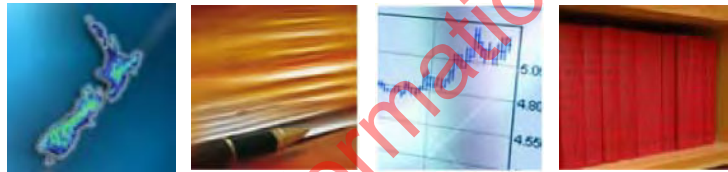


DEPARTMENT
of the PRIME MINISTER
and CABINET



Security & Risk Group



Counter-Terrorism:

*A review of the New Zealand CT
landscape*

May 2013

Released under the Official Information Act 1982

COUNTER-TERRORISM: A REVIEW OF THE NEW ZEALAND CT LANDSCAPE

REPORT TO DPMC/SRG BY SIMON MURDOCH - APRIL 2013

CONTENTS

Introductory Comments	Page 2
Terms of reference	Page 3
Executive Summary and Recommendations	Page 4
Evolution and Key Features of National CT Effort	Page 8
Changing Perceptions and Policy developments	Page 12
Core Functions and outputs of CT community	Page 15
Current State; Views of Officials	Page 17
Outlook and Threat Environment; National and International	Page 21
Elements of a National Strategy and Public Document	Page 26

Released under the Official Information Act 1982

INTRODUCTORY COMMENTS

1. I met with government agencies (and one consultant) over a 14 day period during March/April 2013. The agencies were either members of the standing committee of working level officials on terrorism (WOCOT), within the ODESC system or participants in working groups recently established to develop position papers for the vectors-of-harm framework for national security policies. Two of these six groups have a remit to consider the question of terrorism, and their work has proceeded in parallel to this review. An updated terrorism threat assessment is due in mid-2013, for which work has commenced. The national intelligence priorities approved by Ministers late in 2012 which assign a relative priority to CT collection and analysis were available to me. I was also made aware that there is to be a Law Commission review of the Terrorism Suppression Act (2002) during 2013, and of other legislative initiatives either underway or intended which may impact directly or indirectly on the CT policy context and operational environment.

2. I also examined the public CT strategies of other countries with which New Zealand has particular security and intelligence arrangements, or whose geopolitical interests and size might make them useful benchmarks for comparison of the evolution of policy principles and policy settings.

3. To conduct focussed discussions with agencies, and to remain consistent with my TOR, I put forward the proposition that to permit an accelerated effort against other national security risks in a period of major fiscal constraint, and in light of the emerging consensus of advisers about the terrorism threat outlook, both domestically and internationally, the likely mandate for CT effort across the NZ national security community was towards a 'managed moderation' of that effort. Moderation implies some reduction or consolidation in outputs but managed so as to avoid losing critical effectiveness domestically or good-standing internationally especially with CT partners with whom mutual operational interdependencies exist.

4. I invited agencies to comment on the past evolution, current state and future direction of the national CT effort as they saw it in both their own and cross-agency terms. I have summarised their views and looked for points of commonality in order to pitch the report at the bigger picture level which my TOR implied.

5. In the section of the report dealing with international developments and the international outlook I have ventured into analysis only to suggest the tone which the environment – scan component of a national strategy, especially one likely to be made public, needs to adopt, and the level it should strike. (It has to explain what direction the Government and its advisers think the risk is taking.) The final content should be supplied by NAB/CTAG and others with the relevant expertise and access to current information.

6. The report which follows is my sole responsibility. I was very ably supported by Phil Weir and the DPMC-DESG team, for which I express appreciation.

TERMS OF REFERENCE

7. New Zealand does not have an overarching policy document describing our national approach to counter terrorism (CT). While legislation and the National Counter Terrorism Plan identifies lead agencies and role and responsibilities, in the main, agencies are left to their own judgement with respect to the activities they embark upon with respect to reducing the risk of terrorism. Furthermore the Officials Committee on Domestic and External Security Coordination (ODESC) has very little oversight of agencies individual efforts in implementing CT measures.

Background

8. ODESC at its meeting on 12 October 2012 agreed to the proposition that New Zealand needs a CT strategy. The rationale for developing a CT strategy was essentially that New Zealand needed an over-arching strategy that would guide agencies CT activity domestically and internationally. The need for a strategy now is particularly relevant given: DES Cabinet Committee guidance with respect to the amount of effort agencies are to apply to CT; a change in the terrorist threat level for New Zealand from LOW to VERY LOW; and a paradigm shift since 9/11 from response to risk reduction.

Considerations

9. The CT strategy should address the following considerations:

- the domestic and international threat environment, including the areas where New Zealand is vulnerable;
- government priorities and the National Security System;
- governance arrangements between New Zealand agencies;
- legislative requirements;
- international CT obligations, objectives and efforts;
- de-radicalisation and countering violent extremism;
- building community resilience;
- minimise the harm of any terrorist activity; and
- arrangements for threat and incident response.

Outcome

10. The outcome desired from the CT strategy is a high level document that provides policy guidance to agencies that ensures New Zealand's CT approach is prioritised and therefore calibrated appropriately. Furthermore the document will allow officials to clearly articulate New Zealand's approach to like-minded partners.

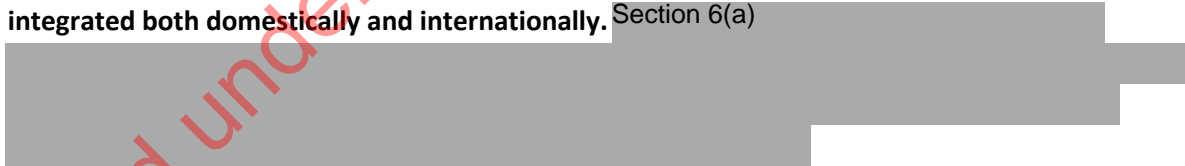
EXECUTIVE SUMMARY AND RECOMMENDATIONS

11. The 2004 National Plan was, in one sense, strategic even if it was not a strategy per se. It carried into force the objectives of the 2002 legislation, establishing the executive framework around which NZ's CT capabilities could be built up so that the then perceived new vulnerabilities in national security could be addressed and new international security obligations could be met.

12. The statement of strategic purpose-not to become a victim of terrorism nor a source of terrorism-related risks to others -came later. It correctly recognised that whilst there are forms of extreme ideological violence perpetrated on New Zealanders by their own fellow citizens that we would categorise as acts of terror, the transnational reach and ambition of the new terrorism post 9/11 was the presenting problem. And since then the two dimensions of homeland protection and "supply chain" risk management have driven our CT threat settings and response architecture. On balance, I think "not a victim; not a source" remains valid as the foundational concept for a national strategy.

13. At the time in 2001-4, failure to invest in and achieve a credible national preventative capability would have left a vacuum. The capability-build had to be expedited. It preceded in part and followed in part the implied principles of the Plan. It was anchored in the generic NZ doctrine for emergency risk management and intentionally based on enhancing interoperability where it already existed between agencies or exploiting sectoral synergies across a wider core of institutional responders. In this respect it also reflected the way in which DPMC's role and the machinery-of-government for national security coordination had evolved. It was consciously modelled, using the 4Rs as cornerstones, on CT response doctrine which key international partners had adopted, and promulgated; this facilitated valuable external linkages which then and now reinforce national capabilities.

14. The CT mission is preventative built upon vigilance and precaution. For homeland protection it relies firstly upon the creation and timely distribution of threat-related knowledge to those with public safety and public protection responsibilities. National data pools (integrating sensitive intelligence with open -source and metadata analysis) and databases have become more integrated both domestically and internationally. Section 6(a)



15. Vigilance over the supply chain to avoid NZ becoming a source of risk to others - the second strategic goal of the CT system- was defined incrementally, and more by practice and international exposure than by being spelled out in the National Plan. Amongst the responsible operational agencies, it is well enough understood that "not a source" means the denial of NZ territory, infrastructure, or commercial markets for operational space, sanctuary, supply or indoctrination for terrorist purposes. The everyday conduct of these denial operations involves both domestic and external interoperability. There are critical dependencies, especially regarding intelligence and information management among and between agencies with regulatory oversight, and core CT agencies. A more detailed mapping of this part of the CT system and a more explicit statement of its priorities (e.g. as regards Australia/NZ) should be undertaken as part of national strategy.

16. CT operational response escalates up a continuum of interventions in which different clusters of agencies play different parts, often interdependently. When vigilance about generic risks turns into response to a crystalizing threat, issues about precaution and proportionateness in the planning and conduct of response operations arise for those with decision rights. Protection of public safety and preservation of civil rights must ultimately be balanced by the law, but in a CT strategy it is appropriate for the government to state its views and articulate the values underlying executive action.

17. NZ's key CT partners and allies are not relaxing their vigilance. Their most recent public statements about the outlook are apprehensive and uncertain, emphasising concerns about the proselytising power and reach into at risk homeland communities of militant Islamist extremist ideology and the regional spread and penetration of extremist (mostly Sunni) networks into marginalised groups or ungoverned spaces in weak and conflict prone states. Their policy settings, for some time now, have been rebalancing-moving beyond effect-minimisation and military suppression to environment- shaping interventions, on the one hand, to address radicalisation factors in at-risk domestic communities, and on the other to deepen institutional resilience in failing states. In both cases CT objectives are being "normalised"-grafted onto longer-standing and broader development policy frameworks for social equity and human security. This shift towards mainstreaming which treats CVE-incubation holistically is consistent with the UN strategy.

18. Unlike other likeminded CT partners, NZ has not so far been forced by events, to review its overall policy settings or capability mix. Were we to do so, in order to remain consistent with these international shifts, it would be at the margins. We could look to graft some CT/CVE objectives onto the existing domestic programmes which are targeted at the general wellbeing and welfare of at risk groups or at risk communities. There are sensitivities about counter-radicalisation, and it would require some careful policy design between the national security agencies with principal responsibilities for public protection and threat management, and those other agencies with "soft intervention" mandates, particularly for resettlement and youth-at-risk.

19. Section 6(a)

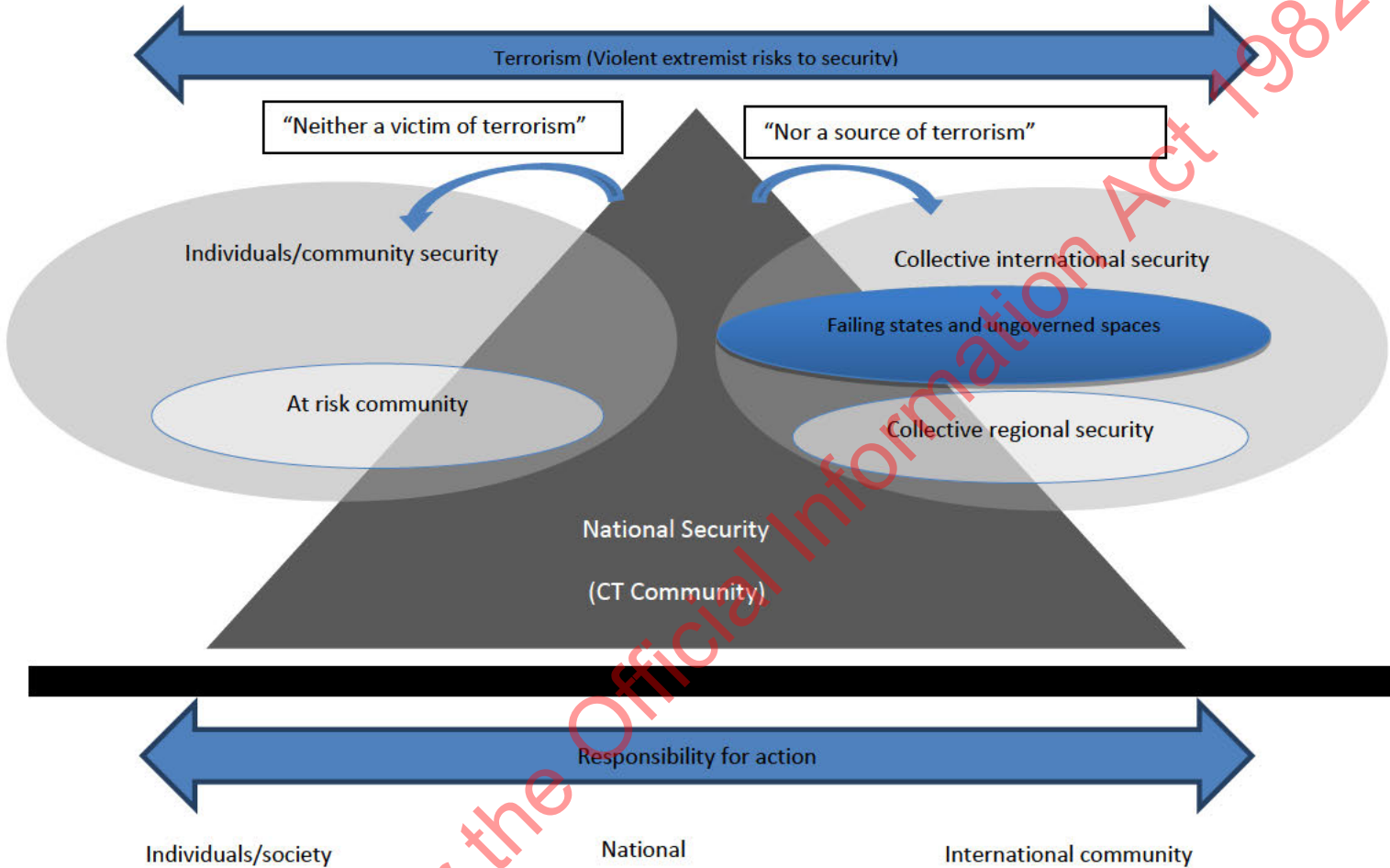
A cross agency stock-take of commitments and demands of off-shore CT activities is needed and from this should come a consolidated approach to international engagement.

20. In neither case, given budget restrictions, would there be scope for step-increases in levels of activity. Rather it would be a matter of refining and refocusing of current outputs. Section 6(a)

21. Such a widening of our national CT goals would take the National Plan somewhat away from its present framework of four "Rs" towards a fifth- "Resilience" (domestic and regional), as depicted in the following diagram;

Strategic framework for post 2013 National CT response mission

Motivation (radicalization) → Intent → means → actors → effects → impacts



22. It is hard to see how or where fiscal savings might be found in the aggregate national CT capability, or capex might be deliberately reduced to reflect the current NZ homeland threat level. It is not the same sort of exercise as, say, a Defence Review. There is clearly some greater scope to moderate CT operational tempo per se, but there are constraints on that arising from the multifunctional character of the CT apparatus which, as in the case of border security, services a range of inter-related risks. Section 6(a)

In a holding pattern, where the capital and operating budgets of CT agencies are declining in real terms, the immediate risk is of unintended impacts on the CT whole from unilateral decisions within participating agencies to cut or re-spread their own spending.

23. CT system architecture is based on the statutory roles of NZP and NZSIS, and, around them, five clusters of agencies with operational synergies. DPMC provides coordination for whole-of-system requirements through WOCOT. There appears to be reasonable clarity amongst agencies within the CT system about day-to-day operational command and control. The sector

clusters seem to have taken benefit from exposure to each other through RWC and CT exercises and should prove robust (i.e. ` bend but not break`) in a real terrorist incident/emergency when the TEG is activated.

24. That said, the foregoing propositions about future CT goal setting; policy priorities; fiscal restraint and capability risk are matters of strategic direction and system coherence which are best addressed in a centre-led governance process, not in the clusters.

25. DPMC should utilise SOCOT for this purpose, and to draw together the National Security Vectors of Harm (VOH) exercise; the updated all-sources terrorism threat assessment and matters relevant to future CT operational performance arising from recent or current law changes. The content of a national CT strategy, along the lines proposed in this report, is dependent on these separately commissioned streams of work

Released under the Official Information Act 1982

EVOLUTION AND KEY FEATURES OF THE NATIONAL CT EFFORT

Evolution

26. In the period 2001-2004, following the series of attacks, or planned attacks against “Western” targets and unprotected populations by AQ expeditionary units in the northern hemisphere and JI in East Asia, New Zealand rapidly upgraded its CT capability and effort. Out of this came a new legal framework¹, a new plan for response to a like threat to our homeland; changes to the machinery of central government both in capabilities and practices; and a new focus on offshore collective security collaborations with a mix of familiar and new security partners

27. To enforce the law and take other steps to combat the challenges of the “new terrorism” national governments across the world were finding their ways to a new policy mix, in some aspects traditional, in others new, on two distinct levels. Firstly, a predominantly American military campaign, which later became the “NATO-plus” mission, was launched, with UN backing, in Afghanistan against AQ and the Taleban. It had the concrete objectives and defined endpoints of conventional war. NZ’s contributions are well known.

28. Secondly the challenges were seen to require adaptations to the existing doctrine and practice for counterterrorism. There emerged, firstly amongst Western nations, and then more widely, a more highly integrated and internationalised strategy incorporating politico-legal, military, police and border-control assets, as well as intelligence and diplomatic tools. It implicitly acknowledged that CT was a more protracted process than a war- not just against a defined aggressor in a specific locale but against a dangerous activity with domestic and trans-boundary dimensions, which might not be capable of being defeated or eliminated, but could potentially be contained to tolerable levels. Success would be defined in terms of both lowering the probability of further surprise attacks, and reducing their adverse consequences. This is the conceptual basis of the NZ National Plan of 2004.

KEY FEATURES

29. When the National Plan was first developed it was consistent with best international thinking and practice, especially amongst NZ’s closest security and intelligence partners [REDACTED]

¹ The 1987 Terrorist Emergency Powers Act had granted the NZ Police access to extraordinary powers to preserve life or prosperity in responding to a terrorist emergency in NZ, which could be deemed to be international in character- ie-perpetrated for the purpose of pursuing political aims outside NZ. (Aircraft hijacking and passenger hostage-taking were prevalent techniques of what some commentators call the “old terrorism”). The characteristics of a terrorist incident were otherwise defined in the Crimes Act- activities endangering the public welfare, persons or property. The 2002 Terrorism Suppression Act was, as its title suggests, a broader consideration of the phenomenon, significantly influenced by the emergence of a degree of international consensus about the ‘new terrorism’ as a threat to international peace and stability in the form of UN Conventions and Security Council or UNGA Resolutions. TSA 2002 allowed for a wider range of measures to be taken by agencies other than the Police to prevent attacks in NZ and in support of collective international or regional security. TSA 2002 took a definitional path similar to that taken in other Western/Commonwealth jurisdictions. It created specific offences for financing and for harbouring, but otherwise it treated acts of terrorism as crimes of serious violence whose gravity would be established by their intent, and the breadth of their intended effects and impacts, not by the idea or cause or ideology of the perpetrator. Justice would be delivered under civil not military codes.

Section 6(a)

Characterisation of the threat was conditioned by the 9/11 experience of the expeditionary surprise attack launched by a clandestine force from abroad which had infiltrated the host state defeating its border protection and homeland security apparatus. The main intent was therefore to raise the bar on homeland security (and then harmonise our protective measures with others). Risk management principles were the conceptual foundation; the Plan was built around a risk continuum escalating through latent (uncrystallised) risk, to emerging (crystallising) to concrete, identified (crystallised) and imminent threat, and on to an incident and the response to it.

30. The National Plan, as first articulated in 2004, (not since amended) has remained the principal policy statement about terrorism and our national policy settings. The Plan provided a high level framework around which national capability could be built and from which command and control for tactical response could be derived. It placed considerable emphasis on anticipatory actions, guided by intelligence and based on monitoring actual or potential threats, to forestall adverse outcomes from a terrorist incident. It implicitly recognised that the measure of success for CT would be intentions thwarted and harm avoided-i.e. `non-events`. Agencies with capabilities and powers to intervene would seek to render would-be attacks less effective, and to harden the targets which terrorists might aspire to attack. It aligned CT incident response with wider national disaster and civil emergency response doctrine. It was to be supported by annual reviews of risk setting and alert levels.

31. The National Plan condensed these goals into four overarching sectors of executive action-the "4 Rs"

- threat Reduction measures (domestic/offshore) and preventative interventions;
- public security enhancements and other response Readiness improvements;
- CT incident Response doctrine to better avoid damage and limit escalation;
- Consequence management to promote Recovery from the effects of an incident.

32. The Plan tended to focus on the later phases of the response continuum, and was more specific about the onshore dimension of policy than the offshore, and the interplay between homeland security ("not a victim") and what might be called "forward defence" or collective threat reduction. However, by 2006/7 the latter dimension had become more central to the policy mix; the risks of NZ being used as a facilitator of terrorist-related risks to others ("not a source") received increasing emphasis in official reports and assessments. Connectivity and interoperability with foreign partners deepened particularly in areas relating to the global threat actor who might not see NZ as a target for attack, but could seek to use it as part of a "supply chain"- as an originator or intermediate destination for the delivery of goods, services (including financial), human data (e.g. identity-related information) or communications contributing to sustainment of terrorist capability.

33. There have been a variety of articulations of NZ's overall approach to the conduct of CT policy in NZ and internationally, in departmental accountability documents, and in Ministerial statements. Tracing a path through them with reference back to the foundational elements- the legislation, National Plan (the 4Rs) and the goal- setting implicit in "not a victim/ not a source" –

and taking account of views given to me by current officials- five underlying principles emerge which can be thought of as the strategic precepts of evolving NZ response policy.

- NZ aspires to a CT regime closely aligned to the emerging body of international law and practice established by UN resolutions, and compliant with its obligations
- Acts of terrorism will be treated as criminal offences of serious violence , not acts of war against the nation state, and will be subject to legal due process under civil codes
- Powers available to the state to act against the new terrorism will be exercised proportionately and with full accountability.
- NZ would be outward-looking ; its CT plans and programmes would be consistent with broader international relations policies and consciously set to optimise cross-border collaborations with likeminded jurisdictions
- The conceptual framework for executive actions in operationalizing counterterrorism policies will align with national emergency response management and will employ risk management principles.

PURPOSE AND BREADTH OF STRATEGY

34. This confirms the view that there has not been a strategic policy vacuum around CT, so much as a de facto strategic approach for which there is no single unifying statement (either classified or public) of strategic intent. If validated politically, these precepts would form the frontpiece for such a statement. And, it would proceed to draw down from them to the “threat-scape”-i.e. problem definition and risk settings- from which the National Plan derives its parameters and its coherence. If there has been a gap, it is one between political strategic intent and the operational environment-sometimes called the “interventions logic” – linking what the government wants to accomplish and why, with how. Other national strategies seek to establish this synthesis, and some also directly address another political issue- the balance in policy values which the precautionary bias of CT response doctrine can pose for constitutional freedoms in open societies².

