ODESC
Officials' Committee for Domestic and External Security Coordination

Australia-New Zealand National Security Dialogue

Briefing Pack

12 March 2021
1015 - 1500 hours

Room 9.13 (Boardroom), Pipitea House,
1-15 Pipitea Street, Thorndon, Wellington

Agenda

Time	Item	Lead	Key Speakers (AU)	Key Speakers (NZ)
1000 - 1030	**Arrival and refreshments**			
1030 - 1045	**Chairs' Introductions** s6(a) and Brook Barrington will provide opening remarks with a focus on the importance of cross-cutting policymaking in building national resilience.	AU | NZ	Secretary PM&C	CE DPMC
1045 - 1140	s6(a) s6(a) s6(a)	AU	Secretary DFAT DGNI Secretary Defence Chief of Defence Force	Secretary MFAT DCE DPMC
1140 - 1230	**Session 2 - National Security Policy and Counter Terrorism** Discussion will focus on: • Planned changes to New Zealand's intelligence community following the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain, including the establishment of a new national intelligence and security agency. • Outcomes of Australia's Comprehensive Review into Intelligence	NZ	Secretary Home Affairs DG Security Commissioner AFP Secretary DFAT	DCE DPMC Commissioner of Police DG NZSIS CDF CE MFAT

Time	Item	Lead	Key Speakers (AU)	Key Speakers (NZ)
	Legislation. • Update on Australia's development of a new electronic surveillance regime. • Opportunities to combat terrorism in the region including the global, and growing, threat posed by the extreme right-wing (XRW).			
1230 - 1300	**Break**			
1300 - 1350	**Session 3 - Cyber, Critical Technology and Infrastructure Security** Discussion will focus on: • The nature of, consequences and responses to the SolarWinds, Acellion (NZ Reserve Bank and NSW Government systems) and NZ Stock Exchange compromises. • Lessons learnt from implementation of New Zealand's Cyber Security Strategy 2019 and Australia's Cyber Security Strategy 2020, including identifying areas for alignment. s6(a) [redacted] • Protecting critical infrastructure from diverse risks, including Australia's Critical Infrastructure and Systems of National Significance reforms and NZ's national risk management approach.	AU	Secretary Home Affairs DG ASD Secretary DFAT	Acting DG GCSB Director IACD DCE DPMC
1350 - 1445	**Session 4 - Countering Foreign Interference** Discussion will focus on: • Efforts to address foreign interference in universities and to improve resilience in public funded research agencies. • Reform of New Zealand's Overseas Investment Screening Regime to manage a range of foreign interference risks.	AU | NZ	Secretary Home Affairs DG Security	DG NZSIS FI Strategic Coordinator

Time	Item	Lead	Key Speakers (AU)	Key Speakers (NZ)
	• Opportunities to collaborate in understanding and countering the threat posed s6(a) s6(a) • The operationalisation of Australia's foreign interference legislation, including the first charges being laid in November 2020.			
1445 - 1500	**Final Remarks and Close**	AU | NZ	Secretary PM&C	CE DPMC

Briefing

Attached are a series of individual briefing notes for each of the following sessions:

Briefing	Page
Cover note: Australia's National Security Settings	9
s6(a)	13
Session One: s6(a) s6(a)	23
Session Two: National Security Policy and Counter Terrorism	39
Session Three: Cyber, Critical Technology and Infrastructure Security	53
Session Four: Countering Foreign Interference	65
Annexes: NAB Assessments	75

s6(a)

s6(a) Foreign interference is a common thread throughout these items and, as such, the overlaps and inter-connections may need to be managed during the dialogue discussion.

In order to reduce duplication, the briefings are focussed on the specific issues expected 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, rather than purely as individual session briefs.

Prepared by National Security Group, DPMC, with briefing supplied by GCSB, MFAT, MOD, NAB, NCPO, NZSIS, NSPD, NZ High Commission Canberra, and NZ Police.

s6(a)

s6(a)

s6(a)

s6(a)

s6(a)

s6(a)

- The Minister of Foreign Affairs has recently approved a package of fiscal crisis financing for Solomon Islands (NZ$20 million) to be provided as direct budget support.

s6(a)

s6(a) To-date financing from the International Financial Institutions (IFIs) (the Asian Development Bank, the International Monetary Fund, and the World Bank) has been able to meet the needs of PICs, s6(a)

s6(a)

s6(a)

s6(a)

s6(a)

s6(a) The impact of COVID-19 threatens to roll back economic progress in South East Asia s6(a)

s6(a) New Zealand has responded by providing COVID-19 related support to ASEAN countries, including activities which build economic resilience. s6(a)

s6(a)

Background

1. Despite the successes in keeping COVID-19 out in many parts of the Pacific, the pandemic is causing an unprecedented economic crisis. It is amplifying existing challenges and creating new and urgent issues that need addressing.

2. We expect severe economic disruption across the Pacific, particularly in tourism-dependent economies. An economic decline will likely erase several years of progress in economic development and poverty reduction. Without large amounts of external financial support, these could turn into major economic crises.

s6(a)

s6(a)

New Zealand's economic support to-date

5. New Zealand has to date provided $62 million in budget support for countries in the Pacific that have been impacted by COVID-19. This comprised $40 million in immediate budget support for a number of Pacific countries disbursed in April and May 2020, with a further $22 million provided to Cook Islands and Niue in September 2020.

6. New Zealand is continuing to work closely with key partners such as the Asian Development Bank, the International Monetary Fund, and the World Bank – as well as Australia – on ensuring that all countries in the region are supported. New Zealand's strengths in providing support are our ability to move quickly, be flexible, and provide grant financing.

s6(a)

s6(a)

s6(a)

8. New Zealand has also launched the Pacific SME Finance Facility to help SMEs respond to the COVID-19 crisis through business advisory services, grants, and concessional loans. The NZ$6.94 million pilot will operate in seven PICs (Cook Islands, Fiji, Kiribati, Papua New Guinea, Samoa, Solomon Islands, and Tonga) until December 2021.

s6(a)

s6(a)

s6(a)

11. In response to the impacts of COVID-19, New Zealand committed $12 million to support pandemic response efforts in individual ASEAN countries and $24 million towards economic resilience and sustainable livelihoods in South East Asia. New Zealand is keen to play a constructive role in enabling economic recovery in the region, including through exploring ways to support ASEAN's Comprehensive Recovery Framework, continuing to advocate for open markets and resilient supply chains, and deepening regional economic integration – including upgrading the ASEAN-Australia-New Zealand Free Trade Agreement.

