, and the commencement and scope of a potential review would depend on Ministerial responsibilities and priorities. A more immediate response for some aspects of mis/disinformation may be needed than could be delivered by the media content review.

---

<sup>3</sup> In August, as part of their awareness campaign to help people understand and recognise mis/disinformation, Netsafe released the result of a nationally representative survey of New Zealanders' perceptions of fake news. <https://www.netsafe.org.nz/yournewsbulletin/>

7. In related work, as noted in the Government's response to the report of the Royal Commission of Inquiry, MOJ is progressing work around possible new hate speech/hate crime legislation, and work is underway to establish a National Centre of Excellence to focus on diversity, social cohesion, and preventing and countering violent extremism.

**We need coordination in order to strengthen New Zealand's resilience to mis/disinformation**

8. Despite the work that has been undertaken and is ongoing, the system remains fragmented. It is lacking overarching leadership and coordination, an enduring monitoring capability (especially for non-COVID-19 related issues), a policy and referrals framework, and guiding principles.
9. Without these we risk continued fragmentation, duplication of effort, lack of strategic direction or critical mass, and an inability to identify and act on threats before or as they emerge. Consequently, in the absence of change, there would continue to be a range of ad hoc activities that do not contribute to a strategic goal of building New Zealand's resilience to mis/disinformation. **We recommend the following steps to ensure coordination of the issue:**

**Establish a workstream lead and an Interagency Coordination Group**

10. While responsibility for managing different aspects of mis/disinformation will inevitably remain dispersed, the strategic oversight of lead agencies is necessary to ensure relevant stakeholders are connected and coordinated, and their actions align with the delivery of the wider policy direction and, if necessary, response.
11. While the issue of mis/disinformation crosses multiple portfolios, there are some agencies that will be better placed to take the lead on this issue, in particular:
  - DPMC, as the central agency for coordinating the national security system and host agency for the Strategic Coordinators that address cross-government work programmes on significant, related national security issues (Cyber Coordinator, Foreign Interference and Counter-Terrorism). DPMC is also home to the Prime Minister's Special Representative on Cyber and Digital, acting as a senior-level interface with the technology and digital sector on security and public safety; and
  - DIA, as the lead agency for Digital Safety and Countering Violent Extremism Online.<sup>4</sup> DIA administers the Films, Videos and Publications Classifications Act 1993 (and is therefore responsible for censorship policy), hosts the Digital Safety Group and Government Chief Digital Officer and, with the Ministry for Culture and Heritage (MCH), is at the early stages of scoping a potential review of the media content regulatory system.

---

<sup>4</sup> DIA and DPMC also jointly lead the government's Preventing and Countering Violent Extremism (PCVE) work programme, which will have significant overlaps with mis/disinformation.

**RESTRICTED**

12. There are potential complications with any one government agency taking the lead. For example, the perception of an agency such as DIA, which is involved in censorship and compliance, leading the government's response to mis/disinformation may reinforce conspiracy theories about state control of media. However, this kind of narrative is likely to surface within conspiracy theory circles regardless of which agency is involved.
13. There are also potential resource constraints for agencies picking up new workstreams. s9(2)(g)(i) [REDACTED] As there is a need to push ahead with this work as a matter of priority, however, **we recommend that DPMC leads this workstream, at least in the short term, working collaboratively with a group of relevant agencies to coordinate the whole-of-system response.**
14. DIA recently convened a meeting of relevant agencies to consider this paper and we recommend that these participating **agencies should form the basis of an Interagency Coordination Group: DIA, DPMC, GCSB, MBIE, MFAT, Ministry of Culture and Heritage, Ministry of Education, Ministry of Health, Ministry of Justice, and NZ Police.** The intention is that this group will begin to monitor (within existing resources) current mis/disinformation risks, start to build connections with non-governmental partners and, where required, inform and coordinate public communications responses.