CHARACTERISING TERRORIST ACTS

35. In other jurisdictions, particularly those in Europe bound into a common EU doctrine³, events themselves have forced review and revision of what a terrorist act is, and what ought to

² For example, the Dutch Strategy discusses some tests of public good, or values which it sees as having to be balanced in CT policy decision making and delivery;

- Legitimacy - the need to establish public consent for and cross- community understanding about CT interventions through communicating effectively;
- the need for proportionality in determining the way in which the protective function by means of coercive or intrusive state powers ought to be exercised from case to case.
- equity in terms of sensitivity to the ripple effects of identifying (“labelling”) an individual, group or organisation as a terrorist suspect

³ Although the Netherlands is not NZ, and has unique historical aspects to its social makeup, the Dutch strategy (2011?) connects its strategic intent and CT intervention logic by means of to an “applied” or “working” definition, extrapolated from the statutory definition, to which all agencies subscribe. The Dutch working definition sets out ,as weighted criteria the threshold elements of a decision to classify a risk as a terrorist risk. The baseline determinant is the threat of serious violence based on ideological motives. Violence is serious if it is life-threatening, or could cause property damage disruptive to society as a whole. Motives are ideological if their aim is to instil fear among (large sections of) the population, and/or to affect

be the aims of CT strategy and characteristics of counterterrorism operational policy. That has not (so far) been the case in NZ. Nor, notwithstanding two high profile cases, have the same definitional issues, and the associated questions of enforceability had the degree of testing in our courts which has been the case elsewhere (including Australia). It has largely been possible for agencies to rely on the statutory definition, and carry that forward in departmental interpretation of policy, or cross-agency frameworks. Most recently the NZ National Security Framework (2012) characterises terrorism as political extremism or violent extremism, a vector of harm to wellbeing, in the same category of risk-bearing activities as “insurgency, paramilitary activities and civil unrest”. Counter-terrorism goals are expressed as:

- preventing activities aimed at undermining or overthrowing government institutions, principles and values that underpin NZ society;
- contributing to a rules-based international system;
- protecting lines of communication, and
- engaging in targeted interventions offshore to protect NZ interests

political decision-making. The specific ideas motivating a particular individual group or organisation are irrelevant.

CHANGING PERCEPTIONS ABOUT TERRORISM AND POLICY DEVELOPMENTS

36. From the analysis of evidence from investigations and other post 9/11 commentary, some of the complexities of the subject began to be acknowledged, and in policymaking amongst NZ's key partners there have been shifts of strategic emphasis from effects and consequence management towards environmental factors, sources and influences. This is explained in their public strategy documents, and it is the context in which they make their current trends and future directions judgements (see Section 7). The processes of strategic re-contextualisation and reassessment are extensive, and continuous, but four principal areas of focus can be highlighted;

- (i) The place of jihadist expeditionary terrorism in the context of sectarian and doctrinal tensions within global Islam. Governments became concerned to avoid CT response strategies which failed to distinguish between fundamentalism, militancy and extremism, and which treated extremism as a symptom of a cross cultural "clash of civilisations". NZ took a leading role (via MFAT) in programmes, including interfaith dialogue, to counteract this perception.
- (ii) The wider question of what in fact was so unique about the "new terrorism" (other than its shock tactics), when viewed through a wider historical lens of post-colonial political development and nation-building in emergent states. Governments found themselves reminded that extremist violence using terror tactics was not that new. It had occurred and was occurring in a wide variety of geographic theatres within established states and in failed or forming states with "ungoverned spaces". Frameworks for CT risk –sourcing needed to remain broad enough to capture diversity of geopolitical environments and conditioning factors-e.g.

- violent intra-communal conflict within domestic borders⁴;
- indigenous ideological/political extremism, including "inspired" jihad
- Randomised, localised, individual acts of extreme ideological violence ("lone wolf")
- cross border and trans regional sectarian conflicts;
- cross border ethnic nationalist extremism/ political separatism
- global non-state expeditionary (including jihadist)
- state- enabled ("proxy") extremism

NZ security service and police policy settings had recognised "politically motivated violence" (PMV) before 9/11 and its transnational character. CT risk frameworks, including those employed by CTAG, remained broad.

⁴ The current NZ threatscape is seen as also comprising risks of nonreligious violent extremism , and potential terrorist acts ,arising from environmental causes ;ethno-cultural separatism ("Maori sovereignty") or other grievances about government policies e.g. affecting the economy/migration. This review did not seek to address those matters in depth.

As regards global jihadist expeditionary terrorism, its paradigm was warfare. It was seen as inherently less transactional in that it did not seek particular concessions to its cause or status from an enemy/ victim state, so much as to alter the fundamentals- i.e. established power structures and accepted socio-political norms. In the case of AQ, its "brand" was an end in itself. The intended outcome of its activities was consciously catalytic, to resonate with a variety of sectarian and intra-communal grievances felt across the developing world, as well as in the Muslim diaspora across the developed world (particularly Western Europe) and transferable between the two. Networked to other Sunni groups (and "franchised") it appeared able to connect its core sectarian message about justifiable violence in defence of the true religion with other more political causes and issues, some with a nationalist, anti-colonialist or anti-American provenance, but others incubated in purely domestic conditions.

- (iii) Multilateral doctrine also developing in parallel, placed increasing emphasis on intergovernmental steps to counter violent extremism ("CVE " not CT) particularly in failed or fragile states. This was expressed in the 2006 UN Global Counterterrorism Strategy and the work the new Global Counterterrorism Forum in which NZ, as a founder member, undertakes regional coordination on rule-of-law matters. Other intergovernmental initiatives some stemming from the CT-related work of UN technical bodies or the specialised agencies (e.g. UNDOC-the UN Office of Drugs and Crime), or others such as the Proliferation Security Initiative have high level statements of purpose and intent to which NZ has subscribed. The effect of these commitments and obligations on the national CT doctrine has been considerable and, in practice, they are a distinct strategic driver of the national policy.
- (iv) It had been recognised that beyond its ideological motivations home-grown/home based extremist/terrorist violence was associated with long run socioeconomic trends arising from changes in patterns of human mobility. With globalised labour markets came diaspora effects and, in OECD countries, where big minority ethnic or ethno-religious enclaves had formed, issues of community development, identity and social attachment. CT strategies were revised to better address the potential for threats to incubate in immigrant; guest -worker and refugee (i.e. 'foreign born') communities, arising from indoctrination, radicalisation of, and recruitment from second-generation young people, especially Islamist sympathisers

37. In Europe the diagnostic broadened further, with controversy about the failure of social development policy generally, and especially multiculturalism, to create social inclusiveness and civic responsibility. (The Brevik massacre showed how polarised this debate had become). Australia too found itself facing this manifestation of the threat quite soon after the Bali bombings. In 2010 the Australian White Paper recorded that 35 of 38 prosecutions had taken place for terrorist -related offences under the Australian Criminal code, and more than 40 Australians had had passports revoked or applications declined for reasons related to terrorism. The revised Australian strategy directly addresses the interplay of socio-cultural

“incubator” forces in at-risk domestic communities, and prioritises de-radicalisation/CVE and resilience-building⁵.

38. In practice NZ has registered this shift. Operationally the relevant CT agencies pay attention to “home-grown/home-based” risk, and it is incorporated in threat assessments as latent, if, as yet, not material threat. But it has not, as yet, been articulated beyond individual agency plans, nor reflected in the settings of the NZ National Plan where it could be captured in refinement to the “4Rs” (a fifth “R” - Resilience?), and perhaps some broadening of the scope of “not a victim/not a source” to acknowledge CVE (indoctrination, incubation and radicalisation) as a CT priority. Before that, however, a scoping process to establish a broadly based CVE policy would be useful.

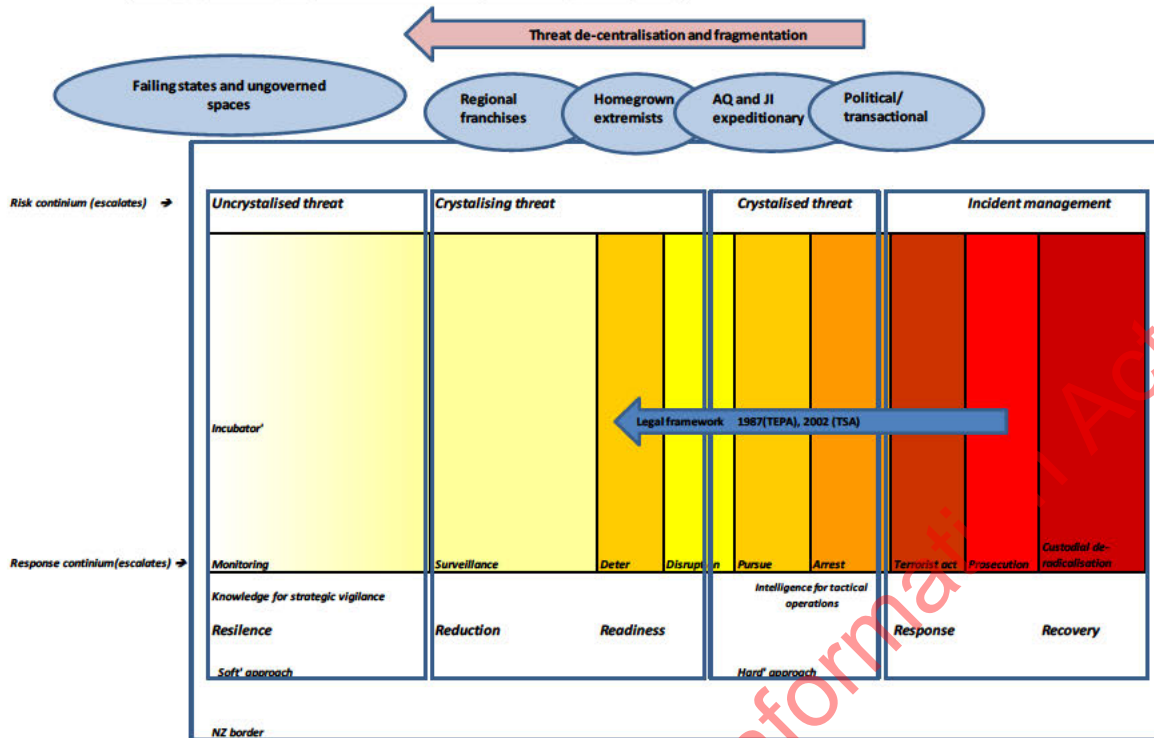
39. I had suggested to me some new arrangements for CVE awareness and vigilance with the lead role taken not by national security agencies but by those, central and local⁶, with socio-cultural mandates already engaged with at-risk communities, whether for settlement; integration; crime prevention or post custodial reduction of reoffending. Their “soft” interventions could serve to increase awareness of radicalisation risk, and preserve understanding and consent for “harder” CT interventions if risk turns to threat.

40. The following diagram seeks to depict the evolutionary development of the NZ system as it stands today and to relate it to the principal expressions of policy intent and operational coherence-the law, the 4Rs and “not a victim, not a source”. It seeks to show the intervention logic for the CT effort -its functions and outputs as it progresses along a risk-escalation continuum from the unknown risk to the known threat, and its relationship to changing perceptions about threat.

⁵ The Australian Strategy has four core policy elements-Analysis, Protection, Response, and Resilience, which is described as “building a strong and resilient Australian community to resist the development of any form of violent extremism and terrorism on the home front “

⁶ I spoke with the Office of Ethnic Affairs, and more broadly with DIA whose mandate encompasses CT – related matters in this and other respects, and whose involvement in WOCOT could be wider than conceived, particularly through its roles in E-government; community relations and local government .

Strategic framework for post 2013 National CT response - Policy and Capability



CORE FUNCTIONS AND OUTPUTS OF CT COMMUNITY

41. From the feedback given to me by individual agencies I constructed an overall map of the NZ system as it has developed. The NZ CT interagency community has, today, the capacity, and the capability, using lead and support agencies, to carry out the CT mission broken out into functions and outputs as follows:

(i) Risk Awareness /Vigilance (Uncrystallised Threat)

- horizon-scanning for threat indicators based on partner data (CTAG and others)
- interrogation of well-maintained databases, designations and profiling applications
- Section 9(2)(g)(i)
- passive collection of open source or windfall information (NZP/NIC and NZSIS)
- knowledge management – consolidation/integration/analysis/distribution (CTAG)
- BAU/ incidental target-hardening e.g. critical infrastructure upgrades-computer & physical security improvements at airports; (NZSIS/GCSB ; regulatory agencies e.g. MOT; consular /safe travel-MFAT)
- regular exercising; offshore; national programme-Lawman series; and subnational (DPMC).

(ii) Risk Recognition/ Threat Identification (Crystalising Threat-early stage)

- frontline border security (led by ITOC⁷ and the border agencies)
- identity protection/document security (DIA)
- targeted (active) intelligence collection (NZSIS/NZP-Special Investigation Groups)
- surveillance (passive/opportunistic/overt/not under warrant) ?
- information integration/knowledge management (CTAG)

(iii) Risk Reduction / Threat Pre-emption (Crystalising Threat-later stage)

- targeted and intensifying (warranted/ covert) surveillance (NZSIS/NZP/ITOC)- joint tactical intelligence gathering and tactical planning (DPMC-SRG/WOCOT)
- active measures-deterrence options (overt/covert)-NZSIS/NZP
- active measures- disruption options (physical/virtual)-NZSIS/NZP
- active measures-confrontation (detain/deport/interdict/arrest NZSIS/NZP/ITOC
- warn-outs, alerting/specific target-hardening (DPMC/SRG/WOCOT/CDEM/MFAT)

(iv) Incident Response (Crystallised-i.e.-Unpreempted- Threat)

- joint intelligence and joint planning (DPMC-TEG)
- general public alerts /specific warn-outs (TEG)
- pursue/arrest (NZP)
- stabilise-contain, confine, cordon, negotiate (TEG/NZP)
- overcome (TEG/NZP/NZDF)
- triage/ damage assessment/de-escalate (TEG/CDEM)

(v) Incident Recovery

- joint planning (TEG/CDEM)
- prosecute/convict/sentence
- custodial/parole (de-radicalisation?)

⁷ Border Agencies – Including Immigration New Zealand (MBIE); Customs; MAF; Police. It is noted that a number of agencies have a direct and indirect role to play in this space.

CURRENT STATE; VIEWS OF OFFICIALS

42. I did not undertake any detailed audit of this system from a fitness perspective. I asked officials to describe their systemic responsibilities and to identify any areas of high value/high sensitivity where they believed weaknesses (gaps ,overlaps, redundancies)might exist or might become exposed either by “wartime” pressures (the impacts of a major terrorist emergency) or “peacetime” needs, such as those which could arise from competing expenditure and resourcing priorities on departmental votes. This exposed some areas of potential (not acute) concern, but none which officials considered could not be remedied .

Information compartmentalisation

43. The most frequently voiced concern was about knowledge needs and information compartmentalisation. The importance of high quality intelligence and well-designed knowledge management practices for effective CT operational performance is common to all CT strategic frameworks, and in some national strategies it is a major point of focus (Australia`s strategy makes `Analysis`- “an intelligence-led response, driven by a properly connected and properly informed national security community”- one of its four key elements). In terms of the NZ CT system there could hardly be a higher priority for risk awareness and risk assurance than the effectiveness of information collection, analysis and reticulation.

44. Besides inviting them to comment on the core principles of CT strategy, I asked officials to consider whether the 4Rs themselves were still sound foundations for executive CT policy going forward , or where there might need to be room made for new or amended priorities

45. Officials had a variety of other reflections about the issues which a strategic review should consider, some of which concerned the broad issues of the risk aversion settings and proportionality-how to strike the balance in ramping up response machinery between excessive precaution, and perceived over-reaction.

Articulating the public good and CT value proposition

46. Section 6(a), Section 9(2)(g)(i)

a growing awareness that the public rationale for counter-terrorism may need to be updated and rearticulated at a levels of both legal principle and strategic purpose, including checks and balances on executive power.

47. Similarly there was some concern that the CT risk tolerances, upon which to rest a level of investment in public protection and terrorist response capability, had not been sufficiently articulated as they are for other kinds of disaster. It was put to me that probability (frequency) is not the measure; the essential nature of terrorist risk - that it is very dynamic; it escalates very sharply; and it has wide-ranging consequences with non-material costs- makes that kind of

quantification problematic . The point felt to be in need of political articulation (in a public strategy document) is the Governments view of the protective duty of the state, and the extent to which, when faced with an apparent crystallising threat, CT response agencies, driven by worst-case scenarios, are expected to default to a precautionary stance, in terms of the exercise of intrusive or coercive powers.

48. I also encountered a view that there has been a decline in NZ public apprehension about terrorism, and a corresponding rise in public distaste for the safety compliance regime, and other more invasive aspects of CT preventative measures. The demands of operational security; protection of intelligence sources, and the inherent preventative nature of CT success combine to limit the public understanding, and contribute to a perception of inflated threat and excess capacity .

Fit for purpose? Assessments of capability and credibility

49. Whilst raising these kinds of questions, officials largely concurred that given the ongoing risks still being posed by the “dangerous activity” in aggregate to national , regional ,and global security, as they saw them (see Section 8) the range of legal vehicles and of lawful interventions available to NZ agencies to carry out the government’s CT policies effectively, and to meet international treaty standards were not excessive, notwithstanding the present very low threat level for the NZ homeland.

50. The NZ CT system is highly integrated, multifunctional and quite deeply internationalised. Officials emphasised that the capabilities enabling homeland protection (“not a victim”) are, in large part, the same ones that enable NZ to avoid becoming a source of terrorism risk to others. Commercial globalisation and regulatory openness created highly efficient international supply chains which are as accessible for criminal as for legitimate purposes.

51. The CT supply chain can be seen as covering the movements of people; goods (particularly proscribed materials e.g. WMD); services (financial; ICT; transport; business establishment and other commercial manifestations); and intellectual property (e.g. internet content). The human border covers all categories of inward movement (from tourists to refugees and others seeking permanent residence), and is closely associated with the protection of national identity documentation from theft, fraud or other illegal manipulations. “Supply chain” vigilance, as it has evolved, is built around well-integrated border security /law enforcement apparatus with high interoperability externally to key partners.

52. In some cases CT capability elements are virtual not actual- they are embedded in the core business and BAU outputs of agencies and are not budgeted directly. If those outputs have to be held or shrunk for fiscal reasons, the impact on CT may not always be immediately apparent.

53. In the past two decades, not just for CT reasons, a generic internationalisation process has occurred across government, but in regard to national security it has been galvanised particularly by the terrorism problem. The practices for exchanging foreign intelligence are now as well - developed for border and document security as for foreign relations, military and counterespionage purposes. The integrated border operation through ITOC, is driven by agreed international standards and practices for goods, under Customs (ICU) and passengers (under ICAO)

alike, as well as by data-sharing arrangements which are required for a variety of security purposes, including identity protection. MFAT has similarly strengthened both its organisational and public (safe travel) protection regimes, and deepened its consular response linkages with core partners. This brings with it benefits of scale and critical mass but at times a range of costs, in terms of equipment and manpower, which are not easily managed for smaller countries, and requires a degree of discrimination as to the areas of critical interest and degrees of interoperability. It would be easy to become "spread too thin".

54. It was noted that contemporary security threats are often a product of global organised crime and vice versa. Multilateral law enforcement (e.g. via Interpol and UNDOC) has expanded, and policing assistance and justice sector institution –building programmes are a prominent part of bilateral ODA programmes for many OECD members, NZ included.

55. Officials judged that NZ was now in good standing internationally as a result of the building of an overall national CT system which complied in practice, not just on paper, with changing international standards such as terrorist designations; in core response capability and in specialised areas e.g. money-laundering. It was noted that, if anything, the international enforcement issues are becoming more complex. Definitional uniformity does not exist internationally, and can cause cross-jurisdictional problems for those engaged in multilateral mutual support and enforcement processes, especially where the foreign jurisdiction operates to different legal codes and standards.

Readiness

56. Officials considered the CT response capability to be well-practiced overall, but were sensible that a real CT emergency of significant complexity or scale would inevitably find gaps and create strains. Well -designed exercises, complemented by exposure to partner (especially Australian) practice and some real-time international event management deployments (notably during RWC) have tested readiness and flexibility.

57. When the National CT Plan was adopted it sat within a system, which placed a high premium on planned response for operational robustness. CT, built around the "4Rs, had to be able to move onto a tactical/deployed footing at very short notice, and if necessary into full crisis mode, with no less efficiency than for other national emergencies under CDEM.

Structures and governance

58. The underlying machinery-of-government for national security was itself geared towards situational coordination more than system governance. (The National Security Framework; the Intelligence Coordination process and accountability/ oversight arrangements through ODESC have since introduced changes which strengthen governance.) This may help explain why the CT system coming from the 2004 Plan emerged structurally as it did. It has developed as an amalgamation of five principal interagency clusters in the modern NZ national security community;

- the (contemporary) intelligence community
- an international security relations and security diplomacy group
- the border management/transport/Identity security group

- the law enforcement agencies group
- the emergency/disaster management (CDEM) community
- A community awareness and resilience group?

59. There is no centralised budget across these groups for the CT effort as a whole. There are coordination and cooperation mechanisms within, and to an extent, between the clusters. Oversight and governance via ODESC is largely focussed on aspects of readiness (exercising) and planning for situational interoperability for major events (e.g. RWC). The predominant medium for coordination is via WOCOT; there is no comparable senior level activity (SOCOT exists but has rarely met). To the extent there is overall CT leadership it is exercised largely by NZP and NZSIS, by virtue of their designated statutory roles. They are members of all 5 clusters.

60. This architecture is strong operationally-practice influences policy; innovation occurs (eg border security harmonisation); and multi-functionality can be developed through the tradecraft commonalities amongst the clustered functions. No official with whom I spoke wanted to create layers of structure or new tiers of process for its own sake, and some were actively concerned that this review could introduce more governance at the cost of loss of flexibility ; distancing of senior practitioner managers; and treating as “pure” policy what really needs to be applied policy.

61. At the same time there are potential problems ahead for the system if ,as a result of a combination of budget restraints on the one hand and rising pressures to contribute to collective security coming from international peer group partners on the other, it becomes stretched from both ends. This is not so much a problem for cluster leadership as it is for system governance-i.e.-it needs to be seen holistically and addressed comprehensively. The appropriate vehicle for this is a WOCOT –led stock-take, coordinated by DPMC-SRG, based on a careful mapping of cluster capabilities and interdependencies, both domestic and with foreign partners.

OUTLOOK AND THREAT ENVIRONMENT; NATIONAL/INTERNATIONAL

NZ – ‘not a victim’

62. In respect of the risks of becoming a victim, the annual (formal) assessments have tracked downwards. The present judgement⁸ of NZ officials is that the homeland threat is low-a relatively benign environment. The potential for expeditionary attacks of the kind mounted by AQ or similar networks in the years after 9/11 appears to have been reduced by a combination of the preventative and disruptive efforts of western and other CT partner states with whom NZ collaborates. The risk of NZ offshore interests being directly targeted by terrorists or violent extremists is seen to have receded, with the exception of NZDF or other uniformed presence deployed in theatres of regional conflict. NZ expatriates or travellers are not seen as being at direct risk so much as incidental risk from being “in the wrong country ‘in the wrong location at the wrong time’, but not more so from terrorist or extremist violence than from other forms of civil disorder or criminal violence. The exception in this category is the proto-extremist whose destination is deliberately chosen.

NZ ‘not a source’

63. Although individual agencies actively review risks and risk assurance, there has been no similar formal cross-agency assessment of NZ’s threat status in terms of avoiding becoming a source of latent or actual risks of terrorist or other violent extremist attack on other countries. But the view of the border security and identity security officials I spoke with, as well as NZSIS, was that supply chain vigilance is well –institutionalised, and mature in terms of established interagency practices. Section 6(a)

The countries of the Southwest Pacific for which NZ has particular security and developmental obligations have received support for enhancing their border and supply chain security. NZ has also collaborated selectively with ASEAN countries for similar purposes.