- Ensuring New Zealand purchases sufficient vaccines to cover the populations of Polynesia and the Realm (Cook Islands, Niue, Tokelau, Samoa, Tonga and Tuvalu) and offering end-to-end support to these countries for the roll out of vaccines through the Polynesian Health Corridors Programme.
- Contributing funding to regional and/or multilateral efforts to supply vaccines to Pacific countries beyond Polynesia.
- Supporting immunisation planning, preparedness and roll-out in the Pacific through UN and Pacific regional agencies.
- Making a further NZ$10 million contribution to the COVAX Advanced Market Commitment (AMC) that will purchase vaccines for developing countries, bringing our total contribution to NZ$17 million (and taking advantage of the UK's offer to partly-match funding).

4. For Polynesia – we are offering the six Polynesian countries access to New Zealand's vaccine portfolio, and end-to-end support for vaccine roll-out (including for example, technical assistance for national vaccine plans and vaccinator training).

s6(a)

s6(a)

s6(a)

Agenda Item 2: National Security Policy and Counter Terrorism

Lead country:	**New Zealand**
Lead presenter:	• Tony Lynch – DCE DPMC
Lead responder (AU):	• s6(a) – Secretary DFAT
Support responders (NZ):	• Andrew Coster – Commissioner of Police • Rebecca Kitteridge – DG NZSIS • AM Kevin Short – CDF • Chris Seed – CE MFAT

Scope of item

This item will focus on:

- *Planned changes to New Zealand's intelligence community following the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain, including the establishment of a new national intelligence and security agency.*
- *Outcomes of Australia's Comprehensive Review into Intelligence Legislation.*
- *Update on Australia's development of a new electronic surveillance regime.*
- *Opportunities to combat terrorism in the region including the global, and growing, threat posed by the extreme right-wing (XRW).*

Outcomes sought from the session

- To provide updates on the New Zealand government's planned response to the Royal Commissioner report.
- To commit to working closely with Australia on the review of our national security policy settings and any machinery of government changes that may result.
- To agree to share information on our respective intelligence legislation reviews.
- To reaffirm the importance of working closely together to counter terrorism in the region.

Planned changes to New Zealand's intelligence community following the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain, including the establishment of a new national intelligence and security agency.

Key questions

- We would be interested in Australia's experience of and insights from the creation of the Office of National Intelligence and the Department of Home Affairs.

Talking points

- In December 2020, the report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain was released, outlining its findings in relation to the events of 15 March 2019 and making 44 recommendations on improving New Zealand's counter-terrorism efforts.

- The Government accepted all of the findings of the report and accepted *in principle* all of the recommendations.

- Taken in its totality, the report suggested the need for a fundamental re-examination of our approach to counter-terrorism if we are to truly address the causes of the systemic failures that were identified. In practical terms, this means that the most effective response to the report will come not from considering each recommendation in turn, but by taking a much broader, holistic approach. Crucially, this will also be based on community engagement and partnership.

- Since the report was received, Ministers has led a series of nationwide engagements with communities to understand their priorities and to ensure the Government is aware of all relevant issues. Feedback from those engagements have driven a number of immediate initiatives and thinking around longer term work programmes to create a more socially cohesive society.

- In order to effectively implement these programmes in partnership with communities, an Implementation Oversight Advisory Group will be established over the coming months, providing advice directly to the Lead Coordination Minister.

Strategic approaches to National Security

- The Royal Commission report made a number of recommendations relating to the national security system, including changes to governance and accountabilities, and the establishment of a new National Intelligence and Security Agency. Before any machinery of government work begins, however, we will be undertaking a review of the overarching policy settings that underpin our collective approach to national security.

- We are conscious that any improved response to national security should be developed in response to the broad range of risks and concerns facing New Zealand's diverse communities, not just the threat of terrorism and violent extremism, as was the focus of the Royal Commission. This process will be carried out in partnership with communities, civil society and academia to give effect to the intent of the Royal Commission, fostering a new public conversation on national security and focusing on identifying practical actions that the public can take to contribute to our national security.

- Australia's experience in establishing the Office of National Intelligence (ONI) will be of great interest to us as we work through our review of national security policy settings and develop options for a new national intelligence and security agency.

National Security and Intelligence Legislation

- A counter-terrorism legislation bill will be introduced next month, introducing a number of new offences (including planning and preparation, travel, and training offences), amendments to improve the overall workability of the Terrorism Suppression Act, and an extension to the Control Orders regime.

- We will also be carrying out a broader cross-government review of all legislation related to the counter-terrorism effort to ensure that it is fit for purpose. As part of this process, agencies are currently looking at whether to bring forward the 2022 statutory review of the Intelligence and Security Act to the second half of this year. We are conscious that this Act provides the framework for addressing all national security threats and must be considered from that perspective, rather than just through a counter-terrorism lens.

Background

1. The events of 15 March 2019 were unprecedented in New Zealand; 51 people lost their lives, many more were injured, and communities were scarred. The terrorist attack was perpetrated against people participating in a peaceful religious service. People around the country had their sense of safety impacted through exposure to violence and extremism never before experienced in New Zealand. The terrorist attack was an attack on New Zealand, but more directly an attack on our Islamic community.

2. In November 2020, the Government received the report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (the Royal Commission). Cabinet discussed the Royal Commission's report twice in December 2020; an initial discussion on the content of the report on 1 December, and a substantive discussion on 8 December 2020.

3. Cabinet directed officials to report back in February 2021 on the implementation of the funded initiatives, as well as initial advice on a longer-term programme of work that will aim to meet the overall intent of the Royal Commission's recommendations.

Community engagement

4. Promoting and ensuring New Zealand communities' safety and wellbeing lies at the heart of the Government's response to the Royal Commission. To understand community priorities, the Government has been engaged in a nation-wide programme of meetings to listen to community concerns and ensure that the Government's response aligns with communities' most pressing needs.