Identify a Group of Ministers

15. Sitting above the agencies, **we also recommend that rather than having a single Minister responsible for disinformation issues, there should be a group of relevant Ministers to whom issues can be flagged.** Given the nature of the challenge, it is more appropriate to spread the issue across several portfolios.
16. Rather than this group meeting on a formal or regular basis, the Interagency Coordination Group will escalate or flag issues to the group of Ministers as necessary, seeking decisions on more sensitive policy and communications issues, and ensuring the Government is well informed on mis/disinformation trends.
17. **We recommend that the Ministerial group should comprise:**

- **Minister for National Security & Intelligence, Rt Hon Jacinda Ardern**

*Mis/disinformation gives rise to and impacts several national security risks, for which the Minister for National Security & Intelligence has responsibility. The response to mis/disinformation will also have implications for other work streams in the national security portfolio, including countering violent extremism and foreign interference.*

- **Minister of Education / Minister for COVID-19 Response, Hon Chris Hipkins**

*A key avenue for strengthening resilience to disinformation is through the development of effective education programmes that ensure continued effort on building science and numeracy literacy, and new areas of focus around critical thinking and media literacy.*

## RESTRICTED

*Disinformation is also one of the most significant risks to our COVID-19 response and the effective roll-out of a vaccine.*

- **Minister of Health / Minister Responsible for the GCSB & NZSIS, Hon Andrew Little**

*The Ministry of Health is the lead agency for the COVID-19 vaccine, which is likely to present our greatest disinformation challenge over the coming year. Many disinformation narratives may be generated by and/or spread by state actors, which means the intelligence agencies will play a key role.*

- **Minister for Broadcasting and Media / Minister of Justice, Hon Kris Faafoi**

*The Minister for Broadcasting and Media, along with the Minister for Internal Affairs, is scoping a review of content regulation which may have overlaps with this work on disinformation. While yet to be finalised, a review of the way content is regulated in New Zealand would seek to address gaps and inconsistencies in the current content regulation framework. The Minister for Broadcasting and Media is also responsible for work programmes that aim to build a strong and independent media sector which may assist in providing accurate sources of information to counter dis/misinformation. This includes the Strong Public Media Programme which is assessing the viability of establishing a new public media entity and the Investing in Sustainable Journalism initiative which aims to protect public interest journalism.*

- **Minister of Internal Affairs, Hon Jan Tinetti**

*In addition to scoping the potential review of media content regulation with the Minister for Broadcasting and Media, the Minister of Internal Affairs also has responsibility for Digital Safety (including CVE online), the Films, Videos and Publications Classification Act, and setting and monitoring the strategic direction of independent Crown Entity the Office of Film and Literature.*

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

*The Minister for the Digital Economy and Communications is responsible for the digital safety work programme, which includes efforts to counter a range of online harms and promote online safety.*

Develop a strategic framework for Cabinet Consideration

18. **We propose that the Interagency Coordination Group develops a strategic framework for strengthening New Zealand's resilience to mis/disinformation. Agencies would look to take this to Cabinet for endorsement in early 2021** (noting that the pre-Christmas period is likely to be filled with RCOI-related issues).
19. Some thinking has already been done by agencies, and subject to Cabinet approval, a strategic framework might build on the proposals outlined in the following section. **Key elements of this framework will need to address the public and statutory mandates**

**for monitoring and addressing the disinformation problem, as well as the potential financial implications for agencies.**

20. It will be essential that this process includes close consultation with academia, civil society organisations, the media council, and other key public stakeholders to ensure it encapsulates the views and experience of experts, is transparent, and achieves public buy-in. It will also be vital to ensure that this work is appropriately connected to other relevant national security and social inclusion workstreams. As noted in the Report of the Royal Commission of Inquiry into the Terrorist Attack on the Christchurch Masjidain, it is important to recognise that everyone in society has a role in making New Zealand safe and inclusive.

### **Possible elements of a strategic framework on disinformation**

#### Encourage the creation of a multi-stakeholder forum

1. **Agencies propose engaging with non-government partners and encouraging them to convene and lead a wider stakeholder group** to consider and address the challenges posed by non-state mis/disinformation.
2. Noting the massive complexity of the mis/disinformation problem, and its all-of-society impacts, **a collaborative multi-stakeholder forum – which brings together all relevant civil society and academic experts, independent organisations, social media and tech platforms as well as relevant government agencies** – would be preferred. A list of potential participants is included at Appendix Three.<sup>5</sup>
3. Recognising the range of research, awareness and counter-disinformation activities already being undertaken by media organisations, tech platforms and civil society groups/individuals, there is a wealth of expertise within New Zealand that could usefully be leveraged to build the country's resilience to mis/disinformation.
4. In many, if not most, cases, these organisations will be better placed than government agencies to publicly counter the effects of disinformation in New Zealand. This has been demonstrated recently in efforts from scientists, academia and the media to provide a steady stream of factual information to counter fake news.
5. It will be important, therefore, that any such multi-stakeholder forum be non-regulatory in nature and that it builds and maintains the public trust. By virtue of its diverse membership, such a forum will also be well placed to create a forward calendar of key events and issues that might be subject to mis/disinformation, as well as to engage in additional outreach to independent experts, community leaders, key influencers and media.