Risks from radicalisation

64. In the “not a source “ context one concern voiced by officials was radicalisation. Section 9(2)(g)(i)

⁸ NZ’s terrorism risk is assessed as a vector-of-harm to national security, calculated by scale through an impact/consequences/probability matrix. In the 2013 assessment, at one end a successful lethal terrorist attack inside our borders would have very adverse impacts, as would a bioterrorism attack which did not cause direct human damage. Both are considered much less imminent (highly unlikely) compared with the almost certain status of more damaging cyber incursions. This section draws on that 2013 assessment. A specific CT assessment is in progress.

Section 9(2)(g)(i)

65. Section 6(a)

To contain and reduce radicalisation risk by early “soft-power” interventions without the use of intrusive or coercive law enforcement powers was seen as emerging international best practice with which, in a measured way, NZ should be associated.

INTERNATIONAL

66. This section draws upon material gleaned from selective, and necessarily partial access to recent CTAG/NAB/DESG –generated material; from conversation with a limited cross-section of agency managers; and from public CT related information from likeminded overseas partners or foreign academic commentaries. A comprehensive (i.e. “all sources”) and high level overview linking international, regional, and national assessments was not available to me (but may emerge from the VOH working group process and the 2013 threat assessment process now under way). What follows are “place-holder” observations about the strategic environment, and strategic trends, necessary in order for this review to achieve completeness ,but it does not pretend to be as in depth or professional a product as that which the NZ CT community can-and should - at intervals- generate

Partner perspectives on global trends

67. There is a sense that this is a particularly difficult point in time to make good strategic judgements about the trajectory of the “new terrorism “. That is because, as USDNI Clapper told the US Congress (12 March 2013), “terrorist threats are in a transition period, as the global jihadist movement becomes increasingly decentralised, and the Arab Spring has created new instabilities, and internal security forces lose their old ascendancy “. Gen. Clapper noted that the degree to which states can protect access to WMD technology may also be weakening. He said there was ‘some evidence’ that there are flow-on effects from the global recession into OECD flows of aid and investment into least developed countries, particularly those already prone to ,or weakened institutionally by other human security threats and natural resource shocks . In fragile or failing states the justice, law enforcement and border security capability erodes exponentially- and ‘ungoverned spaces’ expand.

Section 6(a)

68. The UK Foreign Secretary, outlining UK policy settings in a recent address (to RUSI-15 March), also dwelt on the changing nature of threat. He said it was geographically more diverse; more fragmented because more groups were active and not operating to the same agendas; increasingly closely tied to exploitation of local or regional issues; more opportunistic/pragmatic operationally- "seeking out new areas where terrorists have the greatest freedom to plan external attacks because local defences are weakest". Mr Hague saw global CT strategy as a "long intergenerational campaign" and he said that it was unwinnable militarily. ("Unless our foreign policy addresses the circumstances in which terrorism thrives overseas we will always fight a rear-guard action against it".) From this he went on to give five key points of adaptation of UK external strategy and policy mix.¹⁰

UN global strategy

69. These views are closely matched to the UN Strategy which emphasises integration of CT policies for denial of freedom of operation, movement, supply or sanctuary- but links these goals to wider intergovernmental CVE programmes to address terrorism 'enablers', such as conflict and instability (creates ungoverned spaces and state fragility); technology; ideology (uncontested legitimisation through propaganda); radicalisation pathways (unresolved group or whole community grievances); and recognition of linkages, including logistic, between terrorism and other transnational criminal or human security threats. The Global Strategy (and other national strategies, particularly EU) also commends tying operational CT capability programmes in weak states more closely to wider measures to enable improved application of UN human rights standards and rule-of-law principles. It espouses non-coercive (soft) approaches to building resilience against violent extremism at grassroots level in at risk places. One recent US research overview¹¹ concluded that for CT strategies the "importance of peace-building and state building cannot be overemphasised to continue focussing on reducing tensions related to group grievances and building intergroup cohesion while creating political stability and fostering human rights. "

70. MFAT, in a recent (2012) classified review of its CT capability and outlook¹², summed this up as the evolution of a more comprehensive international CT approach (to address terrorism at source not just respond to its effects) with greater preventative focus.

Regional risks

71. In more concrete terms, the prevailing (and possibly Transatlantic-centred) strategic judgement appears to locate the most acute terrorism/extremism risk-and the highest call upon CT assistance budgets- being generated from three regions;

Greater Afghanistan/Pakistan/Bangladesh
the wider Horn of Africa/East Africa

¹⁰ Denial of terrorist operating space; building law enforcement capability in fragile states; addressing the injustice and conflict situations which promote violent extremism and which terrorism exploits; combat terrorist ideology; join up diplomacy/development and intelligence holistically for UK bilateral inputs and seek plurilateral partnerships.

¹¹ The Global Terrorism Index, (GTI) a publication of the National Consortium for the Study of Terrorism and Responses to Terrorism.

¹² "A Strategic Look at MFAT's Priorities For Future CT Engagement". Other WOCOT agencies may have done similar work -e.g. for internal planning-but it was not available (to me) in the same condensed form as this.

the Middle East (the Arabian Peninsula; Iraq; the Maghreb).

The reputed presence in these regions of significant numbers of European –origin recruits in the ranks of the foreign -fighters is a particular concern to NATO.

Section 6(a)



Priority setting for NZ engagements

75. A process to locate CT assistance within NZ’s overall international security and development priorities is needed, as is a cross agency stock-take of current and future commitments. From this should come a short list of international or regional CT projects and programmes NZ wishes to see sustained and is willing to contribute to. That stock-takes should cover all CT cluster groups and take account of the likelihood that some agencies will face rising pressures from key partners for increased burden sharing due to their own budget constraints or

¹³ NZ has formal links with ASEAN through the 5Power Arrangement and the Treaty of Amity and Cooperation.

¹⁴ See MFAT paper-para 10- for details

the effects of fragmentation. The NZ CT community will need to speak with one voice internationally about NZ's engagement priorities and capacities. This is a governance issue best handled at SOCOT level.

Released under the Official Information Act 1982

ELEMENTS OF A NATIONAL STRATEGY AND PUBLIC DOCUMENT

76. From the preceding sections it follows that a national strategy should be articulated at a classified level which captures all aspects of CT policy and operations and can be used in a way the National Plan cannot, to test for risk. In order to create a public document the sensitive parts can be redacted.

The order and sequence of the document can be argued, but it needs to cover:

1 The place of terrorism/CT in the National Security Framework (drawing upon VOH working group product)

Sources of risk:

- violent intra-communal conflict within domestic borders¹⁵;
- indigenous ideological/political extremism, including “inspired” jihad
- Randomised, localised, individual acts of extreme ideological violence (“lone wolf”)
- cross border and trans regional sectarian conflicts;
- cross border ethnic nationalist extremism/ political separatism
- global nonstate expeditionary (including jihadist);
- state- enabled (“proxy”) extremism

2 The Legal Framework for Terrorism /CT

- the TEP and TSA
- other NZ law relevant to CT response
- any relevant NZ case law and judicial interpretation
- International legal obligations
- applied or working definition¹⁶

¹⁵ The current NZ threatscape is seen as also comprising risks of nonreligious violent extremism, and potential terrorist acts, arising from environmental causes; ethno-cultural separatism (“Maori sovereignty”) or other grievances about government policies e.g. affecting the economy/migration. This review did not seek to address those matters in depth.

¹⁶ What I have in mind is a statement which gives an overall rationale for the posture of the state and can guide whole-of-government operational decision making which has to reach rational judgements about thresholds for intervention as a threat crystallises. It could, for example, say;
“Terrorism is recognisable by its means and its ends. It is the threat or use of serious/extreme and often indiscriminate violence, against NZ persons, property; the public welfare or international interests in order to

- cause panic in the general public
- destabilise vital public or commercial services
- intimidate political decision makers
- polarise intracommunal attitudes
- dramatise or propagandise a social change cause or ideology
- frustrate negotiation and incite conflict or disorder

3 Underlying Principles for Government CT Posture and Policies

NZ aspires to a CT regime closely aligned to the emerging body of international law and practice established by UN resolutions, and compliant with its obligations.

In this regime:

- the activities of the new terrorism would be treated as criminal offences, not acts of war against the nation state, and subject to legal due process under civil codes
- the powers available to the state to act against the new terrorism would be exercised proportionately and with full accountability.
- NZ would be outward-looking; its CT plans and programmes would be consistent with broader international relations policies and consciously set to optimise cross-border collaborations with likeminded jurisdictions
- the conceptual framework for executive actions in operationalizing counterterrorism policies would align with national emergency response management and would employ risk management principles.

4 Strategic Objectives- “Neither a victim, nor a source” –

expanded (teased out) as follows:

- NZ is able to protect itself and its territory from threatened direct harm
- NZ is able to sustain an appropriate level of systemic vigilance and response readiness if so threatened
- NZ is able to deny the exploitation of its territory and infrastructure or its citizens/residents to provide space, support, sanctuary or indoctrination for terrorist purposes (does this sufficiently capture CVE and community resilience ?)
- NZ interests offshore can be protected from direct or indirect harm through collaborations with risk-sharing partners
- NZ CT capability can be drawn upon for wider regional or international security objectives consistent with international law and UN strategy

5 Current National CT Policy Framework and Response System

- the National Plan
- the 4Rs-from 2004 Plan and ? a 5TH R-Resilience)
- International Engagement Framework?

6 CT Missions, Functions and Capabilities

– Structures: agencies and agency clusters

- the (contemporary) intelligence community
- international security relations and security diplomacy group
- border management/transport/identity security group
- the law enforcement agencies group (CLAG)
- the emergency/disaster management (CDEM) community
- A community awareness and resilience group?

Response Deliverables:

- Risk Awareness /Vigilance (Uncrystalised Threat)
- Risk Recognition/ Threat Identification (Crystallising Threat-early stage)
- Risk Reduction / Threat Pre-emption (Crystallising Threat-later stage)
- Incident Response (Crystallised-i.e.-Unpreempted- Threat)
- Incident Recovery

Risks- to- effectiveness

(I.e. fit for purpose? in terms of:

- critical mass; people/competencies/equipment
- intelligence and knowledge management
- functional interoperability
- known external (partner)dependencies

7 The Authorising Environment

- how national plan/strategy are commissioned and approved (i.e. Cabinet Committee-DES & TEG/Ministerial roles)
- system governance- for coherence/coordination/ audit/assurance (i.e. ODESC/ SOCOT?WOCOT/ DESG)
- tactical command and control for the CT interventions continuum (i.e. roles of NZSIS/NZP/ border agencies/Community resilience)

8 The Threat Environment

- international developments/trends
- risks to NZ homeland/NZ interests
- regional risk- SE Asia/SW Pacific
- key partner risk priorities

9 The Threat Level

10 Glossary (for a public document)

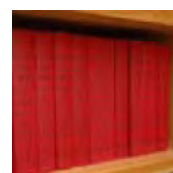
Review of Arrangements for Coordinating National Security and Intelligence Priorities

July 2013

DEPARTMENT
of the PRIME MINISTER
and CABINET



Jacki Couchman





Contents

Introduction	3
Background to this review	12
The definition of "national security"	19
The primacy of Better Public Services	21
A National Security Strategy for New Zealand	23
Coordinating intelligence and national security	32
ODESC	52
The Department of Prime Minister and Cabinet	63
Appendix 1 – Review of Arrangements for Coordinating National Security and Intelligence Priorities – Terms of Reference	73
Appendix 2 – List of interviews	77
Appendix 3 – National security and intelligence agencies	79
Appendix 4 – Draft National Security Strategy Terms of Reference - 9 April 2013	85
Appendix 5 – References	87
Appendix 6 – Glossary	88



Introduction

In mid-2010 I was asked by the then Chief Executive of the Department of Prime Minister and Cabinet, Sir Maarten Wevers, to assist with implementation of changes coming out of the *Murdoch* and *Wintringham* reviews into intelligence and national security. Three years on, it has been a privilege to work with the intelligence and security agencies again – to understand what has changed over the intervening years and to consider next steps for these critical sectors. The terms of reference for this review are attached at Appendix 1.

The context for the review includes the report of the Better Public Services Advisory Group, with its focus on collective impact at sector and system level, strengthened leadership, continuous improvement and innovation. The context also includes the recent Performance Improvement Framework review into the Department of Prime Minister and Cabinet, which made recommendations around DPMC's national security and intelligence roles. Throughout the review I have focused on what the public value is that we are seeking to deliver, on the authorising environment in which all the players are working and on the operational capabilities they possess and which the system requires.¹

In a country like New Zealand it is easy to forget the contribution that our national security makes to our way of life – and the role that government plays in managing our security. National security encompasses:

- Preservation of sovereignty and territorial integrity, including protecting the physical security of citizens.
- Protecting our lines of communication so we can communicate, trade and engage globally.
- Strengthening international order to promote security.
- Sustaining our economic prosperity – including maintaining and advancing the economic wellbeing of individuals, families, businesses and communities.
- Maintaining democratic institutions and national values.
- Ensuring public safety, and;
- Protecting the natural environment.

Each of these aspects of national security covers a set of areas for focus; for each area there is a lead government agency and supporting government agencies. Nine government agencies

¹ These vectors for analysis come from Professor Mark Moore's strategic triangle, in Moore, Mark, *The Public Value Scorecard: A Rejoinder and an Alternative to "Strategic Performance Measurement and Management in Non-profit Organisations"* by Robert Kaplan, The Hauser Centre for Non-profit Organizations, The Kennedy School of Government, Harvard University, May 2003, Working Paper 18



play a role in collecting and assessing intelligence to support our national security objectives. Over 30 government agencies play roles in the management of national security – from the Police’s role around transnational crime, to the role of the Ministry of Primary Industries in biosecurity and the role of MFAT around the security of our interests abroad. Local government, businesses, non-government organisations and communities also have roles to play, as do New Zealand’s international partners.

Our national security system has been tested over the past three years very publicly by earthquakes, the Rena incident, and the events at Pike River. It has contributed proactively to management of risk – such as management of the Rugby World Cup. Behind the scenes, state servants have worked to protect our way of life - our citizens, our institutions, our businesses, our economy, our borders, our communications channels and to support international order.

The breadth of our national security interests, and the large number of players involved, means that leadership of this sector is critical and organisation is key. This review has focused on the way that our intelligence and National Security sectors work together, are coordinated and led. It has focused specifically on the Officials’ Committee for Domestic and External Security Coordination (ODESC) and on the groups within the Department of Prime Minister and Cabinet (DPMC) which have roles relating to national security and intelligence – the Security and Risk Group (SRG), the Intelligence Coordination Group (ICG) including the National Cyber Policy Office (NCPO), and the National Assessments Bureau (NAB).

The review involved interviews of those who lead agencies working in intelligence and national security along with others with an insight into this work. It also involved desk-based research. Those I interviewed were generous with their time and, without fail, open, forthcoming, and supportive of the review’s purpose. I was very fortunate to have the assistance of Sarah Mackey, a Senior Analyst from the National Assessments Bureau during the review.

Following the review, I have made a set of recommendations, which are detailed below. Further information about the review’s findings, which led to these recommendations, is set out below.

A National Security Strategy for New Zealand

I recommend:

- 1.1. Following the report-back of the cluster work to ODESC in July, a cross-agency working group be established to develop a draft national security strategy, with consideration given to working group members from outside of government and to consultation with Five Eyes partners.



- 1.2. Once agreed by Cabinet, the Strategy will determine government priorities around national security, roles of the agencies concerned, enable prioritisation of resources, inform the national intelligence priorities, the national assessments programme, the ODESC and DES agendas.
- 1.3. The starting point for the draft strategy should be the National Security System document (May 2011) including the broad definition of national security agreed by Cabinet through that document. The strategy should encompass the elements of security (information, analysis, policy) and resilience (infrastructure, systems, operations)
- 1.4. The draft national security strategy be completed as a matter of urgency, consulted with all agencies working in intelligence and national security and robustly discussed at ODESC.
- 1.5. The draft strategy be taken to Cabinet for approval – the paper seeking approval should make clear the paramount role the strategy will play in the way the National Security sector is organised and the way decisions, including resourcing decisions, will be made around New Zealand's national security objectives.
- 1.6. Consideration be given to seeking bipartisan or cross-party support for the strategy.
- 1.7. Consent be sought from Cabinet to publish the approved strategy so that all New Zealanders have access to it.

A forum for discussions between Ministers and senior officials on national security

I recommend:

- 2.1 The Chief Executive, DPMC discuss with the Prime Minister the need for a regular forum for free and frank discussions on national security between Ministers and senior officials and the possibility that DES be convened for this purpose on a more regular basis and with relevant Ministers invited.
- 2.2 If the Prime Minister agrees, ODESC be responsible for recommending an agenda for these DES meetings, covering national security and intelligence strategy and priorities, management of these, changes in New Zealand's security environment (both domestic and international), and changes to the security environments of other nations as prioritised by DES.



Further development of the NZIC – a work programme

I recommend:

3.1 The Director, Intelligence Coordination work with the leaders of the NZIC to formulate a work programme for further development of the NZIC². The work programme should include streams focused on areas including:

- Joint work with common consumers to establish their needs and to ensure that intelligence/assessment and policy advice are provided in tandem so Ministers receive a seamless suite of information and advice.
- Effective use of resources, including eliminating duplication, sharing resources and creation of new joint products leveraging value from two or more agencies.
- Creation of new forums to join up the senior leadership groups of the various agencies on a regular basis to work on joint prioritisation, resourcing questions, product development and workforce planning.
- Joint workforce planning, including development of a common competency framework, training (for all forms of intelligence and assessment work), grading and career progression paths.
- Sharing of information, intelligence and assessments where appropriate.
- Shared research and development and testing.
- Devising a common IT strategy.
- Reviewing overseas relationships.
- Establishing a joint NZIC customer relations unit.
- Feedback on the utility of intelligence and assessment products and evaluation around the quality/accuracy of assessments to inform continuous improvement.
- Surge capacity for the sector – the ability to move staff across agencies to respond to high priority work and issues.

3.2 The draft work programme be taken to ODESC(G) for discussion as soon as possible and reported on to ODESC(G) quarterly.

The National Security sector

I recommend:

² Initially, work could focus on intelligence functions for the following agencies: GCSB, NZSIS, NAB, Defence, Police, Customs, GeoInt NZ, Immigration and MPI. Other agencies could be incorporated at a later date by agreement.



- 4.1 ODESC agree that key agencies working within the New Zealand Intelligence Community and on national security work all form part of one, National Security sector.
- 4.2 Cabinet be asked to agree to this sectoral definition.
- 4.3 The terms of reference for ODESC(G) be amended to establish ODESC(G) as the sector board for the National Security sector.
- 4.4 Cabinet mandate be sought for the Chief Executive, DPMC to be lead chief executive for the National Security sector.
- 4.5 SSC seek to amend performance expectations for all chief executives with a role in the National Security sector, to establish expectations around their lead or supporting chief executive role.
- 4.6 ODESC(G) meet prior to 30 September 2013 to agree on terms of reference for the sector board for the National Security sector, along with operating principles around things such as how planning is done, how and by whom decisions are made and around resourcing decisions.
- 4.7 The second tier senior officials' committee described in recommendation 5.10, propose an initial work programme for development of the National Security sector, to take to ODESC for discussion by 30 September. This should give consideration to ongoing forums (other than ODESC), necessary to support collaboration, flows of information to and between agencies (other than through ODESC) and joint workforce initiatives (such as secondments between agencies).
- 4.8 The new DCE, National Security and Intelligence take responsibility for the sector development work programme on appointment.

ODESC

I recommend:

- 5.1 The terms of reference for ODESC be changed to include responsibility for:
 - Keeping the national security strategy (once developed) "alive", including ensuring coordination of advice to government on matters of national security, intelligence and crisis management and coordination of the work programme coming out of the strategy.



- Assisting the work of the Cabinet Committee on Domestic and External Security Coordination by commissioning papers, think pieces and points for discussion and recommending an agenda for DES meetings.
- Discussing and receiving updates on intelligence matters (both policy and operational) as appropriate – with the Chair having exclusive rights to determine members' involvement in matters relating to intelligence.
- Commissioning and overseeing a national security and intelligence public communications plan.

5.2 The membership of ODESC be changed to DPMC (Chair), Defence, Foreign Affairs and Trade, GCSB, NZDF, Police, NZSIS, MPI, MCDEM and Customs with others to attend by invitation as determined by the agenda. DPMC senior leaders to attend as officials as determined by the CE, DPMC.

5.3 ODESC to meet bi-monthly as required.

ODESC(I)

5.4 ODESC(I) is no longer required as a separate committee.

ODESC(G)

5.5 The Terms of Reference for ODESC(G) be amended so that it is the sector board for the National Security sector as well as a board focused on governance for the “core” intelligence agencies (GCSB, NZSIS, NAB). Terms of Reference to include:

- Provide governance and assurance in respect of the GCSB, NZSIS and NAB, with a focus on systemic governance including strategic direction, performance monitoring, oversight, priority setting, and allocation of resources.
- To be the sector board for the National Security sector. The sector board role will include oversight around prioritisation of work within the sector, of resourcing decisions and of development of the sector.

5.6 The membership of ODESC(G) be changed to DPMC (Chair), SSC, Treasury, Defence, Foreign Affairs and Trade, GCSB, NZDF, Police, and NZSIS. Other agencies to be invited as appropriate. DPMC senior leaders to attend as officials as determined by the CE, DPMC.



5.7 That the Chief Executive of DPMC and Chief of New Zealand Defence Force meet to discuss the extension of ODESC(G)'s governance role to DDI and Geolnt NZ and make a decision to include or exclude these agencies.

5.8 ODESC(G) meet bi-monthly in alternate months to ODESC.

ODESC standing committees/working groups

5.9 The current ODESC standing committees/working groups be reviewed by the SRG and ICG for ongoing relevance.

ODESC officials' committee

5.10 A second-tier senior officials' committee be established to provide a discussion forum for, peer review and quality assurance around Cabinet papers concerning intelligence and national security matters. Membership to be second-tier managers of ODESC member agencies, and senior DPMC staff as determined by the CE, DPMC. Other second-tier agency staff to attend as appropriate. The DCE, National Security and Intelligence is to chair the committee - with the Chair having exclusive rights to determine members' involvement in matters relating to intelligence.

ODESC four-monthly forum

5.11 An ODESC four-monthly forum be trialled with the objectives of:

- Updating the broader National Security sector agencies on risk/threats, changes in environment and progress against the national security strategy/ODESC work programmes.
- Maintaining connections between this broader group of agencies and an understanding of the contributions made by each to national security.
- Providing a forum for agencies to showcase new initiatives, with a preference for joint/group initiatives which take a collaborative approach.
- Enabling Ministers to address leaders from the wider group of agencies.

5.12 Invitations to the forum be made to leaders of the National Security sector agencies along with relevant senior staff and high potential staff working within the sector.

Support for ODESC

5.13 ODESC and ODESC(G) receive agenda, secretariat and advisory support to carry out their functions by an advisor specifically tasked (new position). See recommendation 6.2.