5. In the immediate aftermath of the public release of the Royal Commission report, engagement was appropriately prioritised with affected families and survivors in Christchurch in acknowledgement of the deep hurt and pain experienced by the Christchurch Muslim community.

6. In January and February 2021 this engagement extended to Muslim and pan-ethnic/multi-faith communities across New Zealand. Over 30 community meetings have now taken place, with more engagements planned for a broader range of New Zealand communities in coming months.

7. The objectives of this initial phase of engagement have been to:
   - continue to build strong, trusted relationships between these communities and Government as the basis for long-term partnerships,
   - listen to reactions around the report and answer questions,
   - provide information about initiatives underway,
   - understand the key priority issues for communities to inform the development of the Government response,
   - begin a dialogue on how communities can work together with us in shaping the substance of the response and an implementation work programme, and
   - discuss and invite views on the establishment of the Implementation Oversight Advisory Group (recommendation 44).

8. The community meetings were led by Ministers with support from local Members of Parliament from both sides of the House. Officials from a wide range of agencies including the Department of the Prime Minister and Cabinet (DPMC), Office of Ethnic Communities, New Zealand Security Intelligence Service (NZSIS), Ministry of Social Development, Ministry of Business, Innovation and Employment (Immigration NZ), Police, the Ministry of Education, as well as the Human Rights Commission, have participated in and provided support through these events.

9. Based on consistently expressed feedback at the hui and through online Royal Commission response feedback forms, key community priorities include:
   - the provision of ongoing long-term support to the affected whānau and survivors of the 15 March attack,
   - government accountability to communities and a desire for transparency and community involvement in policy development, to include seeing outcomes from their feedback,
   - educational reform to provide culture change and address existing structural racism through curriculum change and improving the cultural competency of teachers,
   - improving the safety of New Zealanders, including through firearms control as well as hate speech/crime legislation,
   - increasing the diversity and cultural competency of the public sector workforce,
   - a well-resourced Ministry of Ethnic Communities,
   - addressing the role of media in perpetuating discrimination and racism,
   - increasing resources to communities to enable their full participation in civil society and to allow for community-led solutions,
   - addressing employment discrimination and providing more employment pathways for ethnic communities, and
   - the need for a long-term work programme on social cohesion that brings together all communities to bring about societal change.

10. There is a need to pivot focus now from listening to community priorities to taking concrete action, noting that some recommendations can be implemented quickly and that others will take more time.

11. Conversations with communities who have not yet been formally consulted with will continue while this work progresses, and channels for community members to provide feedback and receive updates will remain open and ongoing. DPMC will continue to seek community feedback on an engagement forward programme and engagement

design, and agencies will further build capacity to engage in accordance with the IAP2 Public Participation Spectrum.

12. Agencies will also engage with communities on development of individual initiatives and legislative change, and will coordinate and de-conflict to mitigate against engagement fatigue on the part of communities.

13. A new significant phase of engagement on the Government's response will begin from mid-year, once the Implementation Oversight Advisory Group and the Ministry of Ethnic Communities have been established and agencies have progressed a range of other initiatives.

Outcomes of Australia's Comprehensive Review into Intelligence Legislation

We will be in listening mode for this item.

Key Questions

- Any comments from the Australian delegation on their independent intelligence review, including on any challenges and lessons learned, would also be of interest. Insights especially on digital issues would be of great value as we look to conduct our own statutory review of the Intelligence and Security Act and a broad review of public safety and law reform in a digital age.

Update on Australia's development of a new electronic surveillance regime.

We will be in listening mode for this item.

Opportunities to combat terrorism in the region including the global, and growing, threat posed by the extreme right-wing (XRW).

Note: *XRW is a threat within both Australia and New Zealand, but is not considered to be of significant concern in the wider region where Australia and New Zealand already cooperate closely on counter-terrorism efforts. As such, the focus of the material below is largely on domestically focused XRW CT efforts, regional CT cooperation in South East Asia, and cooperation through the ANZCTC.*

Talking points

New Zealand's domestic response to terrorism (NZ Police)

- New Zealand Police is the lead agency for responding to a terrorism or violent extremism event that is underway or an imminent threat. It also collects intelligence on and investigates potential terrorist or violent extremist threats, and undertakes prosecutions or other interventions. Police work in partnership with communities, business and other public sector agencies, Australian counterparts, Five Eyes and other international partners to detect and prevent potential national security threats.

- Police has worked over several years with other agencies on amendments to the Terrorism Suppression Act and Terrorism Suppression Control Orders Act. Police are establishing a programme "Te Raranga, The Weave", to make improvements in identification, recording and management of hate crime, to deliver a service that is more responsive to victims. Police is also undertaking an internal awareness programme to assist frontline to recognise symbology and imagery associated with XRW ideologies.

- A Police-led Multi-agency Coordination and Intervention Programme (MACIP) coordinates multi-agency wrap-around support for individuals who show early signs of harmful behaviour or radicalisation, regardless of any ideological, political or religious motivation. MACIP's purpose is to disengage individuals displaying concerning behaviour and direct their behaviour away from terrorism, violent extremism, and violent acts of hate.

New Zealand's domestic response to terrorism (NZSIS)

- NZSIS has been working on a communications approach to provide regular public updates on New Zealand's terrorism threat environment, including the threat level. This is in line with the Royal Commission of Inquiry's report which emphasised the importance of raising public awareness about national security. The reference to the threat level on the NZSIS website will be updated to show it has been reviewed recently, and the threat review will be referenced in the Director General of Security's speech to the Intelligence and Security Committee later this month.

- NZSIS has been working to proactively identify unknown terrorism threats to New Zealand. We are using indicators of terrorist behaviour to detect previously unknown threats and new intelligence in relation to known threats. We have focussed on collaborating with other government agencies and international partners to further this work.

- NZSIS has been working with other agencies on a range of initiatives to combat terrorism, such as the:
    - amendments to the Terrorism Suppression Control Orders and Terrorism Suppression Act, including a range of new terrorism offences;
    - Public Information Action Plan (published on DPMC's website); and
    - Protecting Our Crowded Places from Attack strategy and guidelines (led by New Zealand Police).

- The upcoming review of the Intelligence and Security Act will also look at the effect of certain provisions on our counter-terrorism efforts.