---

<sup>5</sup> We are aware that a number of academics have already partnered with NetSafe, media and civil society organisations to collectively look at the disinformation problem. In early discussions, they are supportive of an idea to widen this into something like a multi-stakeholder forum.

Develop guiding principles to inform how we counter mis/disinformation

6. It is clear from available research and international experience that efforts to mitigate the effect of disinformation must be based on principles of transparency, integrity, accountability and stakeholder participation. They must also uphold the principles of a free, secure and open internet, privacy and New Zealand's human rights commitments, including the freedom of expression.
7. For this reason, and noting the examples of the European Commission and the OECD, **the lead agencies, in consultation with the multi-stakeholder forum, will develop and refine a set of Guiding Principles** for mitigating non-state mis/disinformation.
8. Recognising that mis/disinformation is not a problem that government can "fix", these principles might build on the guiding principles and values underpinning New Zealand's Cyber Security Strategy<sup>6</sup> and InternetNZ's Internet Policy<sup>7</sup>.

Establish a monitoring function

9. Our ability to understand and if necessary combat mis/disinformation narratives in the future depends on us establishing the mandate and capability to monitor for harmful mis/disinformation online, and establishing baselines of such information in social media now that we can track against later on.
10. New Zealand government agencies do not generally undertake proactive monitoring of social media for mis/disinformation, though there have been recent examples: the JIG and the AOG Insights and Reporting Team conducted COVID-19-related monitoring during the level four lockdown; the NZSIS undertook low-level activity to identify disinformation relevant to the 2020 New Zealand General Election; and the NZ Police Open Source Team has increasingly focused on the criminal and national security end of the disinformation spectrum.

11.s6(a)

in the UK this task is carried out by analysts within the Cabinet Office and the Home Office. The equivalent agencies in New Zealand lack the resources and mandate to do this. There are therefore two plausible ways to establish a mis/disinformation baseline and to monitor content going forward:

- i. Establishing a new "fusion cell" to monitor for mis/disinformation. This might be established in DIA within or alongside the CVE Online programme, and comprise staff

<sup>6</sup> <https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf>


"To deepen collaboration and take effective action ... we will work in a way that:

- Builds and maintains trust;
- Is people-centric, respectful and inclusive;
- Balances risk with being agile and adaptive;
- Uses our collective strengths to deliver better results and outcomes;
- Is open and accountable."

<sup>7</sup> <https://internetnz.nz/policy/> "Internet for all; Internet for good."

**RESTRICTED**

from a range of agencies with relevant capability (however this would require a budget); and/or

- ii. Procuring from outside of the government sector monitoring and reporting on mis/disinformation in the New Zealand social media environment. There are some universities, think tanks and providers who likely have the capability to do this for us s9(2)(j)  

  - iii. A possible mixture of both options.
12. For the same reasons that a multi-stakeholder approach is the suggested approach, **it may be preferable for social media monitoring to be primarily undertaken by non-governmental, non-commercial partners**. Perception issues around government agencies carrying out broad monitoring of social media platforms could serve to reinforce conspiracy theories and narratives of state surveillance, censorship and enforcement.
  13. There is also a mandate issue for agencies that would seek to monitor/assess, and this would require some careful policy work to address. The interagency group could consider the models employed by Australia and the UK, which have both stood up 'research' teams to monitor for disinformation, looking at how these operate and under what authorisation and oversight. This work would further benefit from multi-stakeholder input on the social licence required to proceed.
  14. Non-government partners already have the capability to combine data analytics and discourse analysis to highlight key trends and emerging issues, broken down by theme, geographic area and by demographic. They are also more likely to have or source the capability to look across different language media. It may be possible for regular summaries of key trends and data on pre-agreed risk areas to be produced by these partners for use by the multi-stakeholder forum and government agencies. This would also be consistent with a whole-of-society, modern deterrence approach to addressing this problem.
  15. Drawing on the capabilities of non-government partners may require a certain level of new funding, however there are recent COVID-19-related examples of non-government organisations accessing existing funding pools to monitor and analyse disinformation. **It is recommended that the interagency group explores procurement and funding mechanisms to assess whether anything further would be required.**

Create a policy framework, including for assessments and referrals

16. The mis/disinformation spectrum is a broad one, and while most instances of it will be content that does not stray into illegality, may be somewhat socially acceptable and often will constitute political discourse, there will be instances when disinformation crosses into illegal or dangerous activity. The incitement to attacks against cell towers are a recent example.
17. That said, mis/disinformation is an online content area where significant harm can be caused by otherwise legal material. Compared with content and harm types such as Child




## RESTRICTED

Sexual Exploitation and Abuse (CSEA) material, or Terrorist and Violent Extremist content (TVEC), mis/disinformation features a much wider spectrum of 'grey' content, where the harm caused can be difficult to determine as tropes and memes can be used to deliver coded messages.