The Department of Prime Minister and Cabinet

I recommend:

New second-tier role

6.1 *New second-tier role - Deputy Chief Executive, National Security and Intelligence*

- Creation of a new second-tier role (Deputy Chief Executive, National Security and Intelligence) to support the Chief Executive, DPMC in his role as the lead advisor to the Prime Minister on matters of national security and intelligence.

This role would be responsible for:

- Development, maintenance and promotion of the National Security Strategy including working with national security agencies on delivery against the strategy.
- Supporting ODESC around the strategy and driving the ODESC agenda around all matters relating to both national security and intelligence.
- Supporting ODESC(G) around governance over the core intelligence agencies and development of the NZIC and the National Security sector.
- Working with ODESC to develop the DES agenda.
- The responsibilities of the current Director, Intelligence Coordination.
- This role would be a new direct report to the Chief Executive, DPMC. The current DPMC roles of Director, Security and Risk Group, Director, National Assessments Bureau and Manager, National Cyber Policy Office would report to this new role. This role would subsume the current role of Director, Intelligence Coordination.
- Consideration would need to be given to senior-level advisory support for the DCE.

New advisor role – Advisor, ODESC

6.2 A new Advisor role be established with an exclusive focus on support for ODESC and ODESC(G), including support for agenda and attendance management, secretariat support during meetings, ensuring agencies are preparing information/papers as required, seeking performance information and providing analysis of this information to support ODESC(G).



NAB's role in providing strategic all-source assessment

- 6.3 ODESC and DES be treated as primary audiences and commissioning agents for assessment work by the NAB and are to be supported to understand what they can usefully commission.
- 6.4 Regular assessment updates created by the NAB, such as the annual National Security Contingencies Environment Scan (March ODESC), the "What could interrupt your holidays" report (early December), a scene setter on the year ahead for the Pacific (early February) and Strategic Assessment NAC (late February), be provided to both DES and ODESC as a matter of course. Where relevant, such updates should include clear information about the action/policy response government is going to take in response to risk/threat. After each such report is provided to DES and ODESC, feedback be sought on the usefulness of the report for ODESC and DES.

The role of DPMC's Policy Advisory Group in national security/intelligence matters and the need for second-review advice

- 6.5 The Chief Executive, DPMC, put in place a process to ensure cyber security policy advice is sufficiently tested and challenged, in the way that PAG performs this role for other types of policy advice.
- 6.6 The Chief Executive, DPMC make a decision about which group within DPMC (PAG or ICG) will provide second-review advice on intelligence policy, and how this extra advisory work will be resourced.
- 6.7 The Director, PAG receives ODESC agendas and, with consent of the Chair, is able to attend ODESC meetings as these relate to policy development (e.g. – cyber policy), or concern crises likely to result in a need for policy response.



Background to this review

This review follows a series of reviews and changes impacting on the intelligence and national security agencies over the past four years. Those which are most relevant to this review and report are set out below.

2009 - The Murdoch Report

In June 2009, Cabinet initiated a review of New Zealand's Intelligence Agencies (the "Murdoch review"), which was undertaken by Simon Murdoch on behalf of the State Services Commission. Recognising that formation of New Zealand's intelligence community was the result of historical legacies influenced by overseas partners' doctrines and principles, the review focused on how the community could increase coordination and reform itself to most efficiently support government. The review also recommended strengthening governance, management and coordination arrangements, including adding a governance arm to ODESC - ODESC(G).

2009 - The Wintringham Report

Michael Wintringham led a review entitled "A National Security and Intelligence Framework for New Zealand" (the "Wintringham review") in September 2009. The review considered the New Zealand Intelligence Community's role in supporting a national security system. The review led to a more systematic framework for examining national security risks and prioritising work to mitigate them, including the NZIC's roles of watch and warn, reducing vulnerability, and developing counter-measures.

2010 - Implementation of the Wintringham and Murdoch reports

In 2010, following Cabinet decisions, DPMC began work with other intelligence and national security agencies to implement a number of changes recommended in the Wintringham and Murdoch reports. The reports placed emphasis on coordination, setting clear priorities, ensuring efficiency and undertaking evaluation. Resulting changes included:

- Establishment of the Intelligence Coordination Group. DPMC established the ICG in September 2010 – not because of any specific failure but as a natural extension of DPMC's role as a coordinating agency and agreement that that intelligence community required strengthening at its centre.
- The External Assessments Bureau was renamed the National Assessments Bureau to reflect its expanded mandate, including reporting on domestic security matters, and its stronger coordination and quality assurance role.



- Director NAB, as chair of the National Assessments Committee, was formally given responsibility for the standard of assessment provided by the New Zealand Intelligence Community.
- The National Assessments Committee's mandate was evolved: the committee now considers assessments relating to national security in a broad sense, as well as its more traditional focus on external developments relevant to New Zealand's interests. A national assessments programme was established and is contributed to by all relevant parts of the New Zealand Intelligence Community.
- A specialised sub-committee of ODESC, known as the Intelligence Governance Committee or ODESC(G) was formed. ODESC(G) oversees governance and assurance in the intelligence community.
- The co-location of NAB, ICG, SRG, and CTAG in Pipitea House with the GCSB and NZSIS. This has helped to reinforce the concept of the New Zealand Intelligence Community as 'one community, many agencies'.

2011 - New Zealand's National Security System

In May 2011, Cabinet approved the publication of the paper *New Zealand's National Security System*. This resulted in the adoption by Cabinet of a new, broader definition of national security in the New Zealand context:

"National security is the condition which permits the citizens of a state to go about their daily business confidently free from fear and able to make the most of opportunities to advance their way of life. It encompasses the preparedness, protection and preservation of people, and of property and information, both tangible and intangible."

The definition of national security within this paper encompasses:

- Preservation of sovereignty and territorial integrity, including protecting the physical security of citizens.
- Protecting our lines of communication so we can communicate, trade and engage globally.
- Strengthening international order to promote security.
- Sustaining our economic prosperity – including maintaining and advancing the economic wellbeing of individuals, families, businesses and communities.



- Maintaining democratic institutions and national values.
- Ensuring public safety, and;
- Protecting the natural environment.

The National Security System paper was intended to provide a comprehensive overview of New Zealand's myriad national security interests and to provide a framework for how government agencies will work together to respond to manage national security issues.

The National Security System paper is available publicly, on DPMC's website.

2011 - Implementing the framework established by the National Security System paper

Following Cabinet's approval of the "all hazards" National Security Framework, DPMC's Security and Risk Group has led efforts to refocus whole-of-government planning on national security in a broad sense. This included re-evaluating and strengthening ODESC's mandate, and the development of the national security clusters.

The terms of reference for ODESC were revised to strengthen the quality of advice on national security, intelligence and crisis management as well as to improve planning and coordination in these areas. ODESC now oversees a wider range of issues and provides better alignment of security and intelligence arrangements in accordance to the recommendations of the National Security System.

Interagency security clusters:

In January 2012, cluster groups of agencies were established around six overarching national security themes:

- preserving sovereignty and territorial integrity.
- strengthening international order to promote security.
- sustaining economic prosperity.
- maintaining democratic institutions and national values.
- ensuring public safety.
- protecting the natural environment.



These cluster groups provide a coordinated approach to security management, with established lead and support agency designations. This prevents duplication of effort. The intention of the clusters is to foster a more comprehensive approach to national security in parallel with individual departmental processes – policy development occurs with an integrated national security end-state rather than in department silos. The ODESC Senior Officials Committee is made up of the Chairs from the different clusters and their job is to oversee and coordinate between the different clusters.

March 2013 - Kitteridge report

In March 2013 Rebecca Kitteridge delivered her report on the *Review of Compliance at the Government Communications Security Bureau* (the “Kitteridge report”). The factors leading up to her review and report are well known and in the public domain. That report and this current report on *Review of Arrangements for Coordinating National Security and Intelligence Priorities* are not specifically related. The Kitteridge report did note that ODESC(G) has an interest in the performance of the intelligence sector, which is relevant to this current review in that it has considered ODESC’s role in lifting the performance of the intelligence sector and managing risks relating to that sector and its work. Other recommendations in the Kitteridge report, including those relating to improvement in GCSB’s capability through, for example, structured secondments between GCSB and other public service departments, are part of the backdrop to this current review.

One further note on the Kitteridge report: the report was prompted by incidents which impacted on public confidence in the New Zealand Intelligence Community (NZIC). Quite rightly, those incidents could also impact on the confidence of our Five Eyes Partners. Public response to those incidents and the consequent Kitteridge review and report are a reminder that little information on our security and intelligence system and priorities is provided to the public by the government or by NZIC agencies – meaning there is little public understanding about the need for the work done by the NZIC and the tools used in that work.

Consequently there is insufficient public support for that work and the necessary and legitimate tools used, including legally-sanctioned covert surveillance. The NZIC works in a less open and transparent way than similar agency clusters in other Five Eyes Partner countries. Our partners all have publicly available national security strategies so members of the public understand the security concerns facing their countries and the government work underway in response to those concerns. I note the launch of the NZIC website in May 2012. This is a good start to coordinated NZIC public communications. These are not, however, broader communications



for the public on national security systems or strategy and do not incorporate the national security work of agencies outside of the three core members of the NZIC.

April 2013 – draft Terms of Reference issued for development of national security strategy

Draft terms of reference have been developed by DPMC's SRG for a National Security Strategy. These are attached at appendix four. There is no current timeframe for completing this work. In the context of the recommendations of this report, these terms of reference may require revision.

May 2013 - Performance Improvement Framework review of DPMC (draft)

As part of this review, I am required to consider any key outcomes arising from the Performance Improvement Framework review of DPMC in respect of the Department's work on intelligence coordination and national security priorities. I note that a separate PIF review covering the NZSIS, GCSB and ICG functions of DPMC will be undertaken later this year.

The Reviewers found:

- Good confidence in the capability of the NAB, ICG and SRG to deliver on *current* work programmes/expectations, if expressing some concerns around capacity/resourcing.
- (In relation to their concerns that DPMC establish more capacity/capability to provide advice on future strategy), that the NAB's work does have a future focus in "...assessing the risks and opportunities that could affect New Zealand's national security interests and the international environment for New Zealand's foreign policy. This in turn informs the activities of the Intelligence Coordination Group and the Security and Risk Group, whose work on the national security system is to anticipate, and ensure the country is prepared for, potential national security risks and emergencies.³" The reviewers also noted the work which had begun in the SRG on a National Security Strategy.
- There have been positive moves in relation to intelligence community coordination since the *Murdoch* report (including the joint Statement of Intent and Four-Year Plan and associated combined budget submission for the intelligence agencies), although this area of activity (intelligence coordination) is comparatively new and is under-resourced at present. "The challenge is for DPMC to consolidate the current coordination structures and processes in the (intelligence) sector to ensure that priority activities are appropriately resourced and delivered by the responsible agencies. In this regard DPMC must work

³ PIF Report, DPMC, May 2013, p2.



collaboratively with the intelligence community to achieve more effective policy development and to ensure appropriate coordination and leadership of the roles and responsibilities of all agencies within the wider community including the border security agencies, Police, MFAT, MoD and NZDF.⁴

- A need for further refinement and rationalisation of the ODESC committee structures so they are targeted to deal with specific risks and responsibilities and so ODESC is impactful in its role and provides clear value and support to Chief Executives⁵.
- There remains a gap in DPMC's ability to coordinate the wider security sector (of which the intelligence community is a part). "This may require providing the Chief Executive (of DPMC) with more explicit powers of oversight over agencies and functions dealing with the external security risks in addition to the intelligence coordination role."⁶
- In light of the significant increase in the demands of the security and intelligence sector, consideration should be given to the appointment of a Deputy Chief Executive with specific responsibility for the security and intelligence functions of DPMC "...to strengthen the linkages between the defence and intelligence agencies and provide the Prime Minister with an advice stream that more formally incorporates a national security perspective."⁷
- There is a need to communicate more effectively with the public around the Government's intelligence activities⁸.

The PIF Lead Reviewers also noted that DPMC is not currently adequately resourced to fulfil its role around the Government priority: "The national security priorities and intelligence system are well led, coordinated and managed". They noted concerns around funding for and the capability of staff within the Intelligence Coordination Group and the National Cyber Policy Office, particularly given the challenging work programmes facing each of these groups.

Of these matters covered within the draft PIF report, the following are within scope of this review:

- Consideration around the most effective way for the agencies within the "national security (including intelligence) sector" to work together to deliver collective value – including a definition around which agencies comprise that sector.
- Consideration around the optimal configuration of ODESC so that it is impactful in its role and delivers most value to Chief Executives and Ministers.
- Consideration of the powers/authorisation required to lead and coordinate a "National Security sector."

⁴ Ibid, p6.

⁵ Ibid, p6 and 16.

⁶ Ibid, p16

⁷ Ibid p18

⁸ Ibid, p27.



- Consideration around the optimal management structure within DPMC to support the CE, DPMC in his roles relating to national security (including intelligence).
- Responsibility for government communications to the public around New Zealand's national security objectives, and the roles/functions of the agencies working in the national security (including intelligence) sector.

Released under the Official Information Act 1982



The definition of "national security"

Key finding:

Interviewees accepted that Cabinet had approved a broad definition of "national security" which defines the government's work programme in this space, the role of ODESC and the definition of the National Security sector. Not all agreed with the broad definition – with some preferring a more traditional definition which excludes domestic emergency management.

I have used the broad, "all hazards" definition of "national security" throughout this review, as recommended by Michael Wintringham in his report, agreed by Cabinet and reflected in ODESC's terms of reference.

Not all of those I interviewed agreed with this broad definition. Some thought that it made prioritisation for government a challenge, and diffused ODESC's focus by requiring the committee to focus on a very broad range of risks. The vast majority of those interviewed, however, did agree with the definition used.

Many noted the need for a risk-based approach: *"Rather than categorising particular aspects/forms of security or risk as being in or out isn't it better to consider the size and impact of the risk to decide what we focus on?"*

A number noted that more traditional definitions around national security would tend to exclude some of the major threats New Zealand will face over the coming years: *"(An) all-hazards (approach) is critical because biosecurity could be the single biggest threat to our way of life in NZ."*

Some demanded a definition of national security which was relevant to all New Zealanders: *"New Zealanders tend to think about their own security in terms of things like earthquakes and pandemics, rather than in overseas defence deployments. Isn't it important that we define national security to include the things that concern real New Zealanders?"*

The definition of national security used is important because it will influence our national security strategy and define the government agencies with a role and/or interest in national security,



and, as an extension of this, the local government, business and NGO agencies that government will work with or partner with in support of national security objectives.

Released under the Official Information Act 1982



The primacy of Better Public Services

Better Public Services has been the frame for this entire review. *Better Public Services* is about creating a higher performing State sector that New Zealanders trust that is delivering outstanding results and value for money.

The *Better Public Services* Programme was launched by Prime Minister John Key on 15 March 2012 and was informed by the Better Public Services Advisory Group report, which provided recommendations to Government in December 2011 on how the Public Service could work smarter.

Better Public Services is not just about Government's ten result areas for New Zealanders – it is about fundamentally different ways of thinking and different ways of working to ensure the public receives most value for the investment made in public services. In the words of the BPS Advisory Group: *citizens are expecting better public services, delivered to them in more immediate, responsive and flexible ways*. The Advisory Group noted that the following changes were required:

- The state agencies which provide or fund services need to be managed less as a collection of individual agencies, in pursuit of their own singular objectives, and more as a system that is focused on the results that will have the biggest positive impact on New Zealanders' lives.
- We need to clarify and strengthen leadership and reduce the clutter of decision points, and
- We need to move away from a culture where value-for-money is a secondary consideration, and towards an environment where leaders and workers are motivated to continuously innovate and improve.⁹

Better Public Services requires us to ask different questions around the work we do. For example – instead of *how will we do this work?* The first-order question needs to be: *Who will we do this work with?*

These changes are no less relevant to government agencies working in intelligence and national security. We need to ensure those agencies work together coherently and to produce collective impact and that there is clarity around governance and leadership, including the way in which the security system as a whole is "...tasked, funded and monitored; the way in which conflicting demands, or demands which exceed capacity, are resolved; and the way in which decision

⁹ Better Public Services Advisory Group Report, November 2011, p 5



rights are allocated among the participants.”¹⁰ We need to ensure there is constant focus on continuous improvement of current products and services, and innovation in new realms. I have asked challenging questions of the leaders I have interviewed around how the various agencies working in national security and intelligence are organised, work together, make decisions; around how they know that what they produce is actually wanted and valued by their consumers; around what the future for these sectors will be.

Released under the Official Information Act 1982

¹⁰ Wintringham, *A National Security and Intelligence Framework for New Zealand*, 2009, p.10



A National Security Strategy for New Zealand

Key finding:

We need a single set of organising principles for national security in New Zealand, which enable our national security system to prioritise and plan.

I start here because, although it was not specifically within the terms of reference for this review, it has become clear to me through the course of the review that the lack of a single set of organising principles for national security in New Zealand makes answering the other review questions much more challenging. In general, structure follows strategy.

I also start here because of the focus of *Better Public Services* on results – not just on the ten results areas, but on how government is configured and led to deliver the results that matter to New Zealanders, for the best possible value. We need to know what the results are that the intelligence and national security agencies are seeking to deliver for New Zealanders.

National security strategy – our Five Eyes partners

The national security strategies of the Five Eyes partners share significant common ground.

Section 6(a)

Common themes around the emerging threat environment include public/private sector vulnerability to cyber-attack, the ongoing threat from (but not exclusively) Islamic terrorism, non-conventional threats including chemical, biological, radiological and nuclear (CBRN), and large scale accidents or natural hazards. Climate change, resource security, and proliferation are themes across all five countries. Projection of influence, alliances and relationships, and protection of national rights (the rule of law, democracy, free speech, tolerance and human rights) are also cornerstones of the national security platform in each country.

Australia

Australia's 2013 National Security Strategy is its first, and is aimed both at setting a framework for national security efforts, and also at setting priorities for the next five years. The strategy



follows on from the 2008 National Security Statement, and is intended to be read in company with (and indeed provides the link between) the *Australia in the Asian Century White Paper* and the imminent *Defence White Paper*. Australia has an eight-pillar approach to national security:

- Countering terrorism, espionage, and foreign intelligence.
- Deterring and defeating attacks on Australia and Australian interests.
- Preserving Australia's border integrity.
- Preventing, detecting and disrupting serious and organised crime.
- Promoting a secure international environment conducive to advancing Australia's interests.
- Strengthening the resilience of Australia's people, assets, infrastructure and institutions.
- The Australia-United States Alliance.
- Understanding and being influential in the world, particularly the Asia-Pacific.¹¹

As these pillars highlight, Australia's definition of national security is narrower than New Zealand's all hazards approach, and is focused more on external threats to Australia and the Australian people from traditional threats. Consequently, Australia's vision for its national security is to develop a unified system that anticipates threats, protects the nation, and shapes the world in its interests. This will be achieved through a secure population, resilient sovereignty, protected assets and infrastructure, and a favourable international environment. Australia's Strategy emphasises the importance of regional architecture, especially the East Asia Summit, and prioritises Australian relations with Indonesia, India, Japan and New Zealand, among others.

Australia has set itself three priorities over the next five years which recognise a changing global threat environment and the evolving and complex region in which Australia lives. Australia will concentrate on enhanced engagement in support of regional security and prosperity; integrated cyber policy and operations to enhance the defence of Australia's digital networks; and effective partnerships to achieve innovative and efficient national security outcomes. These three priorities, and the eight pillars of national security, help prioritise funding and resource allocation in an increasingly constrained federal fiscal environment.

¹¹ Strong and Secure: A Strategy for Australia's National Security, January 2013, p.vii



Canada

Canada published its national security policy in 2004, supplementing this in 2005 with a progress report. Canada has tried to develop a security system as capable at responding to a natural emergency or pandemic as it is to a terrorist attack.

The Canadian policy focused on three core national security interests:

- Protecting Canada and the safety and security of Canadians at home and abroad.
- Ensuring Canada is not a base for threats to Canadian allies.
- Contributing to international security.¹²

Previously criticised for its disparate National Security sector, Canada used the development of its policy to create a more integrated and focused security system. In December 2003 (in advance of the security policy release) Canada created a new Minister of Public Safety and Emergency Preparedness to support the core functions of security, intelligence, law enforcement, border control and emergency management, and a Cabinet Committee on Security, Public Health and Emergencies to coordinate government-wide responses to emergencies. The strategy policy established specific action points in six key areas: intelligence, emergency planning and management, public health emergencies, transportation security, border security and international security. The growing pressures on the intelligence sector featured strongly in the policy, resulting in its collection and assessments capabilities being significantly enhanced. The policy creates an overall greater emphasis on connectivity, coordination and collaboration. There has been some criticism of the clear alignment between Canada's national security policy and US national security interests.

Canada's national strategy policy document is nearly a decade old and there is considerable media and academic debate in Ottawa regarding the need for a renewed statement. Canada has issued more recent statements on Cyber security, Arctic foreign policy, Canada's place in a changing world, and Canadian defence strategy. Like New Zealand, Canada takes a wide view of national security.

United Kingdom

¹² Securing an Open Society: Canada's National Security Policy, April 2004, p.vii



The current British administration established a National Security Council and appointed a National Security Advisor as day-one priorities on coming to power. Their national security strategy launched in October 2010 not only helps direct UK foreign policy but is intended to be completely integrated into security thinking – it informs military procurement and other defence thinking. The UK seeks to build Britain’s prosperity, extend its influence and strengthen its security. Explicitly stated in the UK Strategy is a need to ensure continuity of skills and retention of corporate knowledge, including lessons learned from a decade in Iraq and Afghanistan and increased pressure on the domestic security front. Britain’s security strategy establishes the National Security Council’s four highest priority risks for the next five years:

- International terrorism, including chemical, biological, radiological or nuclear materials; and of terrorism related to Northern Ireland.
- Cyber-attack, including by other states, and by organised crime and terrorists.
- International military crises, and;
- Major accidents or natural hazards.¹³

United States

The 2010 US National security strategy explicitly outlines a strategy for “the world we seek”, focusing on renewed American leadership so that American interests can be advanced globally. It notes the need to generate a broad and sustained economic recovery. The US seeks to strengthen international norms and multilateral institutions, and is committed to its allies and partners, but will continue to underwrite global security.

America’s top national security priorities include:

- The security of the United States, its citizens, and US allies and partners.
- A strong, innovative, and growing US economy in an open international economic system that promotes opportunity and prosperity.
- Respect for universal values at home and around the world.
- An international order advanced by US leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges.¹⁴

¹³ A Strong Britain in an Age of Uncertainty: The National Security Strategy, October 2011, p.11

¹⁴ National Security Strategy, May 2010, p.7



America's new strategy (an updated version is due to be published later in 2013) will reflect the US withdrawal from major military commitments in Iraq and Afghanistan, and its pivot/rebalancing of forces from Europe and the Middle East to the Asia Pacific, as well as spending considerations in a tough fiscal climate.