- GCSB and NZSIS received some funding through Budgets 2019 and 2020 which was used for counter-terrorism initiatives, s6(a) . We are currently seeking further funding for improved counter-terrorism services as part of Budget 2021.

- Discovery is NZSIS's first strategic priority. It is about increasing our access to information, including the provision of data related to terrorism, through engagement with communities, the wider public and other government agencies.

Terrorism in South East Asia

- Terrorism in South East Asia continues to evolve and poses an ongoing threat in the region, including to Australian and New Zealand interests. New Zealand seeks to reduce the risk of South East Asia becoming a target for or source of terrorism by helping invigorate mechanisms that promote coherence and coordination of CT practice and policy across the region.

- Drivers of terrorist activity include the spread of global extremist ideology (especially through social media) and social and religious tensions within South East Asian states. A number of groups operating in the region maintain connections well beyond South East Asia, including to the Islamic State in Iraq and Syria (ISIS).

s6(a)

s6(a)

s6(a)

s6(a)

- This activity underwrites New Zealand's contribution to the international effort in relation to countering terrorism.

s6(a)

s6(a)

s6(a)

Background

Australia-New Zealand Counter-Terrorism Committee ANZCTC

1. New Zealand has been a member of the Australia-New Zealand Counter-Terrorism Committee (ANZCTC) since September 2012, alongside Australian Commonwealth, State and Territory governments. Previously New Zealand had observer status on Australia's National Counter-Terrorism Committee (NCTC).

2. The purpose of the ANZCTC is to contribute to the security of both countries:
   - Through the coordination of a cooperative framework to counter terrorism and its consequences;
   - By enhancing the existing relationship between Australia and New Zealand specifically in relation to counter-terrorism.

3. The ANZCTC is based on strong trans-Tasman cooperation and it has established capabilities in areas such as crisis management, command and control, intelligence and investigation, and media cooperation. New Zealand agencies, most notably NZ Police, benefit from access to a significant amount of counter-terrorism joint training with Australian counterparts, facilitated via the ANZCTC. New Zealand has access to, but is not bound by, strategies, policies and Ministerial advice developed by the ANZCTC for the Commonwealth of Australia, States and Territories.

4. New Zealand participation in the ANZCTC is led by DPMC, with senior representation from the NZ Police and NZSIS. The DPMC Strategic Coordinator is currently co-chair of the ANZCTC for 2020/21, together with Australia's Commonwealth Counter-Terrorism Coordinator, who is the standing co-chair.

s6(a)

s6(a)

s6(a) [redacted]

s6(a) [redacted]

s6(a) [redacted]

New Zealand's terrorism threat environment

8. In New Zealand, CTAG assesses white identity extremism (a subset of right-wing extremism) is also likely to increase in over the coming 12 months, with the Christchurch attacks continuing to influence violent extremism locally as well as globally. s6(a) [redacted] s6(a) [redacted] international politics and events s6(a) [redacted] continue to shape the New Zealand terrorism threat environment.

9. New Zealand's terrorism threat level remains at "Medium" meaning a terrorist attack is assessed as feasible and could well occur. There has been no significant change to our threat environment over the past year.

10. Individuals inspired by either Identity-Motivated Violent Extremism or Faith-Motivated Violent Extremism currently represent the most likely terrorist threat to New Zealand. In the second half of 2020, approximately 40 percent of NZSIS counter- terrorism investigations focussed on individuals whose primary ideology was identity-motivated, and approximately 60 percent on individuals whose primarily ideology was faith-motivated.

11. The most likely terrorism scenario in New Zealand is an attack carried out by a lone actor, adhering to any ideology, using readily available weapons, and with little or no warning.

12. We are seeing the broad range of extremist ideologies in New Zealand becoming increasingly diverse. New subsets are emerging and individuals are increasingly identifying with multiple ideologies and views.

13. The terrorist attack on Christchurch mosques continues to influence the nature of violent extremism in New Zealand. Propaganda and material relating to the attacks are still being shared online and have the potential to inspire or influence violence in other individuals (*also see following section*).

14. It is possible COVID-19 will influence extremist ideologies in New Zealand and increase the rate of radicalisation in a small number of New Zealanders with extremist ideologies.

15. A small number of Identity-Motivated Violent Extremists have access to firearms. While the firearms law reform has affected the supply and lethality of legal weapons, it has not significantly impacted the ability to access firearms, either legally or illegally. Some known Identity-Motivated Violent Extremists have recently applied for firearms licences and others may have access to firearms through family, friends or associates.

16. We are concerned about the potential threat posed by individuals with a violent extremist ideology serving in, or being trained by, security forces. We are aware of a small number of Identity-Motivated Violent Extremist persons of interest who have received military training, including firearms training, within the New Zealand Defence Force.

17. We are also concerned about the online environment supporting and driving violent extremist narratives, including the increasing use of encryption and fast pace of technological change.

Agenda Item 3: Cyber, Critical Technology and Infrastructure Security

Lead country:	**Australia**
Lead presenter:	• s6(a) Secretary of Home Affairs
Lead responder:	• Lisa Fong – Director IACD
Support responders (NZ):	• Bridget White – Acting DG GCSB • Tony Lynch – DCE DPMC

Scope of item

This item will focus on:

- *The nature of, consequences and responses to the SolarWinds, Acellion (NZ Reserve Bank and NSW Government systems) and NZ Stock Exchange compromises.*
- *Lessons learnt from implementation of New Zealand's Cyber Security Strategy 2019 and Australia's Cyber Security Strategy 2020, including identifying areas for alignment.*
- s6(a)
- *Protecting critical infrastructure from diverse risks, including Australia's Critical Infrastructure and Systems of National Significance reforms and NZ's national risk management approach.*

Outcomes sought from the session

- To share information on responses and the implications of recent cyber security incidents on national security.
- Commitment to continue working together in implementing our strategies, undertaking joint efforts where it makes sense, to advance our shared goals of a free, open and secure internet, and minimise the risks to citizens and firms.
- s6(a)
- To understand the proposed Australian critical infrastructure security reforms, and the potential impact they may have on New Zealand.

