Hazard Risk Board Terms of Reference

Final – February 2019

Introduction

1. The National Security System is the arrangement by which the New Zealand Government identifies and mitigates risks to national security. A foundation of this arrangement is the Officials' Committee for Domestic and External Security Coordination, which meets both in response mode (ODESC) and in strategic risk management mode (through two chief executive level boards – the Hazard Risk Board, and the Security & Intelligence Board).
2. These terms of reference relate to the Hazard Risk Board (HRB).

Vision

3. A resilient New Zealand that reduces the risk of, prepares for, responds to, and recovers from, the impacts of natural hazards and civil contingencies.

Purpose and Role

4. HRB exists to build national resilience in the face of national security risk; particularly by coordinating government's responsibilities to manage hazard risk, providing assurance that capabilities for risk management are fit for purpose, and enabling the government to function effectively in the face of "all risks".
5. HRB's responsibilities include the strategic governance and stewardship of New Zealand's emergency management system (EMS) – a sub-system of the NSS.
6. HRB will contribute to the wider leadership of the NSS by working collectively to achieve coordinated strategic governance of the risks for which HRB members are accountable. From time to time, this may require coordination with Security & Intelligence Board (SIB) members, and/or other parts of the NSS.

Responsibilities

7. HRB will strive for continuous improvement of the NSS by:

   a. Ensuring that New Zealand's external and internal environment is regularly reviewed in order that emerging risks are identified and the status of current risks are routinely monitored.

   b. Providing collective and system support to individual risk coordinating agencies – by ensuring that risks are holistically evaluated and measured.

   c. Ensuring that in respect of system efforts to build resilience there is alignment between system and agency priorities, investments and policies.

   d. Proactively sharing information and draft policy options, relevant to risks governed by HRB, in order to maximise opportunities for collaborative risk management and messaging.

   e. Providing coordinated advice to Ministers on national security issues and policy relevant to HRB's focus.

f. Providing strategic leadership of the EMS and connecting it with other parts of the NSS as appropriate.

g. Agreeing priority work areas and outcomes for the NSS (including the EMS), which:

   i. Effectively manages risks for which HRB agencies have responsibility

   ii. Clarifies roles and responsibilities across the system

   iii. Builds system capability

   iv. Improves interoperability of system components.

h. Testing and challenging the advice and initiatives coming out of the system to ensure actions are aligned to system outcomes.

i. Championing, supporting and driving system initiatives led by member agencies. HRB will connect the right parts of the system, and effectively address blockages.

j. Reporting annually (or as otherwise directed), to the appropriate Minister(s)[1] about the management of risks governed by HRB, and the strategic-level performance of the EMS.

k. Supporting the development of new initiatives to enhance system performance, including supporting "orphan" projects where there is assessed to be a likely system-level benefit.

Guiding Principles

8. The HRB's work is underpinned by the following principles:

a. *He tāngata* – We recognise that everything we do has the potential to impact on New Zealand communities and individuals, and that some communities and individuals are more vulnerable than others to negative impacts. We strive to deliver equitable outcomes, and to ensure New Zealanders can go about their daily business confidently, free from fear, and able to make the most of opportunities to advance their way of life.

b. *Strategic system focus* – We prioritise system interests above the interests of individual agencies. We recognise that the pooling of resources among agencies with common strategic challenges achieves optimisation of capability in certain circumstances. We rarely (if ever) dip into day-to-day operational issues.

c. *Risk-based* – We focus on the critical and complex areas that require collective resolution both in the short and long term. Criticality is based on evidence drawn from across the system.

d. *Balance* – We take an "all hazards, all risks" approach across each part of the "4Rs" emergency management framework.

e. *Collegiality* – We actively build and maintain supportive relationships across the NSS, so that opportunities to build New Zealand's resilience are proactively identified and acted upon in a collaborative and coordinated manner. We act as "critical friends" to one another.

f. *Accountability* – We are accountable to Ministers and the New Zealand public, where relevant through governing Boards, for our performance as a collective. We are

[1] This will typically be the Minister with responsibility for National Security, or the Minister of Civil Defence where it is about the EMS.

transparent about our challenges and achievements, and we set indicators (in consultation with Ministers) to measure and report on our performance.

g. *Learning culture* - We are not afraid to have difficult discussions. We identify, understand and apply insights learned from exercises and real-life challenges for the benefit of the system.