The US has explicitly stated that addressing its cyber security vulnerabilities is of critical importance. The US military, under the authority of the President, has the responsibility to engage in offensive cyberspace operations: the US defines cyber-attacks as constituting a use of force against the US government and the American people and will respond aggressively under the doctrine of self-defence. It also highlights that the proliferation of weapons of mass destruction, and in particular the pursuit of nuclear weapons by violent extremists, poses the greatest risk to the US.

National security strategy – New Zealand

We have a number of documents and forms of prioritisation which, taken together, could indicate the direction of travel for our strategy around national security. These include:

- The national security system document, which sets out New Zealand's national security interests and system and describes how government agencies will work together to manage and respond to national security issues. Following this framework, the national security cluster work has involved cross-agency examination of risks to New Zealand's security.
- The national intelligence priorities, which provide the New Zealand Intelligence Community with strategic guidance on issues of interest to the New Zealand Government. These have Cabinet's approval as priorities for intelligence work, which is entirely appropriate – but are not reflective of all national security priorities, because not all priorities are able to be informed by intelligence.
- The national assessments programme which establishes a coherent work programme of intelligence assessment, and attempts to link major pieces of assessment up with policy decisions (where appropriate).

Our national security and intelligence agencies have their own sets of agency priorities, authorised by their own Ministers and by Cabinet. I acknowledge the work being done by these agencies to deliver on very challenging work programmes, to collaborate and co-operate with partner agencies and, in some cases, to ensure resources are moved between agencies to support delivery of value for government. Those I interviewed all agreed, without exception, that these agencies need to collaborate and co-operate even more, to deliver even greater value.



Structures like ODESC have been established especially to enable co-operation and collaboration between these agencies. The question is how ODESC can fulfil its role effectively in the absence of a clear set of priorities around New Zealand's national security. How can success be measured in the absence of clear national security priorities? And how can we know what the right roles are for the various players in the system, and the right way for government to allocate scarce resources between them?

I interviewed key players in the New Zealand security and intelligence agencies, along with others with an insight into the work done by these agencies. With one exception, all strongly agreed that New Zealand needed a national security strategy and/or statement – although what that would look like, and mean, differed between those interviewed. What all agreed was that:

- We need a clear way to determine national security priorities, approved by Cabinet.
- We need a clear way to describe those priorities to those working in government, and to the public.
- This work would frame the role of the national security “sector” and of ODESC and establish the legitimacy of the work being done by agencies to support national security priorities (this latter point was of particular concern to the intelligence agencies).
- Those priorities should drive resource allocation, the ODESC agenda and exercise programme, agency work programmes and feed into the national intelligence priorities and the national assessments programme.
- This work must remain live, with priorities tested from time to time by agencies and Ministers and taken back to Cabinet for approval.

I also note here that The 2010 Defence White Paper recommended an “overarching national security policy” be developed which brought together the objectives of all agencies involved in protecting New Zealand's national security.

Creating this product would require good, structured thinking by specialists from across government and perhaps the private sector (for example – in framing threats to cyber security), and even from our partner countries – given that the product formed needs to be cognisant of and connected to New Zealand's place in the world, international interests and partnerships.

We face a number of risks in not having a national security strategy and/or statement – around lack of prioritisation of scarce resources, as an example. A key risk is that various documents, such as the National Intelligence Priorities,

“We need a framework for doing stuff – mandate and authority”.

“The story about the national security space for agencies is key – so everyone knows who is in the space with them, and what responsibilities everyone has.”



become de-facto lists of "priorities" for national security. Another example is a paper that was recently referred to by an interviewee as the "Ten biggest risks paper". The paper being referred to is actually the "National Security Contingencies - an environmental scan for 2013" paper from NAB. While a very good scanning paper, this document provides very particular information – is there anything different for this event/issue this year, or did it represent essentially a business-as-usual issue for New Zealand agencies? This means that some of the serious risks identified in a table at the back of the document (such as a major natural bio-security hazard incident in New Zealand) are not outlined within the document as they are seen as "business as usual for the Government."

The national security cluster work

Key finding:

In most cases, the cluster work has provided a good framework for valuable cross-agency work. The joint report-back from the cluster groups to ODESC in July should provide a very good basis for discussion around national security risks and the actions required to mitigate them. This could be a good contribution towards development of a national security strategy.

As mentioned above, work is currently underway on the development of national security clusters, as was initially outlined in the 2011 National Security System paper.

What is key about these clusters is that they cut across agency boundaries – although there is a lead agency for each aspect of a cluster's work, the work takes a risk lens, rather than an agency lens.

The objective of the cluster work is to establish lead agency responsibility and priority work objectives for the "all hazards" range of national security contingencies. Commissioned in January 2012, the cluster work initially lagged behind competing agency work priorities and, according to a number of those interviewed, suffered from a lack of clear objectives and milestones. The cluster process has since been simplified, with a focus on identifying risks



and attributing clear agency responsibilities, and clear time frames have sped up the process. Progress is uneven and some of the cluster groups are outperforming others. With the exception of the *democratic institutions and national values* cluster, all had presented at ODESC by early June 2013. Given that the concept of democratic institutions and national values substantially underpins the other cluster work, a decision has been made to have this feed into the other five clusters' work rather than form a cluster in its own right. I am advised that the cluster leaders are convening a joint workshop in June, with the aim of making an overall report-back to ODESC in July.

In themselves, the clusters do not form a national security framework, but rather a risk management and response strategy. Each cluster has been asked to identify the top risks in their respective thematic area, and it is intended that these will generate debate in ODESC on emerging priorities. Once these have been identified and agreed to by ODESC there is uncertainty around what ODESC's role is, in terms of a mandate to prioritise work and, potentially, allocate resources.

Those I interviewed had mixed views as to the value of the likely outcome of this work. In particular, there was a lack of agreement on whether the results of the cluster group work would ultimately inform national security priorities for New Zealand and assist with a coherent cross-government work programme. Some of those interviewed thought this possible - others thought that the way the cluster work was framed meant that it was focused at a very operational level, rather than taking a strategic overview of national security priorities and risks.

Overall, whatever the view about the likely outcome of the cluster work, those interviewed tended to agree that cross-agency conversations and linkages on various aspects of national security were of intrinsic value themselves.

A National Security Strategy for New Zealand - recommendations

- 1 Following the report-back of the cluster work to ODESC in July, a cross-agency working group be established to develop a draft national security strategy, with consideration given to working group members from outside of government and to consultation with Five Eyes partners.
- 2 The Strategy will determine government priorities around national security, roles of the agencies concerned, enable prioritisation of resources, inform the national intelligence priorities, the national assessments programme, the ODESC and DES agendas.
- 3 The starting point for the draft strategy should be the National Security System document including the broad definition of national security agreed by Cabinet through that



document. The strategy should encompass the elements of security (information, analysis, policy) and resilience (infrastructure, systems, operations).

- 4 The draft national security strategy be completed as a matter of urgency, consulted with all agencies working in intelligence and national security and robustly discussed at ODESC.
- 5 The draft strategy be taken to Cabinet for approval – the paper seeking approval should make clear the paramount role the strategy will play in the way the national security agencies are organised and the way decisions, including resourcing decisions, will be made around New Zealand's national security objectives.
- 6 Consideration be given to seeking bipartisan or cross-party support for the strategy.
- 7 Consent be sought from Cabinet to publish the approved strategy so that all New Zealanders have access to it.

Released under the Official Information Act 1982



Coordinating intelligence and national security

The *Better Public Services* Advisory Group found that:

“...one of the main obstacles to the state services responding more effectively to cross-agency results is the inflexibility in current organisational arrangements. It tends to be too hard to divert staff from existing work plans. Multi-agency work is on occasion characterised by individual agencies protecting their own patch rather than focusing on solving the problem.”¹⁵

The Advisory Group suggested a broader spectrum of cross-sector organisational arrangements than we had in place at the time of their report – from loose agency groupings to a fully-integrated departmental model – and noted that it was more likely that jointly-owned results would be achieved if accountabilities were clearly defined and all parties had some serious “skin in the game”. They noted that sector-wide decision-making could be formally shared by agencies through establishing oversight boards and specifying clearly their responsibilities. The Advisory Group said: “These arrangements could be *soft-wired* by mutual consent between the agencies...or *hard-wired* through more formal mandates, financial accountabilities and reporting arrangements.”¹⁶

As mentioned above, those I interviewed all agreed, without exception, that our agencies with roles in intelligence and national security need to collaborate and co-operate even more, to deliver even greater value.

Given that ODESC as an institutional arrangement is covered by a later section of this report, I focus here on:

- The Cabinet/Ministerial authorising environment
- Services to the Prime Minister and to Ministers
- The two sectors – the New Zealand Intelligence Community (the “Intelligence Sector”), and the National Security sector.

¹⁵ Better Public Services Advisory Group report, p26

¹⁶ Ibid, p26



The Cabinet/Ministerial authorising environment

Key finding:

Senior officials say that New Zealand would benefit from more free and frank discussion between Ministers and senior officials on national security matters. There is a question about whether this discussion could occur at DES with additional Ministers as appropriate invited to the table.

At present, at least three separate Cabinet Committees cover the range of matters related to New Zealand's national security and intelligence.

The Cabinet Committee on Domestic and External Security (DES), chaired by the Prime Minister, meets as required, with the following terms of reference:

- To coordinate and direct the national response to a major crisis or to circumstances affecting national security (such as a natural disaster, biosecurity problem, health emergency, or terrorist/military threat) within New Zealand or involving New Zealand's interests overseas.
- To consider issues of oversight, organisation and priorities for the New Zealand intelligence community and any issues which, because of their security or intelligence implications, the Prime Minister directs be considered by the committee.
- To consider policy and other matters relating to domestic and external security coordination.

Cabinet External Relations and Defence Committee (ERD), chaired by Hon Murray McCully, meets fortnightly during sitting weeks, with the following terms of reference:

- To consider policy and other matters relating to foreign affairs, international trade, development assistance, and defence.

The Cabinet Committee on State Sector Reform and Expenditure Control (SEC), chaired by Hon Bill English, meets weekly during sitting weeks, with the following terms of reference:



- To control and review government expenditure to improve value for money in the State sector, and to consider State sector reform and other State sector issues.

I mention SEC here as I understand that it is the Cabinet Committee where defence expenditure is currently considered.

These three Cabinet Committees are New Zealand's forums for discussions concerning national security between a group of Ministers and senior officials. Outside of Cabinet Committee, there will, of course, be ad-hoc but formal Ministerial meetings on specific topics, informal meetings Ministers choose to have with one another and the usual meetings between Ministers and their Chief Executives and senior staff.

Those I interviewed expressed a strong interest in an improved ability to discuss the national security environment, priorities, issues and mitigation with Ministers.

There was little agreement or even thinking on what the right "structure" would be, but more certainty about the job of work to be done:

- this is about senior officials being able to meet with one, consistent group of Ministers with a mandate over national security/intelligence matters;
- with time and permission to have conversations about the changing environment, about strategy, government expectations and about the work being done by agencies;
- where assessment and the policy response can be joined up.

The hope is that the knowledge, familiarity with the national security system and relationships developed would lead to better strategy, better decision-making and better ability to respond in times of crisis.

Our partner countries have constructed a number of ways to facilitate these conversations on national security between Ministers and senior officials. As examples:

"This a real hole in the current system. How would this work? How can we get engagement with Ministers on issues and risks and security strategy in a forum where discussion is encouraged and ideas don't have to be fully formed yet?"

"Key Ministers, as a group, need to feel familiarity with the national security systems, the risks, issues and so on – so that when a crisis occurs, the way the response is formed makes sense to them. We might not be supporting them well enough now to feel this familiarity."



Australia's National Security Committee (NSC) is chaired by the Prime Minister and focuses on major international security issues of strategic importance to Australia, border protection policy, national responses to developing situations (either domestic or international) and classified matters relating to aspects of operations and activities of the Australian Intelligence Community.

Canada established an Advisory Council on National Security in 2005, aimed at providing confidential advice on national security and improving the sector. This advisory body was made up of 15 security experts external to government. However, this body was shut down in mid-2012, partly as a cost saving mechanism, and partly because the government felt agency outreach was sufficient to render the Council unnecessary.

The National Security Council is the **United Kingdom's** principal forum for discussions on the government's national security objectives (and how to achieve them in a constrained fiscal climate). It aims to ensure a strategic and tightly coordinated approach across the whole of government to the risks and opportunities the country faces. With purely partisan political membership, it has created a community of ministers who are used to examining the wider picture. A 2011 review of the central national security and intelligence machinery recommended that the NSC's priorities should be the lead driver of the Joint Intelligence Committee's (the UK National Assessments Committee equivalent) agenda. This would marry up national security objectives and the intelligence assessment programme. It also recommended that the wider intelligence apparatus be put at the disposal of the NSC, where appropriate, and that policy implications of analytical assessments should be given to Ministers as a matter of course.

The **United States** system has a traditional National Security Council function. Established in the Truman presidency, the membership of the National Security Council has evolved with each successive president. However, the Council remains the President's principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials.

Our partner countries have taken a range of approaches to the creation of a forum where Ministers and senior officials regularly discuss national security and intelligence priorities and work programmes, the changing environment and emerging threats and crises. All but Canada have found ongoing value in such a forum, along with having a National Security Advisor role responsible for coordination on behalf of the Ministerial forum (I look at the New Zealand equivalent of the National Security Advisor role later in this report). It is not clear to me that we need to create a new forum, when the terms of reference of DES essentially cover this space. The question is whether DES would have an interest in meeting more frequently, with fewer



formal papers, to have more free and frank discussions around intelligence and national security – and which other Ministers would need to be at these meetings to enable fruitful conversation.

A forum for discussions between Ministers and senior officials on national security - recommendations

- 1 The Chief Executive, DPMC discuss with the Prime Minister the need for a regular forum for free and frank discussions on national security between Ministers and senior officials and the possibility that DES be convened for this purpose on a more regular basis and with relevant Ministers invited.
- 2 If the Prime Minister agrees, ODESC be responsible for recommending an agenda for these DES meetings, covering national security and intelligence strategy and priorities, management of these, changes in New Zealand's security environment (both domestic and international), and changes to the security environments of other nations as prioritised by DES.

Services to the Prime Minister and to individual Ministers

Key findings:

- The primary focus must be on the needs of the consumer – what does the consumer need to support his or her decision-making?
- The Prime Minister, and other Ministers, need clear and consistent streams of advice on intelligence and on national security priorities/risks/crises. In each case it needs to be clear to the Minister who will take the lead on information/advice.
- The Prime Minister and other Ministers need the answer to "what now?" once they receive intelligence/assessment product. They need to be advised of the policy implications in a timely manner.
- Even Ministers who do not have portfolios directly covering national security/intelligence matters have an interest in both national security strategy/prioritisation and in how crises are being managed. It is important that these Ministers also have a plain English stream of information available.

Our Ministers are primary consumers for intelligence, assessments, operational

"The Prime Minister does need a filter on these things, and that sometimes doesn't work. We sometimes get agencies sending two reports on the same thing. We need to know (who is responsible for what). We don't want a report from one agency and then an email direct to the PM



and policy advice on national security and intelligence. Are they getting what they need, as consumers? Are the lines of agency accountability and communication clear? Is there duplication?

Those I interviewed were very focused on provision of quality services to Ministers. In general, this is an area of strength for New Zealand government agencies (as evidenced through PIF reports). That said, those I interviewed identified the following challenges in supporting the Prime Minister and other Ministers:

- The Prime Minister, and other Ministers, need clear, simple and consistent streams of advice on intelligence and on national security priorities/risks/crises. In each case it needs to be clear to the Minister which one agency will take the lead on information/advice.
- Ministers (and indeed, Chief Executives who are consumers of intelligence/assessment products), are not always aware of what the intelligence agencies are capable of providing – meaning they are less able to be informed consumers.
- While it is important that intelligence collection and assessment are not inappropriately influenced by policy preferences, it is also important that Ministers have advice on options for actions once they receive intelligence/assessment, so they are not left wondering: “what now?”
- The agencies providing intelligence and assessment products to a number of Ministers were not necessarily joined up in their service provision. It might be that they could join up to deliver some products, or could look to present their products more consistently
- Little feedback is sought from Ministers about the utility of the information they have been provided; little retrospective evaluation is done around the accuracy of the information. A number of our Five Eyes partners have processes for feedback and evaluation to inform continuous improvement.
- Even Ministers who do not have portfolios directly covering national security/intelligence matters have an interest in both national security strategy/prioritisation and in how crises are being managed. It is important that these Ministers also have a plain English stream of information available.



This feedback is addressed in recommendations relating to further development of the New Zealand Intelligence Community (NZIC), and on development of the National Security sector.

Released under the Official Information Act 1982



The two sectors – the New Zealand Intelligence Community (the “Intelligence Sector”), and the National Security sector

What is a sector?

What is an effective sector? What does it look like, do, and create, that is different from the sum of its parts? The Better Public Services Advisory Group report promotes the idea that agencies work in sectoral groupings to produce better value. The report does not describe what a sector looks like, or what determines success from this different way of working.

What we do know, from the sectors we already have operating, is that the following are critical to success:

- The agencies within the sector are connected through co-dependent outcomes or results, joint work programmes or a client pipeline (as in the case of the Justice sector).
- A governance board with responsibility for such things as:
 - strategic advice to Ministers on maximising the collective impact of the sector agencies
 - assurance to Ministers that the resources of the sector have been properly applied and the sector’s work programme will be delivered on, and
 - joint decision-making and delivery on issues that require cross-agency action.¹⁷
- One lead Chief Executive, with other Chief Executives playing supporting roles. In the case of established sectors, each of these Chief Executives has performance expectations agreed with the State Services Commissioner which include the contribution they are expected to make to the sector.
- Clear accountabilities and responsibilities for each agency in the sector.
- Operating principles around things such as how planning is done, how and by whom decisions are made and around resourcing decisions.

¹⁷ This framework comes from the Social Sector Forum Chief Executives’ Terms of Reference to 24 April 2014.



Are the intelligence and National Security sectors separate?

Key findings:

- It is not clear that there is value in treating the "intelligence" and "national security" agency groupings as separate sectors. A number of agencies have feet in both camps.
- All intelligence and national security agencies should be treated as members of one National Security sector.
- The current separation has not supported good engagement - as an example, the core intelligence agencies tell me they have felt excluded from the national security cluster work.
- There is value in continuing with special governance arrangements around the GCSB, NZSIS and NAB and perhaps extending these arrangements to other NZIC agencies.
- There is value in continuing with work to specifically develop the NZIC because the agencies/parts of agencies involved in intelligence work have tradecraft and international partnerships in common and have the potential to share a number of streams of work including workforce development.

A question I posed to myself and to others during this review, was whether there really should be two sectors here, or whether New Zealand would benefit more from one completely joined-up sector. There are a lot of overlaps, including a number of agencies with groups involved in both intelligence work and national security policy, advice or operational functions. Due to these overlaps it is a challenge to separate the agencies involved into two sectors. Rather than planning for the "two sectors" to work more effectively together, my view is that they should be formed into one, National Security sector.

I do want to note here that the New Zealand Intelligence Community agencies have potential to push collaboration the farthest because:

- The NZIC agencies make a joint contribution to a particular set of international relationships (the "Five Eyes" relationships).
- NZIC members use common (intelligence and assessment) tradecraft and work together on a number of fronts to produce end products. This creates potential including a shared workforce, common IT platforms (and this community does already share a secure site), joint work programming, prioritisation and resourcing, and the setting of joint standards



(which has already occurred in the assessments space). There is the potential here for a true sectoral approach to intelligence work.

- Those working within the broader National Security sector (as examples – those working in biosecurity in MPI, in policy for Customs and as diplomats for MFAT), are less bound by similar tradecraft, have different sets of international partners, and are less likely to benefit from joint workforce initiatives. They could however, take a sectoral approach to matters including joint work programming, prioritisation and resourcing.

For this reason, I have first explored the work required to strengthen the NZIC, and then the work required to form a National Security sector, of which the NZIC is part.

The Intelligence Coordination Group and the New Zealand Intelligence Community

Key findings:

- The NZIC has markedly improved the way it works over the past three years.
- The Intelligence Coordination Group and ODESC(G) have played key roles in these improvements.
- NZIC agencies are open about having more work to do before they can be said to be taking a truly sectoral approach – and they do want to do this further work.
- Due to their particular nature and arrangements, there is value in continuing a special governance arrangement over the core intelligence agencies and perhaps extending this to include DDI.

The New Zealand Intelligence Community (NZIC) has three "core" members: the GCSB, NZSIS and NAB. These are agencies which are exclusively in the intelligence/assessment business. Other members include DDI and the intelligence groups within Immigration New Zealand, New Zealand Police, Customs, and MPI. These agencies provide a mix of intelligence and assessment functions, with some also having operational and policy roles. A number of other agencies are also consumers of intelligence, such as MFAT and Maritime New Zealand.

In total around 700-750 staff are employed in intelligence/assessment roles within New Zealand. Within this relatively small NZIC community leaders tend to be well-known to one another, some staff have moved between agencies and agencies share information, intelligence and assessments using a secure system.



In September 2010, following Cabinet decision, DPMC established the Intelligence Coordination Group (ICG), headed by the Director, Intelligence Coordination to:

“(assist) intelligence agencies to provide coordinated and useful information for government decision-making, and (support) the Officials Committee for Domestic and External Security Coordination (ODESC) in its governance role in relation to those agencies. Its key functions are to lead and coordinate the intelligence community agencies for requirements, priority setting, risk management and functional performance reporting. It also coordinates the New Zealand intelligence community's overall relationships with foreign partners.”¹⁸

Creation of the ICG, and its achievements, have been viewed very favourably both within the NZIC and in other related agencies. In particular, the Director's work to bring together the leaders of the intelligence agencies and forums of other senior staff were noted. Questions were raised about the resourcing applied to the ICG, its advisory capacity and capability and the next steps for this role (with some interviewees thinking the logical extension was for the role to also encompass the broader National Security sector).

I elaborate more on the ICG role, achievements and possible future direction below, in the section of this report on DPMC's security and intelligence functions.

There have been a number of changes in the NZIC since 2010, through the work of leaders and agencies within the NZIC and the coordination and direction provided by the ICG. I note the joint Statement of Intent, 4 Year Plan and some shared back office functions for the GCSB, NZSIS and NAB. This is a real step towards a sectoral approach and has led to the movement of some resources between agencies to address priority work. In addition, priorities for intelligence work are now agreed by Cabinet and a national assessments programme including both domestic and external intelligence drawing on material from all NZIC agencies relevant to national security interests and priorities is coordinated by the Director of the National Assessments Bureau¹⁹.

Moves are afoot at senior levels of the NZIC to create a community with genuine career progression. In practice this already happens informally. A security clearance is a valuable commodity in the State sector job market. In a small national sector where savvy operators are

¹⁸ From <http://www.dPMC.govt.nz/icg>

¹⁹ I note that the Director, NAB has recently worked with the heads of the other assessment-producing agencies to create a written agreement around how the assessments programme is coordinated.



generally well known, employees are easily 'poached' between agencies – particularly in the more technical aspects of the sector.