The nature of, consequences and responses to the SolarWinds, Acellion (NZ Reserve Bank and NSW Government systems) and NZ Stock Exchange compromises

Lead: Director IACD. GCSB

Key questions

- How can Australia and New Zealand better work together to address increasingly global cyber incidents that are affecting our security concurrently?
- Are there areas where we need to increase collaboration to address supply chains threats that are affecting trans-Tasman organisations and commerce?

s6(a)

Talking points

- Recent high profile breaches and incidents have been alarming on an individual basis but not surprising in a global context, given expectations around the growing scope, scale and sophistication of cyber threats from criminals and state-sponsored actors.
- The supply chain compromise related to SolarWinds has starkly highlighted the systemic risks of infrastructure providers serving a wide range of clients with the same product. s6(a)
  s6(a)

s6(a) Instances globally of DDoS attacks on financial institutions, including the New Zealand Stock Exchange (NZX) campaign, highlight the need for critical organisations to be prepared for what are increasingly foreseeable events. s6(a)
s6(a)

- While recent incidents confirm the trajectory of the cyber threat, they provide an opportunity to look at our national and collective responses.
- When it comes to ransomware and other sophisticated cybercrime, New Zealand continues to value the opportunity to work collectively. International partners and companies act as a "force multiplier", without which we have far less of an impact.
- While our domestic focus is on building the awareness and resilience of local organisations, we are keen to work with partners to take action against the technical and financial infrastructure supporting this activity. We appreciate your cooperation on these cyber security incidents, and are keen to cooperate on enforcement action against the specific actors where possible.

Background

Australian position

1. Australia's recent experience of cyber security incidents is similar to New Zealand's. The supply chain incident resulting from vulnerability within the Accellion FTP software, which affected the Reserve Bank of New Zealand (RBNZ), affected the Transport for New South Wales (NSW) and the Australian Securities and Investment Commission.

Australian banks also suffered DDoS attacks in early 2020, as part of a wider global campaign by cyber criminals.

2. Australia's approach to addressing cyber incidents where state-sponsored actors are involved has been largely similar to New Zealand's. s6(a) s6(a)

s6(a)

4. The significant cyber security incidents related to global supply chain issues and international cybercrime campaigns have highlighted the shared issues around managing cyber resilience.

5. The shared nature of the issues are highlighted by:

   - International DDoS campaigns that affected Australian banks and the NZX in 2020;
   - Ransomware campaigns that affected trans-Tasman enterprises including Toll, Lion and Fisher & Paykel s6(a) s6(a) ;
   - Supply chain incidents where breaches of US firms' platforms (SolarWinds and Accellion) affected Australian and New Zealand organisations.

s6(a)

Lessons learnt from implementation of New Zealand's Cyber Security Strategy 2019 and Australia's Cyber Security Strategy 2020 including identifying areas for alignment.

Lead – DCE DPMC

Key questions

- How can Australia and New Zealand identify the priority areas for future collaboration in promoting cyber security and addressing cybercrime?
- As the online environment remains dynamic and subject to disruptive innovation, what challenges does Australia anticipate may shape future strategies?

Talking points

- While the disruption and accelerated digitisation of the economy and society caused by COVID-19 has presented some novel challenges, the fundamentals of improving cybersecurity and addressing cybercrime have not changed.
- Continuing engagement between our two countries on all aspects of cyber security and the promotion of a free, open and secure internet will remain mutually beneficial.
- The linkages between our two economies and societies are as close online as they are offline, if not more so. In the majority of cases, alignment, cooperation, and information-sharing will advance national priorities online.
- Collaboration with industry and civil society was crucial for establishing the priorities and underpinning New Zealand's approach to our cyber security strategy, and we expect this to be the case for any future strategy exercises.
- New Zealand is in the early stages of developing a digital strategy. The Cyber Security Strategy will inform and support the delivery of the digital strategy.

Background

Australian position

1. New Zealand's 2019 and Australia's 2020 cyber security strategies are aligned in their general themes of promoting cyber security broadly across the economy and society, and reinforcing responsible state behaviour in cyberspace.

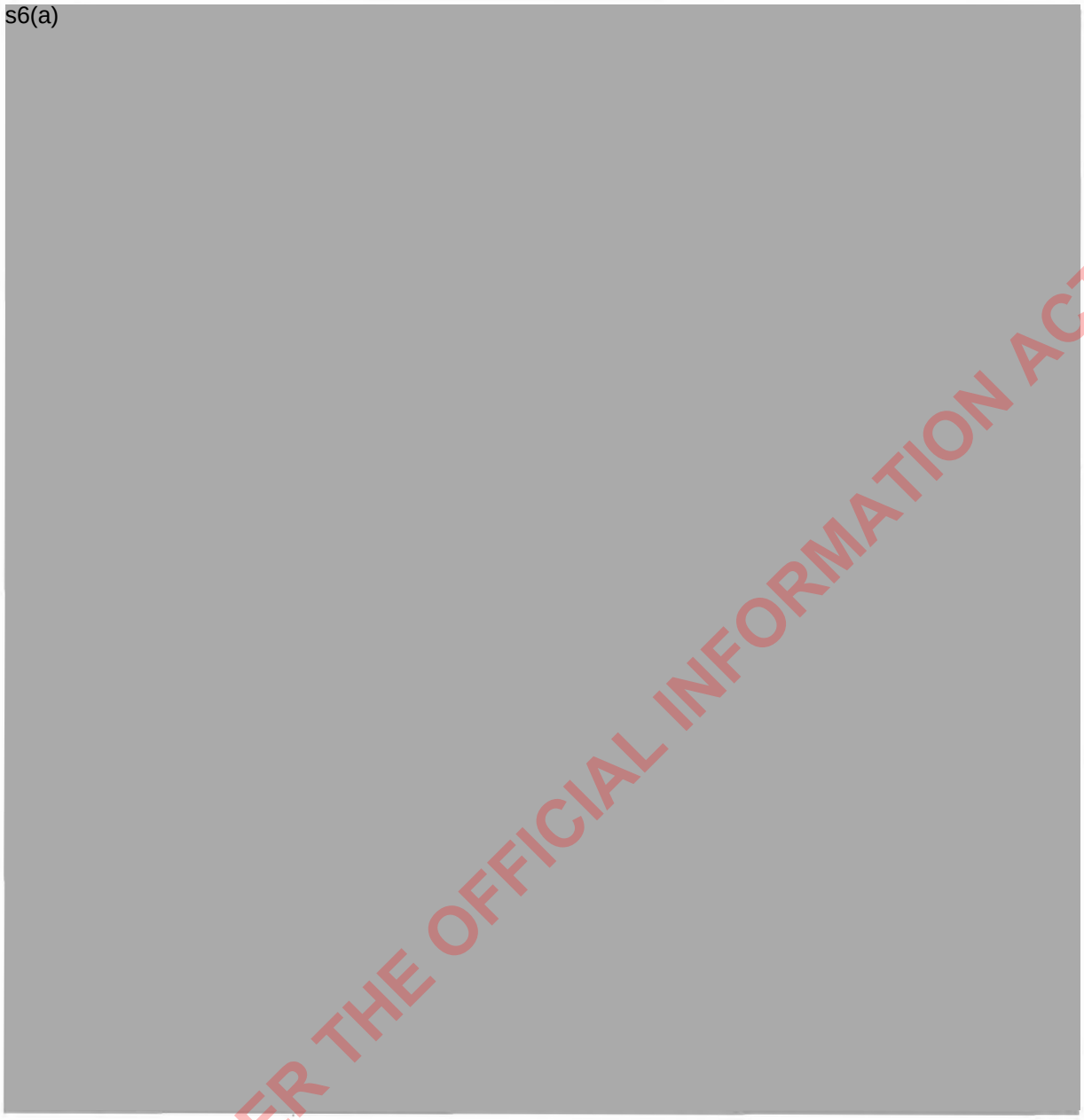
s6(a) [redacted]