18. **The interagency group should therefore work to develop a policy framework for identifying what areas should be monitored for disinformation and which issues, based on regular trends reporting, will require more in-depth analysis and assessment.**
19. The basis for the areas that should be covered by social media monitoring and further assessment could realistically include elements from the National Risk Register and the National Security and Intelligence Priorities (NSIPs). For example:

s9(2)(g)(i)



20. **The interagency group will also develop a detailed framework for referrals, where an instance of mis/disinformation meets a specific threshold (statutory or contractual) that requires a more direct response.** For example:

- A state-sponsored disinformation campaign, to be referred to the Strategic Coordinator for Foreign Interference and the intelligence agencies;
- Disinformation used as a tool for radicalisation, to be referred to DIA, the NZ Police and the intelligence agencies;
- Election-related disinformation, to be referred to the Electoral Commission;
- Disinformation that inspires or supports criminal activity, to be referred to the NZ Police (high tech crimes unit, OS monitoring unit, etc.).

Other referrals may also be required: to the tech platforms themselves, the Race Relations or Human Rights Commissioners, the Ministry for Social Development, etc. Clear guidelines should be established to inform who refers, to whom, for what purpose and under what circumstances.

21. More broadly, **the interagency group will consider a range of other policy implications relating to the mitigation of mis/disinformation.** For example:

- Whether interventions for mitigation of mis/disinformation could be investigated as part of the proposed DIA/MCH review of media content regulation;
- a Code of Good Practice that could be agreed with media organisations (as has been established by the European Commission with European media organisations);
- work to support to the use or development of technology to counter deep fakes; and

## RESTRICTED

- consideration as to whether a separate disinformation risk profile is required, or if mis/disinformation should be considered as a dimension of other nationally significant risks.

### Develop holistic strategies for building resilience to mis/disinformation

22. Two of the key tools for building New Zealand's resilience to disinformation will be through the effective coordination of **clear and proactive public communications**, and a focus on **longer term education and social inclusion** that leverages work already underway in schools around active citizenship and online safety.
23. One of the key lessons learned during the COVID-19 pandemic has been the importance of timely, clear and coordinated public information, delivered through identifiable and trusted channels. During the Auckland lockdown, this understanding became even more important, with the need for nuanced, community-specific messaging from trusted advisors.
24. This concept is equally applicable to other risk areas prone to mis/disinformation. But in order to ensure a coordinated approach to public communications, **lead agencies will need to work with the multi-stakeholder forum to develop a communications framework**. This would not need to be overly prescriptive but could ensure that agencies do not respond to disinformation in an ad hoc fashion. For example, the UK has produced a "Tool Kit" for agencies to address and respond to disinformation. This might be a useful option for helping agencies to calibrate their communications.
25. Key elements of this framework could include:
  - That where possible public communications should be proactive, not reactive. *The aim should be to build trust ahead of time (e.g. a proactive information campaign on COVID-19 vaccines) rather than to respond to or shutdown disinformation or its proponent. Reacting to disinformation can serve to validate rather than counter it.*
  - That where possible public communications should be collaborative – i.e. developed and delivered in partnership with non-government entities, independent experts and community leaders. *Government-driven narratives are not always the most effective communication tools, and they can reinforce conspiracy theories about state control.*
26. **Another vital part of equipping the population to recognise and manage disinformation is to use disinformation awareness campaigns** (e.g. Netsafe's "Your News Bulletin") **and broader education strategies** to develop public understanding of disinformation. Improving science and numeracy literacy has been shown to reduce susceptibility to mis/disinformation. And strategies successfully implemented in Finland and Sweden include the introduction of critical thinking elements into all aspects of the school curricula. The purpose of this is to build, from an early age, the ability of people to

**RESTRICTED**

distinguish between authentic and false narratives and have the tools to question and fact check.<sup>8</sup>

27. New Zealand could implement a similar strategy in order to meet the long-term goal of building resilience to mis/disinformation. We already have 'active citizenship' and online safety initiatives in schools, and it may not require much from a curriculum perspective to extend these to include social media literacy and critical thinking tools. Additional funding may, however, be required. It will be important for the Ministry of Education and organisations such as Netsafe (both members of the Online Harms Prevention Group) and SeniorNet to be part of the multi-stakeholder Forum.