The small size of organisations, often with relatively flat hierarchies, means employees may have little alternative to looking outside of their agency in order to obtain promotion or move into management positions. Increasingly, however, agencies are looking to provide career development opportunities via long and short term secondments. As examples of moves between NZIC agencies:

- NAB currently has two senior analysts on two year secondments to MFAT and MPI.
- In NAB's most recent recruitment round (mid-2012) two very experienced MFAT employees were hired as senior analysts, while a third MFAT staffer is on a two year secondment to the NAB.
- Customs provides analysts to CTAG, NMCC and Police. Customs also has a longstanding secondment arrangement with the NZSIS.
- Section 6(a)
- CTAG is largely staffed via secondments.
- Both ICG and SRG have a mixture of permanent and seconded staff, with secondees from NAB, GCSB, Police, NZSIS and Customs.
- The Ministry of Defence and MFAT have an annual secondment exchange.
- Retired military intelligence corps officers fill a number of senior intelligence positions in the New Zealand System, including at Customs, NAB and Immigration.
- DDI recruited three analysts with MOD experience in 2012.

The New Zealand Intelligence Community has also recognised the need for its assessments to be robust and have a clear audit trail. To this end, National Assessments Committee agencies have signed up to an agreed standard of analytical rigour necessary to have papers approved. Probabilistic language is also being used to ensure consistency across the community, in the hope it will provide clarity for consumers – it gives percentage weightings to what analysts mean if they use the words "likely" or "unlikely", for example. The NZIC has invested in analytical training for staff from a variety of international providers, Section 6(a)

with the intention of creating a self-sustaining assessments training capability.



Supplementing this initiative are agencies' own in-house training and induction programmes, and opportunities with their respective international partners. As has happened in the UK system, the New Zealand Defence Force's School of Military Intelligence (under development) could become the formal repository of training for the wider NZIC.

"The SOI (for the three core agencies) doesn't seem to go to shared intent. Our shortcomings are in measuring what we should do, with a view to finding out what we should stop or what we are doing badly, by talking to our customers."

Continuing development of the NZIC

All of these changes are a good start, but only go a short way towards creating a real sectoral approach – the leaders of the intelligence agencies I interviewed were in full agreement on this. The costs of the current approach to intelligence include loss of opportunity through collaboration, possible poor application of resources, increased likelihood of duplication and limited career opportunities for staff working within the NZIC (not to mention competition for staff). Benefits from a stronger, more collaborative community could include better, more coherent products for consumers, better targeting of resources, enhanced reputation for the NZIC, improved career development and opportunities for staff.

Those I interviewed suggested the following would be indicators of real change in the NZIC:

- A shared sense of purpose for all members of the NZIC – an understanding about the role the NZIC plays and the value it can add - to the point where staff in all the NZIC agencies can tell the story about how the NZIC fits together and works together.
- A focus on what consumers of the NZIC want and need, and the best way to provide this, from the resources available across the NZIC. This would involve joint work with common consumers to establish their needs, rather than various agencies making individual approaches.
- Shared products for consumers and/or integrated delivery, where possible. Having the weekly bulletin incorporate information from all NZIC agencies is a good start.
- While ensuring that intelligence work is not policy driven – making sure that it is policy *relevant* and that Ministers are advised on the policy implications of intelligence and assessments by their policy advisors in a timely manner.
- Prioritisation of work and of resources across the NZIC.
- One workforce - a common pay and grading system for intelligence staff, common training and career progression options across the NZIC.



- Joining up the leadership teams of the agencies on a regular basis to work on joint prioritisation, resourcing questions, product development and workforce planning²⁰.
- Sharing of research and development and testing. Sharing of information, intelligence and assessments as a matter of course, where appropriate.
- Continuation of the good initiatives already in place, including the NZIC leaders' forum (organised by the ICG).

Not all of these will be as relevant to all agencies working in the intelligence space. While the three “core” agencies have intelligence and assessment as their sole business, other intelligence and assessment groups sit within organisations with other core functions. That said, the core agencies and the intelligence and assessment groups within other agencies do share a number of things including a commitment to their tradecraft and a commitment to the Five Eyes relationships.

“There are tools and capabilities that exist across intelligence agencies that aren't well understood ...
Sharing information can be frustrating. Do we have a joined-up picture of all the information and intelligence we hold, across government?”

Further development of the NZIC – a work programme - recommendations

- 1 The Director, Intelligence Coordination work with the leaders of the NZIC to formulate a draft work programme for further development of the NZIC²¹. The work programme should include streams focused on areas including:
 - Joint work with common consumers to establish their needs and to ensure that intelligence/assessment and policy advice are provided in tandem so Ministers receive a seamless suite of information and advice.
 - Effective use of resources, including eliminating duplication, sharing resources and creation of new joint products leveraging value from two or more agencies.
 - Creation of new forums to join up the senior leadership groups of the various agencies on a regular basis to work on joint prioritisation, resourcing questions, product development and workforce planning.

²⁰ I note the work underway with the GCSB and NZSIS leadership teams to facilitate a closer working relationship between the teams.

²¹ Initially, work to focus on intelligence functions for the following agencies: GCSB, NZSIS, NAB, NZDF, Police, Customs, Immigration and MPI. Other agencies could be incorporated at a later date by agreement.



- Joint workforce planning, including development of a common competency framework, training (for all forms of intelligence and assessment work), grading and career progression paths.
 - Sharing of information, intelligence and assessments where appropriate.
 - Shared research and development and testing.
 - Devising a common IT strategy.
 - Reviewing overseas relationships.
 - Establishing a joint NZIC customer relations unit.
 - Feedback on the utility of intelligence and assessment products and evaluation around the quality/accuracy of assessments to inform continuous improvement.
 - Surge capacity for the sector – the ability to move staff across agencies to respond to high priority work and issues.
- 2 The draft work programme be taken to ODESC(G) for discussion as soon as possible and reported on to ODESC(G) quarterly.

The “national security” sector

Key findings :

- The agencies working in the National Security sector are effectively defined as a group by ODESC and by the definition of national security used by ODESC. While recognising current bilateral relationships, working groups (including the cluster groups), and joint work to develop policy or in operations, all agreed that they could work together more effectively as a sector to achieve greater value.
- The Chief Executive, DPMC is considered by other Chief Executives to be the lead Chief Executive for the National Security sector.

The broader National Security sector includes the GCSB, NZSIS and NAB as well as a number of agencies with both intelligence and national security policy/advisory/operational roles, such as NZDF, MoD, Immigration New Zealand, New Zealand Police, Customs and MPI. It also includes agencies with policy, advisory or operational roles which make contributions to national security including MFAT, MBIE, MCDEM, MfE, the New Zealand Fire Service, MOH, DIA, MOJ, MOT, SSC, Treasury and Maritime New Zealand, and groups within DPMC with security and intelligence functions.



In reality a core group of agencies have a day-to-day interest in national security (GCSB, NZSIS, DPMC, MoD, NZDF, Police, MFAT, Customs, Immigration), and others have many core roles, of which a contribution to national security is one. The broad definition of national security (which informs the breadth of ODESC's mandate) is what binds these agencies together.

While the National Security sector is not as joined up as it could be, a considerable amount of cross-agency collaboration is ongoing and has been for many years. This is not a sector which has to be built from scratch. The national security cluster work has enhanced cooperation and introduced a divergent range of agencies to the all hazards concept of national security – and possibly to one another as well.

All those I interviewed agreed that agencies working on national security do work together in a variety of ways on a regular basis - but could collaborate more effectively. ODESC is an important organising construct for these agencies – although there are other working groups, committees and bilateral arrangements between them, it is ODESC where they all meet together – and ODESC at its best would enable them to coordinate, align and prioritise their work effectively as a sector. DPMC's Security and Risk Group is the practical manifestation of ODESC for many of these agencies, with its focus on:

- Strengthening early warning of emerging security issues.
- Assessing and evaluating potential national risks.
- Identifying potential vulnerabilities and likely consequences.
- Determining options for controlling significant risks.
- Developing management strategies for government.
- Coordinating planning and response around security risks.
- Developing long-term strategies for mitigation, preparation, and management of these risks by appropriate agencies.

The advantage we have, as a relatively small bureaucracy in a small country, is that the leaders of our government agencies tend to know one another. We also have networks across agencies at all levels, where information is exchanged and work is shared on a daily basis.

This familiarity and these horizontal networks are critical to getting the job of agencies done.



However, if our leaders knowing one another and our staff sharing information and working together was enough to create an effective sectoral and system approach, we would not have needed the *Better Public Services* Advisory Group report, or the changed approach which is being sought as a result of that report.

I do not underestimate the challenges created by different agency cultures, objectives and incentives. I also note the time taken to achieve change for the NZIC – and in that case the three core agencies, with their joint Statement of Intent, joint 4 year plan and work to shift resources across agencies, also share a Minister in common.

I also note that many of the agencies with an interest in national security are also members of other sectors – Police are members of the Justice sector, for example. National security is not the only lens through which Police view their work. It is important that a sectoral approach to national security delivers new value without unnecessarily duplicating requirements imposed by other sectoral groupings.

One thing that has interested me through this work is how carefully, by necessity, we nurture our various relationships with foreign partners – and I wonder whether agencies put as much effort into nurturing their relationships with their New Zealand “partner” agencies.

The Combined Threat Assessments Group (CTAG) is an interagency group responsible to the New Zealand Security Intelligence Service. CTAG’s role is to inform government’s risk management processes by providing timely and accurate assessment of terrorist and criminal threats of physical harm to New Zealanders and New Zealand interests. CTAG’s staffing needs are met via secondments from the Service, New Zealand Police, the GCSB, New Zealand Defence Force (DDI), Maritime New Zealand and New Zealand Customs Service.

The National Maritime Coordination Centre (NMCC) was established in 2002 to manage New Zealand’s maritime surveillance, coordinating inter-agency or multi-agency operations to detect offending in the maritime domain, as well as the civilian use of sea and aerial patrols. The NMCC has responsibility for anything in the marine environment that could impact on New Zealand’s sovereignty, security, safety, economy or foreign policy interests. While operationally independent, it is a part of the New Zealand Customs Service, and is staffed by analysts and liaison officers from Customs, the Ministry for Primary Industries and the New Zealand Defence Force.

The New Zealand Police host the organised crime assessment centre. Because this work is multi-agency, analysts from Police, Customs, Health, Immigration and Internal Affairs are co-located at the Police National Headquarters in Wellington.



To achieve our international aspirations, so much work needs to be done at home – and not only in conjunction with other government agencies, but in the public and political arenas.

I am proposing a deliberate work programme be set for development of the National Security sector, drawing on what we have learnt from other sector groupings in the State sector, and on the energy created through the national security cluster work.

What does the sector need to ensure success?

The agencies within the sector are connected through co-dependent outcomes/results, joint work programmes or a client pipeline.

In this case, the agencies concerned are connected through current joint work and, in some cases, long-established working relationships, through work that has been coordinated by the ICG and by the SRG (such as pandemic planning and the national security cluster work) and through other ODESC contributions. A national security strategy and resulting work programme will make clearer the connections between agencies.

A governance board with responsibility for:

- *strategic advice to Ministers on maximising the collective impact of the national security agencies*
- *assurance to Ministers that the resources of the sector have been properly applied and the sector's work programme will be delivered on, and*
- *Joint decision-making and delivery on issues that require cross-agency action²².*

There is a need for a governance board for the National Security sector. ODESC(G) could perform this role.

One lead Chief Executive, with other Chief Executives playing supporting roles

In this case, it is agreed by the sector Chief Executives that the Chief Executive, DPMC is the lead Chief Executive for the sector and that other Chief Executives are supporting Chief Executives. Mandate for these roles should be sought from Cabinet. Each of these Chief

²² This framework comes from the Social Sector Forum Chief Executives' Terms of Reference to 24 April 2014. It may be that a different configuration of responsibilities for the National Security sector will be more appropriate – ODESC is the forum for this discussion.



Executives should have performance expectations which include the contribution they are expected to make to the sector.

Clear accountabilities and responsibilities for each agency in the sector

These are set, to some extent, through the national security system work, backed by the national security cluster work, though the national intelligence priorities and the national assessments programme and (by threat type) through response plans coordinated by the SRG and other agencies for such events as earthquakes, pandemics, mass arrivals, terrorist attacks and biosecurity threats. A national security strategy and resulting work programmes will make clearer the accountabilities and responsibilities for each agency in the sector.

Operating principles around things such as how planning is done, how and by whom decisions are made and around resourcing decisions.

These need to be set for the sector through the sector board.

The National Security sector – recommendations

- 1 Agreement be reached by ODESC that key agencies working with the New Zealand Intelligence Community and on national security work all form part of one, National Security sector.
- 2 Cabinet be asked to agree to this sectoral definition.
- 3 The terms of reference for ODESC(G) be amended to establish ODESC(G) as the sector board for the National Security sector.
- 4 Cabinet mandate be sought for the Chief Executive, DPMC to be lead chief executive for the National Security sector.
- 5 SSC seek to amend performance expectations for all chief executives with a role in the National Security sector, to establish expectations around their lead or supporting chief executive role.
- 6 ODESC(G) meet prior to 30 September 2013 to agree on terms of reference for the sector board for the National Security sector, along with operating principles around things such as how planning is done, how and by whom decisions are made and around resourcing decisions.
- 7 The second tier senior officials' committee described in recommendation 5.10, propose an initial work programme for development of the National Security sector, to take to ODESC for discussion by 30 September. This should include consideration of ongoing forums (other than ODESC) necessary to support collaboration, flows of information to



and between agencies (other than through ODESC) and joint workforce initiatives (such as secondments between agencies).

- 8 The new DCE, National Security and Intelligence take responsibility for the National Security sector development work programme on appointment.

Released under the Official Information Act 1982



ODESC

Key findings:

- ODESC is a very effective coordination and reporting mechanism in times of crisis.
- Lack of definition around ODESC's "non-crisis" role leads to uncertainty from agencies about its function and role, and their own functions and roles.
- ODESC is not performing, and should not be expected to perform, the role of an Officials' committee providing peer review and assurance around Cabinet papers.
- The functions and roles of ODESC, ODESC(I) and ODESC(G) all need reconsideration.

Nearly everyone I interviewed had a clear view on the current role and structure of ODESC. In most cases this view was tempered by the current relationship between the interviewee's organisation and ODESC, and the degree of utility ODESC was seen as providing to the work of that organisation.

Some of those I interviewed wanted more support for their work from ODESC; some wanted a different form of support from ODESC. Some immensely valued a "seat at the table"; others did not consider the time commitment they made to ODESC commensurate with the value delivered to their work through ODESC. What I did hear consistently, was that ODESC has a good reputation. It is seen as an important forum and one critical to our system of national security.

It is always good to understand perceptions of current value, as a starting point. I started with the current form of ODESC and asked those I interviewed what was working well. I then asked what could be improved. I did this for the "general" ODESC monthly meeting (which some participants refer to as ODESC(P) and some refer to as "Part One", based on how the agenda is set out). I also did this for ODESC(I) and for ODESC(G), where those I interviewed were participants. I set out the feedback received, below, by ODESC "type".

ODESC/ODESC(P)

ODESC is a generic committee of chief executives of government agencies chaired by the Department of the Prime Minister and Cabinet, whose membership reflects the coordination roles of the Cabinet Committee on Domestic and External Security Coordination. Attendance at meetings of ODESC, or sub-groups it may establish, is by invitation of the Chair, depending on the matters to be dealt with or the nature of any threat or crisis.



In practice, heads of the following agencies are invited to each monthly meeting: DPMC (Chair), CTAG, Defence, Foreign Affairs and Trade, GCSB, NZDF, Police, NZSIS, Treasury, MBIE, MPI, MCDEM, Customs, Environment, Fire Service, Health, Internal Affairs, Justice, SSC, Transport, Treasury, along with the Directors of DPMC's Intelligence Coordination Group, National Assessments Bureau and Security and Risk Group.

ODESC terms of reference:

- Ensure coordinated advice to government on matters of national security, intelligence and crisis management.
- Exercise policy oversight, strategic planning, and priority setting across all matters of national security, intelligence, and crisis management.
- Oversee the development of national and sector strategies for treating major security risks, addressing critical vulnerabilities, and enhancing national resilience.
- Work to ensure that government agencies are prepared and have plans for comprehensive risk management of national security issues, including civil contingencies.
- Coordinate government's strategic response to major crises, threats or circumstances affecting New Zealand or New Zealand's interests abroad.
- Provide governance and assurance in respect of the New Zealand Intelligence Community (NZIC), with a focus on systemic governance including strategic direction, performance monitoring, oversight, priority setting, and allocation of resources.
- Facilitate interagency cooperation within the NZIC, and coordinate joint projects.

ODESC/ODESC(P) - what is working well

ODESC(P) is seen as being a particularly effective organising mechanism in times of crisis. It is the "one right door" in such events and throughout government there appears to be good recognition of ODESC's role and authority in crisis and about how crisis situations are handled.



In times of national crisis, ODESC(P) is seen as a supportive atmosphere for the “lead” chief executive. It is seen as a place that the lead chief executive can come to for discussion, without necessarily having a whole solution already mapped out. It is also seen as an effective way to coordinate advice for Ministers in times of crisis.

ODESC(P) was also seen by a number of those we interviewed as being effective in organising exercises to prepare agencies to work in crisis situations (ODESC is supported by DPMC’s Security and Risk Group in this function).

Exercises were seen as a good way to ensure plans were in place and appropriate and that everyone knew the chain of command, and the role they/their agency would play for particular type of crisis. There were some questions about whether the exercise programme covered all of the right topics – and comments that an overarching national security strategy would assist ODESC to identify priorities for exercise.

ODESC(P) was generally recognised as working well when multiple agencies had a genuine interest in one matter – for discussion at senior level, to ensure each agency has the right level of involvement in the matter, and to ensure that all relevant agencies are prepared to brief their own Ministers around papers on the matter going up to Cabinet.

ODESC(P) is seen as a place where agencies can test ideas and emerging areas of risk/work. Examples we were given included:

- MPI brought the biosecurity response guide – where ODESC members worked in partnership to form the document and made commitments around their own agencies’ involvement in responding to a biosecurity incident.
- Police brought a national organised crime paper – this led to a strategy on this topic and to the creation of OFCANZ.

“There is huge value in the simplicity of the system. Our Australian colleagues regard our system as simple, useful and effective – simple to activate – uses operational connections – people know the members and the drill.”

“It is seen as the “one place” to go, whether it’s for counter-terrorism, an earthquake, cyber security, or a ship grounding. This simplicity is valuable. ODESC proved itself during the earthquake and Rena”.

“ODESC keeps us prepared and in a state of readiness.”

“ODESC(P) lifted (the discussion on cyber security) to a broader space than the New Zealand Intelligence Community – such as MBIE, MPI and DIA. This is the value of ODESC.”



- The GCSB brought a paper on cyber security – this led to development of New Zealand's National Cyber Security Strategy, establishment of the National Cyber Security Centre and the National Cyber Policy Office.

ODESC(P) provides an opportunity for senior officials to be exposed to the national security work that other agencies are involved in, to provide information on the work of their own agencies, and to meet other senior officials working in areas related to intelligence/national security. A number of those I interviewed noted the importance of this information sharing/networking opportunity – both to improve their own agencies' effectiveness and to ensure that all the major players knew the other players in times of crisis.

“Agencies need to make conscious decisions to engage with ODESC – there's push (want to engage), and pull (ODESC asks for or requires engagement). We might need more pull from ODESC to create pressure for involvement, as agencies are so stretched, that pushing things to ODESC might not be top of mind.”

ODESC(P) was not seen as a way to replace general consultation requirements for Cabinet papers. It was generally seen as a place to seek endorsement of the recommended approach; perhaps mandate for the approach and even offers of support/resourcing by other agencies. In general those I interviewed said they would have completed “proper” consultation on their paper before it came to ODESC, including with SRG and ICG as appropriate.

ODESC(P) was seen as generating some useful actions – action points were assigned to agencies; the cluster work was established and this had led to good conversations and work on cross-agency actions.

ODESC/ODESC (P) – what could be improved

These views were expressed by the majority of those I interviewed:

- There are too many agencies around the table at the ODESC(P) meeting for it to be a useful forum for discussion. Some agencies were consistently represented by a Chief Executive or Director – other agencies had delegated their membership down as far as fourth level, leading to questions about whether they had a “decision-maker” at the table.
- The agenda was considered, overall, to be inconsistent – with items not sufficiently

“I've got no idea how I decide whether a paper goes to ODESC – there's no guidance.”



weighted and time allocations not relative to the importance of the agenda items.

- There should be more discussions of “substance” at ODESC(P) – to understand what is changing in our risk environment; what is happening in the rest of the world; to hear from those from partner countries and to hear from those outside of Government with an interest in our national security (such as major commercial organisations with an interest in their own cyber-security).
- It was noted that economic security was not often addressed directly, even though it is so critical to our way of life and so connected to other aspects of our national security decision-making (such as why we enter into particular defence arrangements).
- There are no rules or guidelines around what should come to ODESC(P) for discussion. Heads of agencies make their own decisions – some are confident that they have this right - others appeared less confident. In some cases agencies which are affiliated with ODESC(P) also have other forums for their discussions/papers, such as sector forums, working groups and officials’ committees.
- It is not clear what Ministers expect from ODESC(P) around non-crisis business. What do Ministers understand when they are told that something has “been to ODESC”? The terms of reference for this ODESC group include a role to “assist the work of the Cabinet Committee on Domestic and External Security Coordination by commissioning and organising papers, and ensuring their quality.” Those I interviewed were unsure that ODESC(P) either commissioned/organised papers or ensured their quality. It was also noted that a number of papers related to national security were prepared for Cabinet Committees other than DES. The risk here is that Ministers think “has been to ODESC” guarantees some depth of analysis by ODESC which may not have occurred.
- ODESC(P) does not perform well over single-agency issues or matters. As examples (and these did not come from the Defence agencies) – it was considered that defence engagements were a good topic for consideration at ODESC(P), but defence procurement on the other hand, was a topic that it was hard for other agencies to robustly interrogate because so few people have the knowledge required.
- There was demand for a clear sense of priorities, standing work streams, coordinated action on priorities and then reporting back against those priorities/workstreams.



ODESC(I)

ODESC (I) was a former ODESC subcommittee which met to consider issues relating to national security which have an intelligence component. Following the implementation of changes to ODESC in 2010 which established ODESC(G) the ODESC(I) terms of reference effectively became defunct. On 21 April 2010 Maarten Wevers, former Chief Executive of DPMC wrote to Chief Executives about the ODESC structure and noted: *“There is a case...for phasing out the current ODESC(I), partly because any of its functions are to be taken up in the new ODESC(G), and partly because government wants to see more direct use made of intelligence agencies across a wider range of security topics. That will not happen as readily if intelligence continues to be handled within an ODESC(I) silo.”*

In reality, there has continued to be a separate ODESC meeting to consider issues relating to national security which have an intelligence component and these items form “part two” of the monthly ODESC meeting, with some agencies leaving ODESC after “part one” (ODESC(P)), and others staying on. Even in the absence of a terms of reference, the agencies attending this “ODESC (I)” meeting seem to value the opportunity to discuss intelligence matters as a group and note the high level of commitment from those who attend.

“It’s not the “meeting” that’s the key – it’s the acceptance that there needs to be coordination and leadership around national security, and that DPMC is the natural fit for those functions.”

There was feedback about the need to weight ODESC(I) agenda items to ensure items receive the right degree of focus/time.