s6(a) Both Australia and New Zealand's current cyber security strategies build upon previous iterations and reflect the relative evolution of policy priorities. s6(a) [redacted]

s6(a) [redacted]

4. s6(a) [redacted] s6(a) [redacted] New Zealand's funding is targeted at cross-government and non-government projects; funding for agency capability is not counted as strategy funding (including approximately NZ$8 million over four years for CERT NZ in the 2019 Budget).

s6(a)



6. In December 2020, New Zealand issued a position statement on how international law applies to state activity in cyberspace. s6(a)

s6(a)

s6(a) With this statement, New Zealand joined a range of countries – including Australia – that have sought to articulate their own positions on this issue, bringing greater clarity to areas of agreement and disagreement.

Protecting critical infrastructure from diverse risks, including Australia's Critical Infrastructure and Systems of National Significance reforms and NZ's national risk management approach.

Note: *New Zealand does not have the equivalent of the Australian Critical Infrastructure Centre in the Department of Home Affairs, nor do we have an agreed definition or specific legislation for critical infrastructure. Responsibility for this is devolved across government, local government and owners. The CDEM Act, which covers a range of "lifeline utilities" is currently under review, and there is a broader critical infrastructure workstream under the Hazards and Risks Board (HRB).*

As such, the briefing material below is focused on the cyber security dimensions of critical infrastructure and critical technology.

Key questions

- How will the additional security controls on the Australian critical infrastructure sector work in practice? How will compliance be managed?
- What has been the reaction from your domestic industry to the proposed changes?
- Is Australia planning any new regulation that may apply specifically to critical technologies?

Talking points

Critical Infrastructure

- The National Cyber Security Centre (NCSC) provides advice, and primary consent based technical cyber security support to nationally significant organisations, which may include critical infrastructure. The primary benefit of a consent model has been to build public trust and confidence.
- The Intelligence and Security Act also allows the GCSB to conduct protective security activities with a Ministerial authorisation or warrant.
- Under the New Zealand Information Security Manual, Government agencies are required to report serious cyber incidents. There are also reporting obligations for public and private sector entities under the Privacy Act 2020. We are interested in learning from the Australian experience, including about how positive security obligations will work, and to understand the benefits and any disadvantages of a regulatory approach. We also want to engage closely with you as we consider how New Zealand organisations operating in Australia may be affected.
- s6(a) s6(a) Officials are now undertaking a policy process to look at the best levers to improve cyber resilience of critical systems.

s6(a)

s6(a) [redacted]

Background

Australian critical infrastructure reforms

1. Australia has introduced legislation (the Security Legislation Amendment (Critical Infrastructure) Bill 2020) to build on the Security of Critical Infrastructure Act 2018 – which itself reformed Australia's management of critical infrastructure security, most notably by establishing a Register of Critical Infrastructure Assets. The Act enabled the government to assess vulnerabilities across high priority assets and work with industry to address these, while imposing only a minimal regulatory burden. The Act only applied to electric, gas, water, and maritime ports assets. The new Bill builds on this, including by:
    - Expanding coverage of the Act to a further 11 sectors and introducing definitions of "critical infrastructure assets" specific to each sector;
    - Introducing a "positive security obligation" for critical infrastructure operators, which will entail adoption of a critical infrastructure risk management programme (which takes an "all hazards" approach); mandatory reporting of serious cyber incidents; and in some circumstances providing ownership and operational information to the Register of Critical Assets;
    - Enhanced cyber security obligations for some critical infrastructure and national assets; and
    - Establishing an assistance regime, which creates powers for the government to respond to significant cyber attacks affecting critical infrastructure assets and sectors.
2. These changes will affect New Zealand organisations operating in Australia that fall into the category of critical infrastructure, or systems of national significance, as well as impacting New Zealand organisations that provide services to either category of organisation. DPMC will undertake work to explore the impact of legislation on New Zealand businesses operating across the Tasman, and what support we can provide to those businesses.
3. Under the Privacy Act 2020, entities that have a privacy breach that is likely to cause anyone serious harm, are obligated to inform the Privacy Commissioner and any affect individuals as soon as possible. The New Zealand Information Security Manual outlines the process for entities to record and report breaches, and recommends that entities report serious and critical cyber incidents to the GCSB's National Cyber Security Centre (NCSC). However, unlike the Australian reforms, there is no blanket legislation mandating cyber breach reporting, or a positive security obligation for critical infrastructure.

New Zealand's approach to the cyber security of critical infrastructure

4. s6(a) [redacted]

s6(a)

s6(a) Several agencies have responsibility for critical infrastructure protection generally, including MBIE, MBIE, and Treasury.