Released under the Official Information Act 1982

---

<sup>8</sup> An added benefit of these programmes, which fit within the scope of what is sometimes termed 'modern deterrence', is that they can also build resilience to radicalisation and can provide a boost to other social cohesion programmes.

## APPENDIX ONE: The mis/disinformation problem

### Mis/disinformation<sup>9</sup> gives rise to and impacts several national security risks...

1. While dis and misinformation are not new phenomena - and are not neatly confined to the online environment - the internet has decentralised the production and dissemination of information, amplifying the volume, speed, and reach of mis/disinformation.
2. Social media presents a particularly effective and low-cost enabling platform, from which billions of users source their news. Echo-chamber dynamics, 'social proof' and the pursuit of viral content are manipulated by state and non-state actors to place mis/disinformation into online spaces and boost their prominence. This can be further amplified by users with pre-existing biases and can raise doubts among those not already predisposed to conspiracies. Users with lower levels of formal education or literacy in a specific topic, as well as those communities with an historic distrust in government, are especially susceptible.
3. The significance of mis/disinformation for national security became particularly apparent during the 2016 US Presidential election, when disinformation about candidates and policies was spread by malicious actors to interfere with the electoral process. It has been further highlighted by an explosion of disinformation during the COVID-19 pandemic ("the infodemic"). State actors have used disinformation campaigns to divert blame, showcase the 'failings' of other systems, and are exploiting the situation to achieve longer-term strategic goals. Non-state actors, meanwhile, have used mis/disinformation to undermine public health narratives, including by spreading views about the cause and origin of the pandemic (e.g. claiming it is a bioweapon, or linking it to 5G), questioning the political motives of lockdowns and mask use, and promoting conspiracy theories about future vaccines.
4. s6(a), s9(2)(g)(i)  
 And as mis/disinformation continues to grow and technology evolves (e.g. deep fakes), people may find it increasingly difficult to discern fact from falsehood. This confusion over what is true could not only result in individuals making misinformed choices in their own lives, it could also have significant consequences for national security:
  - the politicisation of scientific fact (e.g. on a range of issues including pandemics and climate change) contributes to anti-intellectualism and can **undermine effective policy responses**, including on public health responses to COVID-19;

<sup>9</sup> **Disinformation** is false or misleading content (or the omission of content) designed to achieve a strategic purpose. Whether the actor producing and disseminating the disinformation is pursuing ideological or commercial goals, the effort is designed to influence audience perceptions, opinions and/or behaviour (e.g. QAnon conspiracy theories). **Misinformation** is information that is false or misleading but, unlike disinformation, is not produced or disseminated in pursuit of an underlying ideological or commercial purpose (e.g. anti-fluoride information). **Malinformation** is information that may be based in reality, but is spread with the intent of causing harm.