Due perhaps to lack of clarity about the existence/role of ODESC(I), some ODESC(P) participants wondered why they were excluded from this meeting.

ODESC(G)

ODESC(G) was established in 2011 as a result of Cabinet decisions following the *Murdoch* and *Wintringham* reviews. It has no formal terms of reference, instead taking its role from the wording of a Cabinet decision:

“ODESC(G) is charged with governance of the New Zealand Intelligence Community (NZIC). In this role, ODESC(G) oversees the performance of the intelligence community and individual agencies with respect to both domestic and



external intelligence matters. The Committee provides a mechanism to ensure there is full and effective coordination and co-operation within the NZIC, and that there is no unnecessary overlap of activities of responsibilities.

ODESC(G) acts on the Prime Minister's behalf in meeting government's responsibilities in respect of intelligence, and advises him of any action that it recommends should be taken. In order to fulfil this role, but without prejudice to very sensitive operational details, ODESC(G) is kept informed by the Directors of NZIC agencies on all relevant matters.

ODESC(G) oversees the management and conduct of New Zealand's international intelligence relationships in respect of the New Zealand intelligence community as a whole. In exercising this function, the Committee takes account of the established direct agency-to-agency relationships, while ensuring that these contribute to an effective, integrated international liaison process.²³

The current members of ODESC(G) are the leaders of the following agencies: DPMC (Chair), SSC, Treasury, NZDF, MFAT, Police, with the Directors of the ICG and NAB attending as officials. The Directors of GCSB and NZSIS are not members but attend most meetings. ODESC(G) currently meets four times each year.

Since establishment, ODESC(G) has been occupied with a number of changes for the NZIC, including work to co-locate a number of agencies in Pipitea House and to support the core intelligence agencies to deliver an efficiency dividend, joint Statement of Intent and Four year plan, with associated resourcing decisions.

There is value in having governance for the core intelligence agencies outside of the organisations themselves for at least two reasons. Firstly: by nature these are organisations which are not able to open themselves up to much external scrutiny. They are not able to be examined by Parliament in the same way that other government agencies are. I do note the upcoming PIF review of the GCSB, NZSIS and role of ICG, which will provide useful scrutiny on their fitness for purpose both today and into the future. Secondly: the agencies all currently report to the Prime Minister as their Minister. The Prime Minister has less time to ask questions relating to agency performance and sustainability than do other Ministers. ODESC(G) is

²³ DES(10)2



undertaking a governance role in lieu of the usual forms of scrutiny which other State sector agencies are subject to.

The ODESC(G) members I interviewed said that ODESC(G) had delivered some good value through its governance over the core intelligence agencies, including work around co-location, a joint Statement of Intent, 4 Year Plan and shared back-office services. It has worked hard to make changes around the intelligence community, and particularly around the core intelligence agencies working more effectively together, and all intelligence agencies coordinating their work more effectively.

A number said that ODESC(G) had been hindered by infrequent meetings, insufficient performance information on the agencies it was overseeing and lack of analyst support to analyse papers and information and advise ODESC(G). All were of the view that this form of governance was valuable for the core intelligence agencies, should continue and should be taken even further, with better support around performance information.

A number of those I interviewed also questioned whether DDI should also be designated a “core” intelligence agency, given its role in the system and work with and to support the other three core agencies. This should be considered, as should the extension of ODESC(G)’s governance role to DDI.

ODESC – what needs to change

Given the feedback received on ODESC, it seems pertinent to:

- Clarify the roles of all and any ODESC committees.
- Create an officials’ group of second-tier leaders to provide discussion, peer review and assurance over Cabinet papers, so it is clear where this function lies.
- Reduce the number of agencies at the table for each meeting, to facilitate better discussion – while ensuring the agenda is handled carefully, with invitations extended for each meeting to other agencies as appropriate.
- Trial a new regular forum serving the needs of national security agencies to receive updates, share information, meet and network.
- Ensure ODESC has sufficient advisory support for agenda/attendance management, minute-taking and analysis of performance information and accountability documents relating to the GCSB, NZSIS and NAB.



ODESC - recommendations:

The terms of reference for ODESC be changed to include responsibility for:

- Keeping the national security strategy (once developed) “alive”, including ensuring coordination of advice to government on matters of national security, intelligence and crisis management and coordination of the work programme coming out of the strategy.
- Assisting the work of the Cabinet Committee on Domestic and External Security Coordination by commissioning papers, think pieces and points for discussion and recommending an agenda for DES meetings.
- Discussing and receiving updates on intelligence matters (both policy and operational) as appropriate – with the Chair having exclusive rights to determine members’ involvement in matters relating to intelligence.
- Commissioning and overseeing a national security and intelligence public communications plan.

The membership of ODESC be changed to DPMC (Chair), Defence, Foreign Affairs and Trade, GCSB, NZDF, Police, NZSIS, MPI, MCDEM and Customs with others to attend by invitation as determined by the agenda. DPMC senior leaders to attend as officials as determined by the CE, DPMC.

ODESC to meet bi-monthly as required.

ODESC(I)

ODESC(I) is no longer required as a separate committee.

ODESC(G)

The Terms of Reference for ODESC(G) be amended so that it is the sector board for the National Security sector as well as a board focused on governance for the “core” intelligence agencies (GCSB, NZSIS, NAB).

“Agencies need to maintain public trust and confidence and establish the legitimacy of their work. The public understands defence, first responder and threat or natural disaster – but the (GCSB issue) woke up the public to GCSB. The more transparency we can have (while maintaining confidentiality where we must), the better.”



Terms of Reference to include:

- Provide governance and assurance in respect of the GCSB, NZSIS and NAB, with a focus on systemic governance including strategic direction, performance monitoring, oversight, priority setting, and allocation of resources.
- To be the sector board for the National Security sector. The sector board will include oversight around prioritisation of work within the sector, of resourcing decisions and of development of the sector.

The membership of ODESC(G) be changed to DPMC (Chair), SSC, Treasury, Defence, Foreign Affairs and Trade, GCSB, NZDF, Police, and NZSIS. Other agencies to be invited as appropriate. DPMC senior leaders to attend as officials as determined by the CE, DPMC.

That the Chief Executive of DPMC and Chief of New Zealand Defence Force meet to discuss the extension of ODESC(G)'s governance role to DDI and Geolnt NZ and make a decision to include or exclude these agencies.

ODESC(G) meet bi-monthly in alternate months to ODESC.

ODESC standing committees/working groups

The current ODESC standing committees/working groups be reviewed by the SRG and ICG for ongoing relevance.

ODESC officials' committee

A second-tier senior officials' committee be established to provide a discussion forum for, peer review and quality assurance around Cabinet papers concerning intelligence and national security matters. Membership to be second-tier managers of ODESC member agencies, and senior DPMC staff as determined by the CE, DPMC. Other second-tier staff to attend as appropriate. The DCE, National Security and Intelligence is to chair the committee - with the Chair having exclusive rights to determine members' involvement in matters relating to intelligence.

ODESC four-monthly forum

An ODESC four-monthly forum be trialled with the objectives of:

- Updating the broader National Security sector agencies on risk/threats, changes in environment and progress against the national security strategy/ODESC work programmes.
- Maintaining connections between this broader group of agencies and an understanding of the contributions made by each to national security.



- Providing a forum for agencies to showcase new initiatives, with a preference for joint/group initiatives which take a collaborative approach.
- Enabling Ministers to address leaders from the wider group of agencies.

Invitations to the forum be made to leaders of the National Security sector agencies along with relevant senior staff and high potential staff working within the sector.

Support for ODESC

ODESC and ODESC(G) receive agenda, secretariat and advisory support to carry out their functions by an advisor specifically tasked (new position).

Released under the Official Information Act 1982



The Department of Prime Minister and Cabinet

Key findings:

- National security agencies support and respect DPMC's coordination role in relation to national security and intelligence.
- Those agencies also recognise and support the role of the CE, DPMC as New Zealand's national security advisor.
- Overall, they want DPMC to take an even stronger leadership role in the national security space - to push more strongly for prioritisation, effective and efficient use of resources and for performance.
- Taking a stronger leadership role will require more senior leadership capacity and capability within DPMC. It will also require more analytical capability.
- Thought must be given to the sustainability and effectiveness of the DPMC teams working in this area, given their broad mandates and very small sizes.
- The NAB can provide even more value through support to ODESC and DES as consumers.
- The Chief Executive, DPMC, should consider the need for second review policy advice for the Prime Minister on all intelligence and national security matters.

Leadership within DPMC's national security and intelligence functions

I want to note here, right at the start, the high regard in which DPMC's second-tier national security and intelligence directors are held by their colleagues in the state sector.

The Director, Intelligence Coordination has played a critical role in changes made in the NZIC – appreciation for the coordination and support he has provided to these agencies was mentioned in every interview I conducted with an intelligence agency leader. Those leaders were very keen for this focus on development of the NZIC to continue.

The work of the National Cyber Policy Office was noted in a number of interviews – this policy work is seen as critical to our future national security.



The Director, Security and Risk Group has increasingly taken on new cross-sector work (such as the cluster work, and the start to formulation of a national security strategy), alongside a busy ongoing programme to evaluate, coordinate planning for and response to risks.

The Director, National Assessments Bureau has led work around standards of assessment and around the National Assessments Committee's broader mandate, encompassing assessments from a variety of government agencies. I am also impressed with the new NAB outreach programme and the potential here - which will require more partnering with other agencies to be fully effective for consumers.

One of the objectives of this review was to: "ensure DPMC has an optimal structure in place for the efficient and effective delivery of DPMC's coordination and leadership priorities on national security and intelligence". In considering what an optimal structure would be I have had reference to feedback received during DPMC's recent PIF review and feedback received during the interviews I conducted (which included not just leaders of intelligence and national security agencies but also representatives of consumers such as the Prime Minister's office). I have also had regard to models from our partner jurisdictions and to the needs and requirements of the CE, DPMC, as expressed by him.

DPMC's PIF review, which involved interviews with numerous stakeholders, noted that:

"We...observe that the responsibilities for security and intelligence on the Chief Executive are large and growing. We suggest that the appointment of a Deputy Chief Executive with responsibility for the security and intelligence activities might be desirable to strengthen the linkages between the defence and intelligence agencies and provide the Prime Minister with an advice stream that more formally incorporates a national security perspective."²⁴

The leaders I interviewed were firmly of the view that the Chief Executive, DPMC, is New Zealand's "National Security Advisor" and leader of the National Security sector. This was seen as a key leadership role within the system and a role that needed strengthening – it needs more teeth.

That the CE, DPMC is New Zealand's National Security Advisor (NSA) has in effect been confirmed by Cabinet in their decisions following the *Murdoch* and *Wintringham* reviews. Having this role for our system aligns us with our international partners. Our counterparts in the Five Eyes all have a National Security Advisor, with the US supplementing the role with a Director of

²⁴ PIF Report, DPMC, May 2013



National Intelligence to coordinate the vast US intelligence apparatus. In each of these jurisdictions, the success and influence of the role has been personality driven.

Australia created a National Security Advisor position in 2008. This role was created to help coordinate the intelligence bureaucracy, to provide the Prime Minister with a principal stream of advice on all policy matters relating to the security of the nation and to oversee the implementation of national security policy. I understand this position is not considered to be bipartisan and may be disestablished if there is a change of government in the next federal election.

The **Canadian** National Security Advisor position was established in 2003 and reports to the Clerk of the Privy Council. This position is responsible for intelligence and threat assessment integration and interagency cooperation, and for assisting the Minister of Public Safety and Emergency Preparedness in the development and overall implementation of an integrated policy for national security and emergencies. With a mandate to coordinate the security and intelligence activities of all Canadian government departments, the National Security Advisor is accountable to the Minister of National Defence for the policy and operations of the Communications Security Establishment.

The **UK** National Security Advisor position was established in 2010. The position is held by a civilian and heads up the National Security Secretariat, acts as the Secretary of the National Security Council and is a senior foreign policy advisor to the Prime Minister. The role's current tripartite requirements means there is the potential for duplication or divergent advice with the Foreign and Commonwealth Office, Ministry of Defence and the Intelligence Services.

The **US** National Security Advisor is appointed by the President rather than the Senate. The role is not connected administratively to the Departments of State or Defence but offers independent advice, effectively creating a policy triad that the President may rely upon for advice.

The newer Office of the Director of National Intelligence (ODNI) was established in 2005 as part of a set of sweeping changes recommended for the US intelligence establishment in the 9/11 Commission review. The Director of National Intelligence is the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. The Director's goal is to integrate foreign, military and domestic intelligence in defence of the United States homeland and its interests abroad. The ODNI's responsibilities include provision of timely and objective national intelligence to the President and relevant senior officials, establish priorities for the intelligence cycle and



standards of assessment, and coordinate overseas relationship, as well as budgetary and acquisition responsibilities.

The leaders I interviewed were unanimous in their view that the national security advisor role is a challenging role for the Chief Executive of DPMC to hold, given his other responsibilities. Their view was that the Chief Executive needed more senior-level support to deliver on this role.

I do agree that the CE, DPMC needs more senior-level support to carry out his role as New Zealand's national security advisor and as the lead Chief Executive for the National Security sector.

Ensuring that the Prime Minister is well supported and advised in relation to national security, leading a sector through formation and being the effective owner of a national security strategy will all take significant time and energy.

“The idea of having a DCE with DPMC covering the security and intelligence space is a good one – but the question is how you’d resource this. You would still need to have the Director, ICG role or the DCE will become inundated with intelligence coordination work and not get into the strategic space required to support the CE, DPMC. The credibility of the person appointed to the DCE role will be critical.”

Following further consultation, I recommend the establishment of a new, very senior Deputy Chief Executive role covering both intelligence and national security to provide support to the CE, DPMC (and subsuming the current role of Director, Intelligence Coordination). The advantage in creating such a role now is that it would give the CE, DPMC one second-tier leader with responsibility for all matters national security and intelligence. This would be an attractive, permanent role with a wide mandate, which would appeal to a number of very senior candidates and send a signal to the system about DPMC's ambition around development of the National Security sector.

The disadvantage of proceeding to create such a role now is that there is a lot of work to do to develop the NZIC, to develop the National Security sector, to work with DES differently, to bring life to a new National Security Strategy and to work differently within ODESC. The risk is that a very senior appointee will end up mired in both small and large change rather than being able to work at a strategic level. If this role is proceeded with at this time, I would recommend very senior analytical support being put in place (two new positions), to provide support to the DCE.



Support for ODESC by DPMC

The current configuration of ODESC is supported by DPMC's SRG and ICG – with SRG taking responsibility for ODESC(P) and ICG taking responsibility for ODESC(I) and ODESC(G). Both SRG and ICG have worked with limited resources to manage agendas, papers due, minute-taking and report-backs. I received feedback on the need for agendas to be more actively managed so that items are weighted – and the proposed new forms of ODESC and ODESC(G) will require effective management of attendees for relevant items. I also note feedback from ODESC(G) members around the need for analysis of performance information to support them to perform their governance role.

All of this leads me to the conclusion that a dedicated advisory role is needed within DPMC to support ODESC and its functions, including support for agenda and attendance management, secretariat support during meetings, ensuring agencies are preparing information/papers as required, seeking performance information and providing analysis of this information to support ODESC(G).

NAB's role in providing strategic all-source assessment

The terms of reference for this review required me to: “consider NAB's role in providing strategic all-source assessment and how this could be enhanced in ODESC, while retaining NAB's independence from policy making.”

Since 2010, the Director NAB, as head of the National Assessments Committee, has been responsible for development of a national assessments programme which is contributed to by all relevant parts of the NZIC. I understand that this has led to a broader variety of contributing agencies, delivering assessment on a broader range of topics.

I note that the Director, NAB is already working on enhancements to NAB's own customer service. The NAB now has a position specifically focused on “outreach”, who targets Chief Executives and Ministers who are not necessarily established customers for NAB's products, to inform them about the product available and understand what they are interested in receiving assessment on. This very positive initiative was sparked by the DPMC *Value for Money* review conducted by Dr Murray Horn, which noted that the NAB was missing opportunities to engage with customers/consumers.



I also note that the GCSB, and possibly other NZIC agencies, are also approaching customers/consumers to discuss the needs of those individuals and I wonder why there is not a coherent approach being taken by the NZIC.

“In a very small country, can NAB really be separate from policy making? We need to think about what we give to ministers and how we write so it makes sense to them. We want them to be engaged and challenged by an assessment.”

I have made a recommendation around this as part of the proposed work programme for the NZIC: *“Joint work with common consumers to establish their needs and to ensure that intelligence/assessment and policy advice are provided in tandem so Ministers receive a seamless suite of information and advice”*.

The question is how NAB’s role in all-source assessment can be enhanced in ODESC. I note that ODESC is not currently an NAB “customer”, although individual agencies around the ODESC table are. DES is not an NAB “customer”, although individual Ministers around the DES table are. In my view, ODESC and DES should be treated as primary audiences and commissioning agents for assessment work and supported to understand what they can usefully commission to support their discussions and decision-making. ODESC and DES should also be recipients of regular assessment updates created by the NAB.

The role of the Policy Advisory Group in national security/intelligence matters and the need for second-review advice

It became clear to me during the review, both through interviews with those within DPMC and outside, that the relationship between DPMC’s Policy Advisory Group (PAG) and the DPMC groups involved in national security and intelligence is not as strong as it should be.

At best this means that all the skills and experience within DPMC are not brought to bear on government priorities. At worst this is a reputational risk for DPMC with the possibility of contradictory advice being provided to the Prime Minister by two different parts of DPMC.

Given that I am already aware of the roles of the ICG, SRG, NCPO and NAB, I looked at the role of PAG. This is how DPMC describes PAG’s role:

- PAG advisors provide free and frank advice on all items of government business, including issues of the day directly to the Prime Minister and, on occasion, to other ministers.
- The Group contributes to policy development across the full range of government issues, and supports the Prime Minister in all Cabinet Committees.



- The Policy Advisory Group facilitates cross-government linkages amongst agencies working on related issues and seeks to ensure that officials' advice takes account of broader government priorities.
- Where possible the Group takes a medium to longer term view that incorporates a strategic perspective, to ensure policy coherence.
- The Group also has an important role in providing the Prime Minister with up-to-date information on emerging policy issues and giving support to his office.

There is one blind-spot in PAG's coverage – and that is intelligence policy. It seems that there has never been a PAG advisor tasked with covering this area of policy.

There are two questions here. One concerns the role of the National Cyber Policy Office in producing cyber security policy advice for government. This raises an interesting question over the positioning of the NCPO within DPMC – what process should DPMC use to ensure cyber security policy is sufficiently tested and challenged, in the way that PAG performs this role for policy produced by other agencies?

The second question concerns intelligence policy created by agencies other than DPMC. I assume that DPMC should provide second-review advice on intelligence policy for the Prime Minister. The question is whether this is properly a role for PAG, or one for the Intelligence Coordination Group (which does not currently appear to have this role, or capacity to undertake it).

Regardless of any decision made on second-review advice, PAG, ICG, SRG, NCPO and the

“The DPMC security and intelligence Directors went to the recent PAG offsite. That was great. We need more interchange to improve collaboration.”

NAB would benefit from strengthened relationships. I am advised that in the past, a representative from the equivalent of the SRG attended PAG's weekly meeting. Small changes like this can make a big difference. It is also important to consider where PAG can usefully contribute to SRG's planning work, or the national security cluster work or to strategy or response work being undertaken by ODESC where that work will have policy ramifications.



DPMC's coordination and leadership roles for national security and intelligence

Although it is outside of the terms of reference for this work, I received a number of pieces of feedback about the way that DPMC's national security and intelligence roles are organised and resourced. This feedback was given in a constructive and well-considered way and I want to note it here. The concern is that the national security and intelligence functions within DPMC are too small and fragmented to be either sustainable or as effective as they could be. The staff numbers in the various groups are:

- National Assessments Bureau - 25
- Security and Risk Group - 7
- Intelligence Coordination Group - 5
- National Cyber Policy Office – 4.5 (intended to be 7-8)

The question raised by some of those interviewed was whether the SRG, ICG and NCPO functions should be merged to create a larger group of specialists focused on national security and intelligence coordination, cyber policy and intelligence policy. The thinking here was that the small team sizes and stretch required within those teams to cover their current functions might not be the optimal operating environment for these talented public servants.

With their current configurations these teams are staffed by professionals with specialist skills – although all have core skills in common, including the ability to take a broad view of national security, to work across government in co-ordinating activity and to analyse, plan and advise. All play leadership roles across the system within their own areas of speciality.

I also note here that there is potential for the NAB to be better supported by colleague agencies with the further development of the NZIC. As an example: a move to common competency definitions and training for assessment advisors, and a more flexible assessment workforce might provide more workforce security for the NAB.

As this topic is outside of the terms of reference for this review, I make no recommendation here – simply provide this feedback for consideration.



The Department of Prime Minister and Cabinet - recommendations

New second-tier role

1 *New second-tier role - Deputy Chief Executive, National Security and Intelligence*

- Creation of a new second-tier role (Deputy Chief Executive, National Security and Intelligence) to support the Chief Executive, DPMC in his role as the lead advisor to the Prime Minister on matters of national security and intelligence.

This role would be responsible for:

- Development, maintenance and promotion of the National Security Strategy, including working with National Security agencies on delivery against the strategy.
 - Supporting ODESC around the strategy and driving the ODESC agenda around all matters relating to both national security and intelligence.
 - Supporting ODESC(G) around governance over the core intelligence agencies and development of the NZIC and the National Security sector.
 - Working with ODESC to develop the DES agenda.
 - The responsibilities of the current Director, Intelligence Coordination.
- This role would be a new direct report to the Chief Executive, DPMC. The current DPMC roles of Director, Security and Risk Group, Director, National Assessments Bureau and Manager, National Cyber Policy Office would report to this new role. This role would subsume the current role of Director, Intelligence Coordination.
 - Consideration would need to be given to senior-level advisory support for the DCE.

New advisor role – Advisor, ODESC

A new Advisor role be established with an exclusive focus on support for ODESC and ODESC(G), including support for agenda and attendance management, secretariat support during meetings, ensuring agencies are preparing information/papers as required, seeking performance information and providing analysis of this information to support ODESC(G).

NAB's role in providing strategic all-source assessment

- ODESC and DES be treated as primary audiences and commissioning agents for assessment work by the NAB and are to be supported to understand what they can usefully commission.



- Regular assessment updates created by the NAB, such as the annual National Security Contingencies Environment Scan (March ODESC), the “What could interrupt your holidays” report (early December), a scene setter on the year ahead for the Pacific (early February) and Strategic Assessment NAC (late February), be provided to both DES and ODESC as a matter of course. Where relevant, such updates should include clear information about the action/policy response government is going to take in response to risk/threat. After each such report is provided to DES and ODESC, feedback should be sought on the usefulness of the report for ODESC and DES.

The role of DPMC’s Policy Advisory Group in national security/intelligence matters and the need for second-review advice

- The Chief Executive, DPMC, put in place a process to ensure cyber security policy advice is sufficiently tested and challenged, in the way that PAG performs this role for other types of policy advice.
- The Chief Executive, DPMC make a decision about which group within DPMC (PAG or ICG) will provide second-review advice on intelligence policy, and how this extra advisory work will be resourced.
- The Director, PAG receives ODESC agendas and, with consent of the Chair, is able to attend ODESC meetings as these relate to policy development (eg – cyber policy), or concern crises likely to result in a need for policy response.