5. More specifically, supporting the cyber security of critical infrastructure organisations is a key aspect of New Zealand's Cyber Security Strategy 2019. The GCSB, through the NCSC, responds to and mitigates cyber threats, and provides defensive, consent-based cyber threat services to public and private sector organisations of national significance. These programs are called CORTEX, which provides technical cyber services to nationally significant organisations, and Malware free networks (MFN).

The NCSC operates its technical services primarily on a consent based model

6. Malware free networks (MFN) is a detection and disruption capability that the NCSC has developed and are deploying with Internet Service and Managed Security Providers (ISPs &MSPs). MFN enables the NCSC to scale CORTEX benefits to a wider set of organisations by partnering with these providers, who provide it free of charge to their customers. It is notable that, in our engagement with ISPs and MSPs consent features part of those conversations, as these Providers consider how they will ensure customers are willing to receive the service.

7. The effectiveness of NCSC's focus on consent is difficult to measure, but it's value has certainly been felt since the initiation of project CORTEX and over the past five years. The primary benefit of a consent model has been to build public trust and confidence.

s6(a)

s6(a) However, the Intelligence and Security Act allows the GCSB to conduct protective security activities both with consent and with Ministerial authorisation or warrant. s6(a)

s6(a)

s6(a) The Intelligence and Security Act allows the NCSC to conduct protective security activities both with consent, but also with a Ministerial authorisation or warrant. s6(a)

s6(a)

9. The NCSC also engages with industry sectors directly through Security Information Exchanges (SIEs). These Exchanges occur regularly throughout the year, and are opportunities for sectors to become better coordinated, develop standards, and create a community of best practice.

s6(a)

Agenda Item 4: Countering Foreign Interference

Lead country:	**Australia & New Zealand**
Lead presenter (AU):	• s6(a) – Secretary of Home Affairs
Lead presenter (NZ):	• Rebecca Kitteridge – DG NZSIS
Support responders (NZ):	• Tony Lynch – DCE DPMC • Carolyn Tremain – CE MBIE • Kevin Moar – FI Strategic Coordinator, DPMC

Scope of item

This item will focus on:

- *Efforts to address foreign interference in universities and to improve resilience in public funded research agencies.*
- *Reform of New Zealand's Overseas Investment Screening Regime to manage a range of foreign interference risks.*
- s6(a)
- *The operationalisation of Australia's foreign interference legislation, including the first charges being laid in November 2020.*

Outcomes sought from the session

- Commitment to continue working together to share information about foreign interference, and the measures we are taking to build resilience and counter it.

s6(a)

Efforts to address foreign interference in universities and to improve resilience in public funded research agencies

Talking points

- Our university sector's experience of foreign interference is a microcosm of what New Zealand experiences.

    a. The sector is the target of economic espionage through a range of vectors.
    b. Its infrastructure, networks and data are targeted by cyber actors.
    c. It is vulnerable to threats of economic coercion.
    d. Foreign actors can seek to cultivate relationships of influence with academics and management through covert and overt means.
    e. There are concerted efforts to shape discourse among students and academics.
    f. Students, including international students, can be monitored and harassed by those working for foreign states, and are vulnerable to coercion.

- Most of our effort to date has been on protecting New Zealand's sensitive technology. We know there is leading edge research carried out in our universities and Crown Research Institutes that is targeted by foreign states s6(a) . We are focused on technology that is dual-use, or which has the potential to underpin significant economic value for New Zealand.

- Our first line of defence is to raise awareness and give institutions tools to manage these risks. Government can provide regulatory backstops, but research organisations themselves need to manage and understand the risks. Properly informed, the interests of research organisations align with New Zealand's national interest: our universities do not want to contribute to military capabilities that can be used against our interests, or to the creation and maintenance of oppressive systems of state control.

- Through 2019 and 2020 we delivered a programme of awareness briefings to the leadership teams of every university, Crown Research Institute, and a range of other intermediaries. These briefings were developed and delivered jointly by NZSIS, GCSB, MFAT, MBIE, and DPMC.

- This month NZSIS, Universities New Zealand and Science New Zealand are launching joint guidance on "trusted research". This is the public face of ongoing collaboration to develop and implement good security practices in our research institutions.

- Universities New Zealand has established a senior working group to develop internal policies in relations to all aspects of sensitive technology, including: HR policies, staff travel, student visas, research conduct, ICT policies, and ethnics committees.

- We are funding the Royal Society of New Zealand to update and promulgate a Research Charter of principles underpinning sound research practice in New Zealand. "Research integrity" and "scientific ethics" are major lenses through with we will engage the research community.

- Our outreach is backed by a range of policy and regulatory improvements.

- Crown science investments are generally allocated via competitive bid processes, and these bids are now subject to a national security due diligence that looks at risks associated with the research field, and risks associated with international collaborators. A range of proportionate risk mitigation measures are used, depending on the assessed level of risk, and enforced by contract. They include, for example, requiring the implementation of Protective Security Practices in line with government guidelines, or requiring the organisation to undertake regular risk-assessments and report them to MBIE.

- We have extended the scope of the catch-all controls under our export control framework, in relation to items that have a military end use. We are preparing for further modernisation of our Export Controls framework, including to control Intangible Transfers (i.e. the transfer of knowledge, rather than goods).

s6(a)

- We have mechanisms for engaging with universities on specific matters of concern, ranging from international collaborations of security concern, through to handling visiting delegations. Like our other work, case management is an inter-agency effort.

- Taken together, these measures will allow us to manage risks to sensitive technology effectively. Our assessment is that we are near the forefront among likeminded countries in responding to this risk.

- Our universities have three missions – research, teaching and public service. We have more work to do to manage risks to the integrity of the last two missions. We need to ensure the safety and rights of students and academics are protected from foreign threats. We would welcome learning how Australia is thinking about this issue.

Reform of New Zealand's Overseas Investment Screening Regime to manage a range of foreign interference risks.

Talking points

- In late-2018, the New Zealand government commissioned a review of the Overseas Investment Act (Act) A key objective of this reform was enhancing the government's power to manage foreign investment risks, including national security risks.