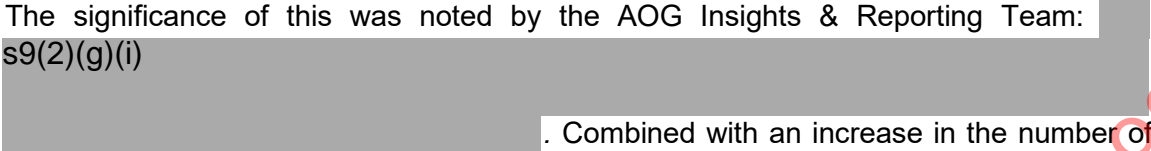

## RESTRICTED

- mis/disinformation about specific groups of people **can create and amplify social divisions, challenge national values, foster extremist views and lead to radicalisation**, break down social cohesion and, in some cases, incite violence towards minority groups;
  - mis/disinformation and conspiracy theories can permanently **damage the reputation of elected officials and/or their policies, undermining the integrity of elections and democracy** more broadly;
  - mis/disinformation and conspiracy theories can have a corrosive effect, **undermining trust in public institutions and the social contract**, with attendant consequences for policy making and service delivery;
  - mis/disinformation can have an **impact on critical infrastructure**: conspiracy theories during the COVID-19 pandemic led people in a number of countries, including New Zealand, to attack 5G and other cell towers. A recent British report noted the possibility of disinformation being used to overload the power grid through the false promotion of cheap power during peak hours;
  - mis/disinformation can also have **economic repercussions**, including through influencing the stock market and investment decisions. For example, a 2013 tweet from the hacked account of the Associated Press claiming that former President Obama had been injured in an explosion, resulted in a brief \$130billion devaluation of the US stock market; and
  - mis/disinformation can also **undermine confidence in the online environment**, directly threatening our ability to achieve the vision in the cyber security strategy that New Zealand is confident and secure in the digital world, enabling New Zealand to Thrive Online. In addition to the attendant cybersecurity issues this gives rise to, it can also have significant economic and service delivery impacts, affecting uptake of digital technology.
5. Amongst our closest security partners, oversight of the disinformation issue is coordinated by several different agencies and responses vary from state-controlled counter-narratives through to funding for civil-society initiatives. A summary of their responses is attached at Appendix Two.

### ...and infodemics are spreading in New Zealand

6. New Zealand's relatively high trust in the mainstream media and government institutions has largely inoculated the general population from believing disinformation. However, this did not create total protection against the increase in COVID-19 and elections-related disinformation that circulated online following the August lockdown in Auckland.
7. The internationalisation of disinformation emanating from the US and/or amplified on US-based platforms is one factor in this. Anti-mask and anti-lockdown narratives, often couched in broad human rights and basic freedoms terms (and often grounded in narratives linked to the US Constitution), found fertile ground amongst followers of a few influencers, political parties and some church congregations.

**RESTRICTED**

8. Some of these theories included that the government was intentionally withholding information from the public, that the outbreak in Auckland was worse than reported, that the government was “utilising” the outbreak to impose martial law or otherwise erode human rights, and that the outbreak was intentionally planned to manipulate the election.
9. The significance of this was noted by the AOG Insights & Reporting Team:  s9(2)(g)(i)  . Combined with an increase in the number of anti-vax views being expressed and shared on social media platforms, this highlights that there remains a significant risk for the rollout of a COVID-19 vaccine.
10. More broadly, there was also during this period a proliferation of New Zealand-based Facebook groups promoting far-right QAnon theories alleging that the world is run by a cabal of Satan-worshipping paedophiles who are plotting against President Trump while operating a global child sex-trafficking ring. The US “documentary”, ‘Plandemic’, which claims a secret society of billionaires is plotting to gain global domination by controlling people through a COVID-19 vaccine, has also been widely shared in New Zealand.
11. Many people sharing these conspiracies may have good intentions, but they also have a fundamental distrust of government, “experts” and the media.<sup>10</sup> This is also evident within New Zealand’s Māori and Pasifika communities, where an intergenerational distrust of government and media, plus lived experience of systemic neglect and racism are all factors that have enabled false information to gain traction. One example of this was the rumour that those who tested positive for COVID-19 would have their children removed from them by Oranga Tamariki.
12. There is potentially a Treaty of Waitangi element to this, with racist disinformation narratives, and disinformation about the Treaty itself, of concern. Additionally, through engagement with Māori on other digital issues (e.g. Budapest Convention accession, cloud computing and data governance) several partners have identified susceptibility to disinformation and conspiracy theories among Māori communities as an area of particular concern.
13. Gendered disinformation has received less public attention, but also poses a significant threat internationally and in New Zealand. A recent UK/US report has found that online spaces are being systematically weaponised against women leaders, with politically motivated gendered stereotypes and personal attacks posing a serious threat to women’s equal political participation.

---

<sup>10</sup> A number of studies also suggest that poor science and numeracy literacy is linked to greater susceptibility to conspiracy theories and fake news.

## APPENDIX TWO: The international dimension

1. Amongst our closest security partners, work to counter disinformation is coordinated by a number of different agencies, and responses vary from state-controlled counter-narratives through to funding civil-society initiatives. This work is evolving very quickly and, as such, below is only a very brief snapshot of the various parts of Five Eyes' governments that are addressing the issue of mis/disinformation. We will be engaging more closely on this issue in 2021 to learn more about partner approaches.
2. In Australia, while efforts are underway to understand the domestic social and behavioural impacts of disinformation, the focus has predominantly been on state-sponsored disinformation:
  - **Counter-disinformation taskforce hosted by DFAT**, set up in June 2020. Focused on tracking and responding to mis/disinformation and malign messaging in the Pacific and South East Asia.

s6(a)