Appendix 1 – Review of Arrangements for Coordinating National Security and Intelligence Priorities – Terms of Reference

Objectives

- 1 Review the current institutional arrangements for coordinating intelligence and national security, including whether there would be added value in closer collaboration between the two sectors and, if so, what that closer collaboration would entail in terms of overall organisation and structure.
- 2 Ensure that the architecture and operation of the ODESC system is fit for purpose in terms of delivering domestic and external security leadership and coordination for the Prime Minister and Ministers.
- 3 Ensure DPMC has an optimal structure in place for the efficient and effective delivery of DPMC's coordination and leadership priorities on national security and intelligence.

Modalities

- 4 This review will reference and build on the findings of the Intelligence Agencies Review by Simon Murdoch and A National Security and Intelligence Framework by Michael Wintringham. It will also involve research and analysis, including interviews with DPMC staff and key ODESC stakeholders.
- 5 This work should include some consideration of the management structures supporting similar intelligence and national security priorities in other relevant overseas partner jurisdictions.
- 6 Based on the findings of this research and analysis, and assuming no additional resources beyond those foreshadowed in agencies Four Year Plans, the review will make recommendations to the Chief Executive DPMC about options that would be expected to achieve the objectives outlined above in paragraphs 2 and 3 (for ODESC and DPMC respectively).
- 7 The Chief Executive DPMC will consult with the Chief Executives of the ODESC stakeholder agencies and provide an opportunity for comment and feedback before



making any recommendations (based on the review's findings) to the Prime Minister and Ministers.

- 8 If changes to the present DPMC structure are recommended then a consultation process would occur with any potentially impacted managers and staff.
- 9 For the avoidance of any doubt, this review is focused exclusively on the institutional arrangements affecting national security and intelligence and will not consider any other sectors in the public service.

Context

- 10 The Intelligence Agencies Review conducted by Simon Murdoch examined how the effectiveness of New Zealand's intelligence and security arrangements could be optimised across the NZIC, and how further efficiency gains could be extracted from existing funding, so those gains could be reinvested into more effective intelligence and security capability. A key outcome from Murdoch's review was the need for closer collaboration among the three agencies in the NZIC (NZSIS, GCSB, NAB).
- 11 In recent years a range of changes have impacted on - and redefined in a broader sense - the concept of national security. These included convergences between state and non-state actors, foreign and domestic environments, and economic and non-economic interests. Addressing these challenges has required even closer working relationships between the intelligence agencies and the national security community, and especially with NZDF, Ministry of Defence and the Ministry of Foreign Affairs and Trade.
- 12 Providing greater efficiencies within the public sector is a top priority for the Government. Achieving the goals of the Better Public Services programme will require stronger collaboration between agencies (particularly in specific sectors), a focus on results, better use of technology, improved services and value for money.
- 13 The 2010 Defence Assessment and subsequent White Paper recognised that the responsibility for promoting and defending national security rested with a range of agencies, and that it would be rare for the NZDF to undertake any operation without partnering another agency in some way. The Assessment recommended an "overarching national security policy" be developed which brought together the objectives of all agencies involved in protecting New Zealand's national security.



Key Tasks

- 14 Test the hypothesis that the Government will be better served by a more effectively coordinated security sector that integrates both the national security and intelligence elements.
- 15 Consider whether the current ODESC system is fit for purpose and could be improved to deliver better results and value for the Prime Minister and Ministers, including whether intelligence could be used more effectively to support national security priorities and whether any change in DPMC's structure would better enable prompt, coherent and coordinated decision making on national security and intelligence issues.
- 16 Consider the structure and process for ODESC supporting the Prime Minister and Ministers and whether this could be enhanced, utilising relevant overseas examples where appropriate.
- 17 Consider NAB's role in providing strategic all-source assessment and how this could be enhanced in ODESC, while retaining NAB's independence from policy making.
- 18 Consider any key outcomes arising from the Performance Improvement Framework review of DPMC in respect of the Department's work on intelligence coordination and national security priorities.
- 19 Make recommendations on an optimal organisation and structure (including proposed mandates) for ODESC's domestic and external security leadership and coordination, incorporating as seamlessly as possible both the intelligence and national security elements.
- 20 Make recommendations on an optimal management structure for DPMC's coordination and leadership roles for national security and intelligence. This should include proposed mandates and proposed responsibilities for management positions and the relationship between these positions and key stakeholders.
- 21 Prepare appropriate documentation for the Chief Executive, including a draft Cabinet paper in the event of any proposed changes to the structure and operation of ODESC.



Stakeholders (apart from DPMC SLT and staff)

- Selected DES Ministers
- Prime Minister's Office
- Intelligence Agencies
- Central Agencies
- MFAT, Defence/NZDF, Police

Released under the Official Information Act 1982



Appendix 2 – List of interviews

DPMC:

- Andrew Kibblewhite, Chief Executive
- Roy Ferguson (Intelligence Coordinator, Director of the Intelligence Coordination Group and National Cyber Policy Office)
- Steve Brazier (Director, Security and Risk Group)
- Gregory Baughen (Director, National Assessments Bureau)
- NAB Assessments Managers – Section 6(a)
- Paul Ash (Manager, National Cyber Policy Office)
- Rob Mackie (Security and Risk Group)
- Pat Helm (Security and Risk Group)
- Graeme Roberts (Intelligence Coordination Group)
- Helen Wyn (Director, Policy Advisory Group)
- Mark Hickford (Policy Advisory Group)
- Ben King (Policy Advisory Group)
- Rebecca Kitteridge (Cabinet Secretary and author of *Review of Compliance at the Government Communications Security Bureau*, 2013)

Other Stakeholders:

- Ian Fletcher (Director, Government Communications Security Bureau)
- Warren Tucker (Director, New Zealand Security Intelligence Service)
- Commissioner Peter Marshall (Commissioner of New Zealand Police)
- LT GEN Rhys Jones (Chief of New Zealand Defence Force)
- COL Angela Fitzsimons (Director, Directorate of Defence Intelligence, New Zealand Defence Force)
- Andrew Coleman (Deputy Director General Compliance and Response, Ministry of Primary Industries)
- Robert Lake (Deputy Comptroller, Operations, New Zealand Customs Service)
- Nigel Bickle (Deputy Chief Executive, Immigration New Zealand, Ministry of Business, Innovation and Employment)
- Keith Manch (Director, Maritime New Zealand)
- Oliver Valins (Manager, Justice and Security team, Budget and Public Services, New Zealand Treasury)
- Paula Oliver (Advisor, Prime Minister's Office)
- Helene Quilter (Chief Executive and Secretary of Defence, Ministry of Defence)



- John Allen (Chief Executive and Secretary of Foreign Affairs and Trade, Ministry of Foreign Affairs and Trade)
- Felicity Buchanan (Director, International Security and Disarmament Division, Ministry of Foreign Affairs and Trade)
- Iain Rennie (State Services Commissioner, State Services Commission)
- Bridget White (Assistant Commissioner, State Services Commission)
- Sandi Beatie (Deputy State Services Commissioner, State Services Commission)
- Section 6(a) (Manager, Combined Threat Assessment Group)
- Huntley Wright (Manager, Development Branch, Ministry of Defence)
- Simon Murdoch (Author, *New Zealand Intelligence Agencies Review*, 2009)
- Jon Day (Chairman, Joint Intelligence Committee, United Kingdom)

Released under the Official Information Act 1982



Appendix 3 – National security and intelligence agencies

New Zealand Security Intelligence Service (NZSIS)

The NZSIS, among its many functions, is New Zealand's human intelligence (HUMINT) collection and dissemination agency. NZSIS investigates threats to our national security and works with other government agencies to ensure that threats identified within New Zealand are disrupted. It also supports the multi-agency Combined Threat Assessment Group (CTAG), as well as undertakes counter terrorism and counter espionage activities. The NZSIS conducts vetting for security clearances for all NZ government agencies.

Government Communications Security Bureau (GCSB)

GCSB is a major contributor of intercept-based foreign intelligence (SIGINT) to the New Zealand Government through its foreign intelligence collection and liaison relationships. It provides a 24/7 watch and warn function to government. The Bureau is also responsible for providing advice and expertise to ensure that the Government's official information and New Zealand's critical national infrastructure is protected from cyber threats.

Department of the Prime Minister and Cabinet (DPMC)

The DPMC has two specific intelligence components: leadership and coordination of the community through the intelligence Coordination (ICG) function and assessment by the National Assessments Bureau (NAB), as well as the Security and Risk Group (SRG – the successor to DES) and the National Cyber Policy Office (NCPO). The latter two groups are consumers of intelligence rather than assessments agencies, but both draw on intelligence in their function. The Chief Executive of the Department of Prime Minister and Cabinet is New Zealand's de facto national security advisor.

Intelligence Coordination Group (ICG), DPMC

The ICG leads collaboration within, and coordination of, the New Zealand Intelligence Community. ICG works closely with the DPMC chief Executive, providing advice that will assist in fulfilling the Chief Executive's responsibility to be accountable to the Prime Minister for the systemic performance of the intelligence community. ICG provides support to ODESC(G) in carrying out its roles of systemic governance, including performance monitoring, oversight, priority setting and allocation of resources across the intelligence community. ICG's key functions are to lead and coordinate the intelligence community for requirements, priority setting, risk management and functional performance reporting.



National Assessments Bureau (NAB), DPMC

The NAB's function is to provide policy-relevant assessments to the Prime Minister, and other ministers and senior officials, on events and developments that bear on New Zealand's interests, especially in regard to national security matters. These assessments may call on the resources of the whole intelligence community. They are coordinated with the policy and operational work of other government agencies, and are intended to support the government's national security and external relations agendas and to help inform government decision-making. Formerly the External Assessments Bureau, the Unit was renamed in 2010 to reflect a more holistic function within a more integrated NZIC. Following the Murdoch review (2009), the Director NAB has responsibility for the standard of assessment provided by the NZIC in his capacity as chair of the National Assessments Committee (NAC). This has resulted in improved coordination of the assessments programme, and provides cross-community quality assurance.

Security and Risk Group (SRG), DPMC

SRG combines policy and operational roles, and coordinates and provides leadership on a range of strategies, policies, and operations for strengthening national security and stability. It is responsible for developing a coherent, whole-of-government approach to the preparation of national security strategies. Given the evolving nature of potential security risks, work on current and emerging national security risks in order to prepare for these and to ensure risks are well understood and appropriately managed. SRG coordinates the government's response to situations that have significant consequences for New Zealand's national security or interests. On behalf of government, it provides support and coordination around all major security issues. SRG collaborated with ICG to publish New Zealand's National Security System, a document that updates the terms of reference for government decision-making on national security.

National Cyber Policy Office (NCPO), DPMC

NCPO was established in 2012, and is responsible for oversight and coordination of the development, implementation and review of national cyber security policy and strategies. NCPO also facilitates engagement with the private sector on cyber security policy issues.

Ministry of Defence (MoD)

The Ministry of Defence provides policy advice on the defence of New Zealand and its interests for the government, manages the New Zealand Defence Force's procurement programme, and supports the functions of the military. The Secretary of Defence is a core participant in ODESC



meetings and the Ministry's International Defence Relations (IDR) branch represents the Ministry in the intelligence community through the NAC process.

New Zealand Defence Force (NZDF) – Directorate of Defence Intelligence (DDI)

The NZDF has a number of intelligence units and functions. At the strategic level, the Directorate of Defence Intelligence provides military intelligence to the Chief of Defence Force, Service Chiefs of Staff and operational commanders. DDI is well connected into the New Zealand Intelligence Community and is represented at the NAC. Through DDI, intelligence collected by the NZDF's various assets can be fed into the wider intelligence community. Below DDI sits the J2 operational intelligence function, and the Air Force, Army and Navy's own intelligence capabilities. NZDF intelligence also includes the Joint Electronic Warfare Support Facility and work with the New Zealand Geoint function (in coordination with the GCSB).

Ministry of Foreign Affairs and Trade (MFAT)

MFAT supports the national security and intelligence community in numerous ways. As well as being a consumer for assessment (and, increasingly, by commissioning assessments, directing the intelligence cycle) MFAT is a key part of our national response. In the event of New Zealanders being impacted by offshore terrorism or conflict, MFAT's consular reach will be critical and MFAT will be at the forefront of any response. MFAT has a significant role in all national security clusters, and is the lead agency for territorial claims, the security of New Zealand's interests abroad, regional disasters, international initiatives and international terrorism. MFAT also provides a unique stream of reporting into the New Zealand system: through MFAT reporting from our overseas missions, foreign affairs staff and assessment agencies can gain considerable insight into governments, opposition groups and civil society.

Ministry of Civil Defence and Emergency Management (MCDEM)

MCDEM is the ministry responsible for local and nation-wide civil emergencies. It has the cluster lead for natural disasters (earthquake, tsunami, flooding or volcanic eruption) and for mass evacuations or casualties.

New Zealand Customs Service

The New Zealand Customs Service (Customs) is charged with ensuring the security of New Zealand's borders. Customs works closely with other government agencies (especially NAB, MFAT, SRG, NZDF and Immigration) on mass arrivals, and has exercised a response to a maritime mass arrival, as well as helped author (with SRG) a national contingency plan for mass arrivals. Customs has the cluster lead for border violations and the smuggling of arms and



drugs into New Zealand, and is a support agency for illegal migrants/people smuggling and transnational organised crime.

Immigration New Zealand (Ministry of Business, Innovation and Employment)

Immigration New Zealand is responsible for undertaking advanced passenger screening and investigating immigration fraud. It ensures compliance with New Zealand law around work visas and working holidays, and seeks to prevent the exploitation of foreign workers who might not understand their legal rights and obligations. It coordinates closely with Customs and the NZSIS over persons of interest seeking to enter New Zealand. The Ministry of Business, Innovation and Employment is involved in the cluster work around preserving sovereignty and territorial integrity, and has the agency lead for illegal migrants/people smuggling. Immigration supports Customs on border violations work.

Ministry of Primary Industries

MPI is responsible for fisheries, forestry and agriculture. Fisheries, in particular, is linked in with a cross-agency initiative to protect New Zealand's EEZ and our Ross Sea interests, and works closely with other parts of the National Security sector (MFAT, NZDF, NMCC and NAB). MPI is also charged with the leadership of the New Zealand biosecurity system, and is the lead agency for this cluster work, along with food safety and illegal fishing. The agency supports cluster work around economic prosperity and pandemic human influenza. The food safety authority aims to control the incidences of foodborne disease and reduce food related risks.

Maritime New Zealand (MNZ)

MNZ, along with other central and local government agencies and industry is jointly tasked with protecting New Zealand's marine environment. MNZ is responsible for maintaining a nationwide capability to respond to marine oil spills of any size. This capability was publically tested following the 2011 *MV Rena* grounding on the Astrolabe reef near Tauranga. As well as being the lead agency for work around marine oil spills, MNZ is a supporting agency for cluster work around pollution.

New Zealand Police

The New Zealand police are a crucial part of the national security and intelligence sector, and work closely with all agencies across the sector. They are the guarantors of public safety, prevent and detect financial crime, and assist in preventing counter terrorism, transnational organised crime, and cyber-crime. Police are increasingly occupying an important space in the intelligence community on organised crime assessment. The Police are heavily involved in the



cluster work: Police are the lead agency for almost all aspects of the Maintaining democratic institutions and national values cluster, which includes insurgency and paramilitary activities, terrorism, civil unrest, domestic extremism and protection of VIPs. Police provide support to the work of the other five cluster groupings.

New Zealand Treasury

As the Government's lead advisor on economic, financial and regulatory policy, Treasury, along with the Reserve Bank of New Zealand and the Ministry of Economic Development, is responsible for ensuring New Zealand's economic security. Treasury is involved in cluster work around sustaining New Zealand's economic prosperity.

Ministry of Health

The Ministry of Health is responsible for improving, promoting and protecting the health of all New Zealanders. It is involved in the cluster work around Ensuring public safety, as the lead agency for pandemic human influenza, a public health crisis and chronic disease. The Ministry of Health is also a key stakeholder in the response to civil emergencies such as an earthquake or flooding.

Ministry for the Environment

The Ministry for the Environment supports New Zealand's economic prosperity through management systems for our natural resources. Environment is involved in cluster work on protecting the natural environment, specifically environmental catastrophe and pollution.

New Zealand Fire Service

The Fire Service is an integral part of New Zealand's emergency response apparatus. They are involved in cluster work around natural disasters and mass evacuation.

Department of Internal Affairs

The Department of Internal Affairs is a peripheral player in the National Security sector. It is involved in the cluster work on economic prosperity, where it is the lead agency for internet manipulation or restraint. It is a support agency for cyber security work and VIP protection.

Ministry of Justice

The Justice Ministry is the lead agency for the maintaining democratic institutions and national values cluster. It is also the lead agency on transnational organised crime.



State Services Commission

The State Services Commission is involved in the maintaining democratic institutions and national values cluster. More broadly, the Commission has a role in ensuring the National Security sector is performing well.

Ministry of Transport

MOT is responsible for the security of New Zealand's transport networks. Within the economic prosperity cluster, MOT is the lead agency for public transport failure and international sea lane and air lane closure.

Released under the Official Information Act 1982



Appendix 4 – Draft National Security Strategy Terms of Reference - 9 April 2013

Purpose

The National Security Strategy outlines the actions the Government will take to manage and reduce the principal national security issues faced by New Zealand. National security processes support a decision making framework that assists the government in identifying significant national security objectives and actions through:

- A regular assessment of the risk environment
- The identification and prioritization of risk management strategies
- The Ongoing review of the effectiveness of these actions

Inputs

An ongoing assessment of 'all risks and/or issues' facing New Zealand in these categories:

- Preserving sovereignty and territorial integrity;
- Strengthening international order to promote security;
- Sustaining economic prosperity;
- Maintaining democratic institutions and national values;
- Ensuring public safety;
- protecting the natural environment.

Outputs

- Coordinated advice to government on matters of national security, intelligence and crisis management
- Policy oversight, strategic planning, and priority setting across all matters of national security, intelligence and crisis management
- The development of national and sector strategies for treating major security risks. Addressing critical vulnerabilities, and enhancing national resilience
- Assurance that government agencies are prepared and have plans for comprehensive risk management or national security issues, including civil contingencies
- Support for the coordination of the governments strategic response to major crises, threats, or circumstances affecting New Zealand or New Zealand's interests abroad
- The Prime Minister and the Cabinet Committee on Domestic and External Security Coordination are suitably advised by commissioning and organising papers of appropriate quality
- Support for Better Public Services (BPS) goals.



Governance

ODESC is made up of CEs from key agencies. The Senior Officials Committee (SOC), a subcommittee of ODESC. The Security and Risk Group of DPMC is the secretariat, chairs the meetings and is responsible for general oversight of the process, the preparation of annual reports and periodic reporting to Ministers and DES.

Process

National Security assessments are carried out by the government agencies with particular responsibilities in these areas. Each category represents a clustering of issues and risks with a common theme. A lead agency and supporting agencies meet regularly, but no less than every two months, to assess issues and risks, review the effectiveness of their mitigation and management, and to identify changes in their relative significance. Lead agencies prepare a formal annual report on the situation in their clusters. Each lead agency is responsible for the effectiveness of the oversight process in its cluster.

A Senior Officials Committee (SOC) drawn from the lead agencies, and with two external members, meets every two months to discuss progress. An annual report from the SOC is sent to ODESC and then to DES.

Annual report and five yearly appraisals

The Annual report is a framework for the critique of existing policies and the identification of the actions the government is taking to ensure that over a five year period the nation will be more resilient in the specific areas of risk and opportunity, that priorities have been reassessed where necessary and that sufficient resources have been allocated to ensure success.

Stakeholders

Prime Minister, Cabinet, Members of Domestic and External Security (DES) Committee, ODESC, SOC, Lead agencies, supporting agencies.



Appendix 5 – References

Departmental/Sectoral Reviews

- *Better Public Services Advisory Group Report*, November 2011
- *Department of the Prime Minister and Cabinet Performance Improvement Framework Report*, May 2013 (NB – this is yet to be published)
- Horn, Dr Murray, *Department of the Prime Minister and Cabinet Value for Money Review*, August 2012
- Kitteridge, Rebecca, *Review of Compliance at the Government Communications Security Bureau*, March 2013
- Murdoch, Simon, *Report to the State Services Commissioner: Intelligence Agencies Review*, June 2009
- Wintringham, Michael, *A National Security and Intelligence Framework for New Zealand*, September 2009.

National Security Documents

- *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2011
- *New Zealand's National Security System*, May 2011
- *Strong and Secure: A Strategy for Australia's National Security*, January 2013
- *Securing an Open Society: Canada's National Security Policy*, April 2004
- *United States National Security Strategy*, May 2010

Academic Articles

- Moore, Mark, *The Public Value Scorecard: A Rejoinder and an Alternative to "Strategic Performance Measurement and Management in Non-profit Organizations" by Robert Kaplan*, The Hauser Centre for Non-profit Organizations, The Kennedy School of Government, Harvard University, May 2003, Working Paper 18
- Whibley, James, "One Community, Many Agencies: Administrative Developments in New Zealand's Intelligence Services", *Intelligence and National Security*, February 2013



Appendix 6 – Glossary

BPS	Better Public Services
Clusters	The national security multi-agency “cluster” work currently underway
CTAG	Combined Threat Assessment Group
Customs	New Zealand Customs Service
ERD	Cabinet External Relations and Defence Committee
DDI	Directorate of Defence Intelligence
DES	Cabinet Committee on Domestic and External Security
DIA	Department of Internal Affairs
DPMC	Department of Prime Minister and Cabinet
Five Eyes	Australia, Canada, New Zealand, United Kingdom, United States
GCSB	Government Communications Security Bureau
ICG	Intelligence Coordination Group
ISED	International Security and Disarmament Division
MBIE	Ministry of Business, Innovation and Employment
MCDEM	Ministry of Civil Defence and Emergency Management
MFAT	Ministry of Foreign Affairs and Trade
MfE	Ministry for the Environment
MoD	Ministry of Defence
MOH	Ministry of Health
MOJ	Ministry of Justice
MOT	Ministry of Transport
MPI	Ministry of Primary Industries
MNZ	Maritime New Zealand
NAB	National Assessments Bureau
NAC	National Assessments Committee



NCPO	National Cyber Policy Office
NCSC	National Cyber Security Centre
NMCC	National Maritime Coordination Centre
NSA	National Security Advisor
NSC	National Security Council
NZDF	New Zealand Defence Force
NZFS	New Zealand Fire Service
NZIC	New Zealand Intelligence Community
NZSIS	New Zealand Security Intelligence Service
ODESC	Officials Committee for Domestic and External Security Coordination
ODNI	Office of the Director of National Intelligence (US)
OFCANZ	Organised and Financial Crime Agency New Zealand
PAG	Policy Advisory Group
PIF Review	Performance Improvement Framework Review
SEC	Cabinet Committee on State Sector Reform and Expenditure Control
SRG	Security and Risk Group
SSC	State Services Commission

Released under the Official Information Act 1982