- In June 2020, legislation was passed to strengthen the Act in three key ways:
  - A national interest test was introduced, to allow the government to block any investment ordinarily screened under the Act deemed contrary to the national interest.
  - A temporary Emergency Notification Regime (ENR) was introduced, to allow all controlling investments (irrespective of the value of those transactions) to be screened to ensure they were not contrary to the national interest. This was to respond to the risks posed by COVID-19, including falling firm values which may take important assets outside the normal screening regime (where a $100m threshold ordinarily applies).
  - A narrower national security and public order call in power will take effect when the ENR is repealed (in general terms, when the COVID crisis has passed). This will only apply to investments in strategically important businesses – such as telecommunications providers – and the Minister will only be able to block transactions if they pose significant national security or public order risks.

s6(a) [redacted]

- NZSIS and GCSB are responsible for providing national security advice to support the Overseas Investment Office and responsible Minister in their decision making. s6(a) [redacted]

- In 2021, Australia passed legislation that will enable it to share case specific data with foreign governments in certain circumstances. New Zealand is interested in better understanding how such arrangements would work and what the requirements for entering into them would be.

The operationalisation of Australia's foreign interference legislation, including the first charges being laid in November 2020.

Background

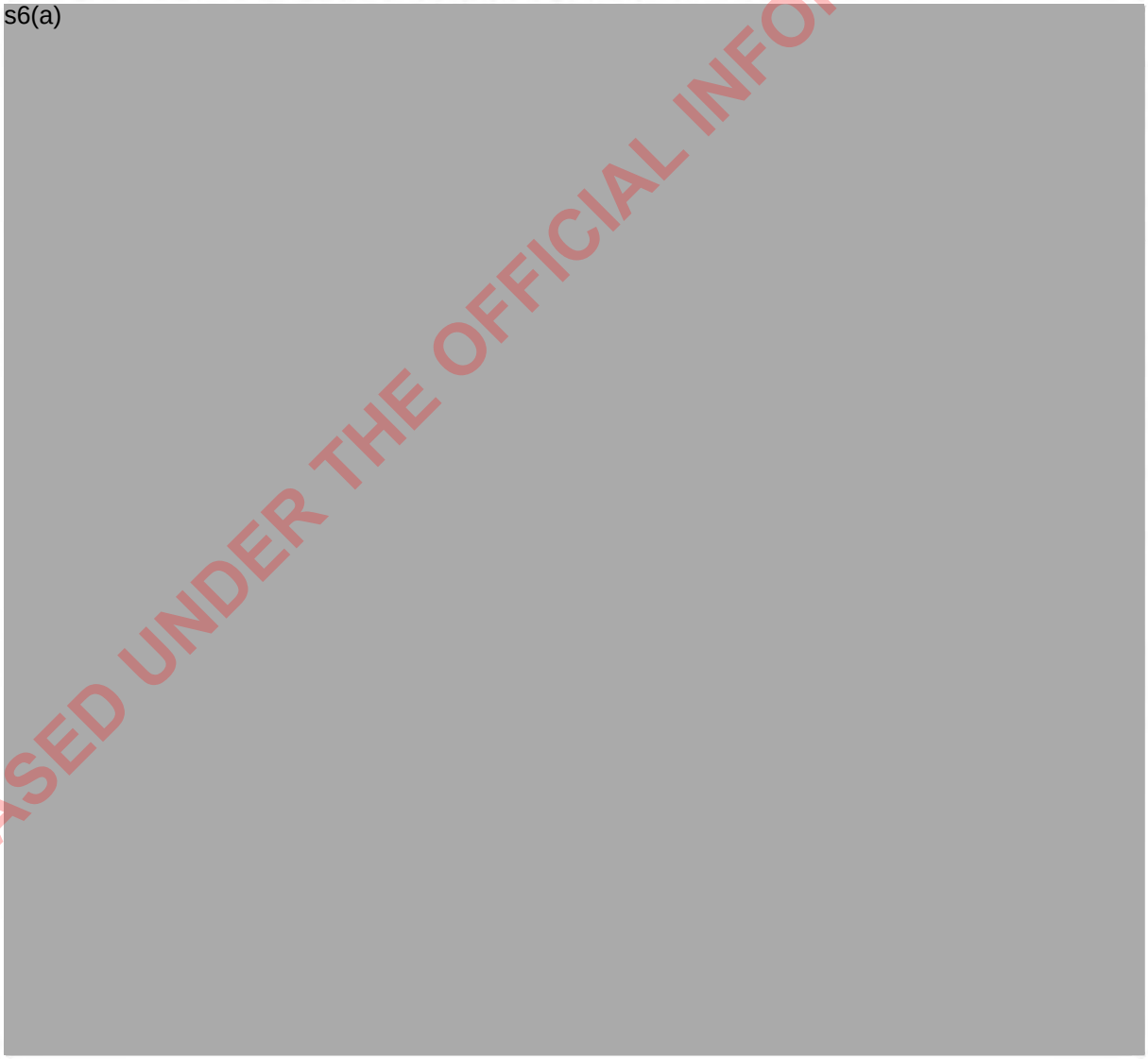
Australia

1. In 2018 Canberra passed a suite of laws to tackle interference. This included an criminalising interference activities that fall short of espionage, and creating a Foreign Interference Transparency Scheme that requires those undertaking a range of activities on behalf of foreign governments to be on a public register.

2. In December 2019, the Australian Prime Minister announced the formation of a Counter Foreign Interference Taskforce. The taskforce is led by ASIA, and includes the federal police, ASD, Austrac (financial intelligence agency) and others. It was accompanied by A$87.8m of funding.

3. In November 2020, Federal Police laid their first criminal charges under the foreign interference laws. Sunny Duong is active in a range of South-East Asian and Chinese-Australian community groups. He has ties to the Liberal Party.

s6(a)



9. No significant state-driven interference was observed in the 2020 General Election. s6(a) s6(a) We have observed concerning relationship building and donation activity across the political spectrum.

s6(a)

12. During lockdown, NZSIS and GCSB moved swiftly to deliver protective security advice to key researchers and organisations in the public and private sectors to help them understand and manage potential risks related to COVID-19 testing, medical research and intellectual property.

Annex: NAB assessments

NAB will separately distribute the following Assessments to support the Australia – New Zealand National Security Dialogue:

s6(a)