3. In Canada, there has been a dual track approach:
  - **Rapid Response Mechanism Canada (RRM)**, part of the G7 RRM, undertakes focused research to understand potential foreign threats against Canada, and to identify tactics and trends. Member also of the Security and Intelligence Threats to Elections (SITE) task force.
  - **Canadian Heritage has the lead on non-state disinformation** and takes a multi-stakeholder approach in working with civil society to address the problem through education and awareness campaigns.
  - **Public Safety Canada** also hosts the **Canada Centre for Community Engagement and Prevention of Violence (Canada Centre)**, which promotes coordination, planning, funding and research, and supports interventions.
4. In the UK:
  - **The Department for Digital, Cultural, Media and Sport** coordinates the British response to disinformation through the interagency Counter Disinformation Cell.
  - **A Rapid Reaction Unit within the Cabinet Office** was set up to respond specifically to COVID-19-related disinformation issues, including through working with tech companies to block harmful mis/disinformation.
  - **The Home Office**, through its **PREVENT** and **RICU** teams, has a monitoring function working on online TVEC and radicalisation, that has also focused closely on disinformation over the past year or so.
  - **The Government Communication Service** created "**RESIST**", a **counter-disinformation toolkit** designed for both the government and private sector to help prevent the spread of disinformation.

5. In the US:
  - There are a range of agencies involved in the issue of disinformation, including the intelligence community, the Department of Homeland Security, the Department of Justice and the State Department.
  - Constitutional conventions around freedom of expression and jurisprudence complicate the issue of disinformation, as does the current state of political discourse and deeply entrenched political polarisation. This makes disinformation a complicated issue to address in the US.

### **We are likely to be invited to join an increasing number of international actions**

6. New Zealand has received numerous requests to share reporting, analysis and approaches on countering mis/disinformation, from a range of likeminded partners in both bilateral and multilateral contexts (in Five Eyes (FVEY) fora, NATO and the Canadian-hosted G7 RRM).
7. We joined public statements made by the Freedom Online Coalition<sup>11</sup> in May and November. The statement in May read (inter alia): *[T]he FOC is concerned by the spread of disinformation online and activity that seeks to leverage the COVID-19 pandemic with malign intent. This includes the manipulation of information and spread of disinformation to undermine the international rules-based order and erode support for the democracy and human rights that underpin it. Access to factual and accurate information, including through a free and independent media online and offline, helps people take the necessary precautions to prevent spreading the COVID-19 virus, save lives, and protect vulnerable population groups.* More broadly, FOC members have signalled a need to keep working on disinformation issues.
8. At the 3 September meeting of the Aqaba Process, partners recognised the need for collective work on disinformation issues, recognising the corrosive effects of disinformation on public safety.
9. We expect that likeminded partners will increase offers to work together on further actions, statements, or attributions relating to disinformation. Developing a stronger domestic approach to mis/disinformation would effectively and credibly support our collective understanding and mitigation of the risk.
10. This international work may involve engaging closely with a range of those partners most constructively engaged in this work. Given the sensitivities involved in working on disinformation, the principles applied domestically may also stand us in good stead for international engagement. It is likely that the pool of those able to work well on this issue would be relatively small at present, composed of a subset of liberal democracies that belong to the FOC, and where disinformation has not already substantially undermined the ability of institutions to engage effectively.

---

<sup>11</sup> A partnership of 32 governments, of which New Zealand is one, working with civil society and the private sector to support Internet freedom.

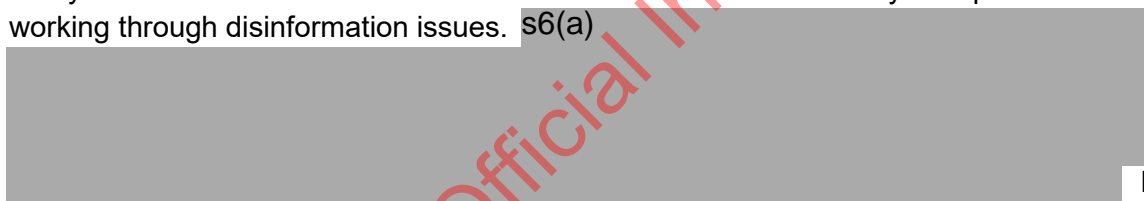


11. s6(a)



12. As with domestic efforts, multi-stakeholder engagement will be critical in working internationally on this issue. We are potentially well-placed to engage on this, building on relationships established through the Christchurch Call. Major technology firms have indicated some interest in further work with New Zealand on disinformation issues. So too have civil society organisations prominent in this area (Global Network Initiative, Global Disinformation Index, Witness, the Web Foundation), many of which participate actively in the Advisory Network to the Christchurch Call. Such engagement provides an important opportunity to understand and engage in international work on combatting disinformation, in ways that are consistent with New Zealand's approach to internet governance and international human rights law.


13. A key issue in this international discussion is the absence of a widely accepted forum for working through disinformation issues. s6(a)



It nonetheless indicates sufficient interest and urgency directed to constructive multi-stakeholder work on disinformation that it might be possible, with careful work, to build a stronger platform for collective action on disinformation.

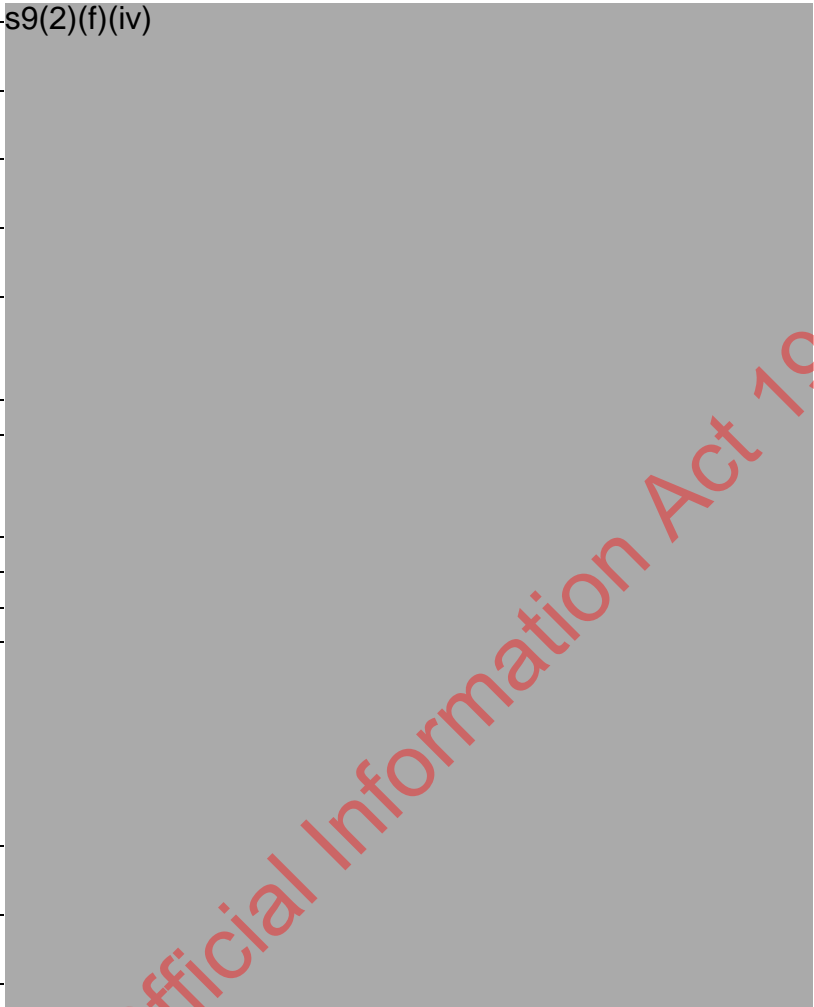
Released under the Official Information Act 1982

**APPENDIX THREE: List of relevant potential stakeholders**

Government Agencies <sup>12</sup>	Non-core government partners	Social media companies and tech platforms
<i>DPMC (NSPD, NAB, Strategic Coordinators)</i>	s9(2)(f)(iv) 	
<i>DIA (Online Harms, CVE Online, Office of Ethnic Communities)</i>		
MBIE		
MFAT		
<i>MCH (including the Broadcasting Standards Authority)</i>		
<i>Ministry of Education (critical thinking and media literacy in the national curriculum)</i>		
<i>Ministry of Health (public health communications)</i>		
<i>Ministry of Justice (electoral disinformation)</i>		
<i>NZ Police (High Tech Crimes, OS Hub)</i>		
NZSIS / GCSB		

<sup>12</sup> The agencies in *italics* are likely to form the basis of the interagency group that will further develop the proposals outlined in this paper. The wider set of agencies listed could participate in the multi-stakeholder forum on a case by case basis (noting that this forum should not be dominated by government agencies).

Te Puni Kōkiri
Te Arawhiti
Ministry for Pacific Peoples
Ministry of Social Development
Treasury
Cert NZ



s9(2)(f)(iv)

Released under the Official Information Act 1982