Funding

9. We recognise that the pooling of resources among agencies with common strategic challenges achieves optimisation of capability in certain circumstances. We have adopted a "shared responsibility" model based on the State Services Commission's System Design Toolkit. As such, within the defined ability of the respective organisations, HRB will fund system initiatives through any combination of:

   a. Joint resourcing (staffing) of shared functions,

   b. Individual agencies committing to specific activities and funding these from baselines,

   c. Agencies each contributing agreed funding amounts, or

   d. Agencies pooling underspends.

Board Composition

10. HRB members will include:

   a. The Chief Executives of the following agencies (or their delegates):

      i. Department of Internal Affairs (DIA)

      ii. Department of the Prime Minister and Cabinet (DPMC)

      iii. Fire and Emergency New Zealand (FENZ)

      iv. Ministry for the Environment (MfE)

      v. Ministry for Primary Industries (MPI)

      vi. Ministry of Business, Innovation and Employment (MBIE)

      vii. Ministry of Civil Defence and Emergency Management (MCDEM)

      viii. Ministry of Foreign Affairs and Trade (MFAT)

      ix. Ministry of Health (MoH)

      x. Ministry of Transport (MoT)

      xi. New Zealand Defence Force (NZDF)

      xii. New Zealand Police (NZP).

11. The Chair of the Board will be appointed by the Chief Executive of DPMC, in his or her capacity as Chair of ODESC.

12. New agencies may be invited to join HRB. This will be documented appropriately, and noted in any future refresh of this Terms of Reference.

13. Non-member government agencies, non-government organisations and private sector entities may be invited to attend HRB meetings in support of specific agenda items, by agreement with the Chair.

HRB Secretariat

14. DPMC's NSS Directorate (NSSD) provides the HRB Secretariat. The Secretariat supports HRB's work programme, leads key strategic projects and champions system-wide collaboration. It also provides the Board with administrative support services and policy advice, and reports against any Board performance measures.
15. The Secretariat will act as a coordination and liaison point for the Board as needed.

HRB Meetings

16. HRB meetings will be held approximately six times per year. The Chair may call additional meetings as needed, and any HRB member may ask the Chair to call a meeting outside of the forward meeting calendar.
17. Consideration of issues and related decisions may be made outside of formal meetings as required, if this is documented by the Chair (either a record of conversation, or an email trail) and retained by the Secretariat.
18. The Chair may exercise a casting vote in the event of any deadlocks.

Agenda and Papers

19. Procedures for the submission of papers are noted in Annex 1.
20. Agencies will put forward agenda items, with the Chair determining the final agenda.
21. With the exception of items raised in 'General Business', all agenda items are to be supported by a paper prepared by the sponsoring agency.
22. Late papers will only be accepted in exceptional circumstances and only by agreement between the member agency CE and the HRB Chair directly.

HRB Senior Officials Group

23. A Senior Officials Group (SOG), chaired by the HRB Secretariat, will support HRB.
24. The SOG's purpose is to support the HRB's work programme by managing the forward agenda, and ensuring that the work programme and related action items are managed appropriately.

HRB's Work Plan

25. HRB's existing focus areas were retired on 30 June 2018 and will not be replaced by new focus areas.
26. HRB may commission specific time-bound projects, if the objectives, deliverables, accountabilities and resourcing mechanisms are clearly defined by the sponsoring member(s) and agreed by HRB.

Accountabilities

27. The HRB reports through the Chair of ODESC to the Minister with responsibility for National Security, as well as other EMS Ministers as appropriate.
28. Completed action items will serve as HRB's primary deliverables, with credit given to the lead and supporting agencies as appropriate.
29. The HRB Secretariat will coordinate the delivery of a concise annual report about HRB's risk management activities, in consultation with the HRB SOG.
30. Where possible, the timing of the annual report will be aligned with that of SIB.

Annex 1: HRB Procedures

Paper Submission Requirements

31. The originating agency is responsible for consulting all papers with HRB SOG members, and with any other appropriate agencies, before papers are finalised and submitted to the Secretary.
32. Final papers are to be submitted to the HRB Secretary at least 10 working days before the relevant HRB meeting.
33. Submitting agencies should identify what they wish HRB to do with each paper, bearing in mind that the "value-add" of an HRB meeting is the opportunity for members to discuss and test thinking about sector-related risk management and proposed courses of action, and provide guidance to member agencies.
34. The final agenda and papers for each meeting will be circulated by the HRB Secretary no later than 5 working days before the relevant HRB meeting.
35. All papers must have a cover sheet. Cover sheets may be prepared by the submitting agency, or by the HRB Secretary in consultation with the submitting agency.
36. HRB papers should generally use the templates provided by the Secretary, but it is recognised that this may not always be possible (e.g. if HRB is considering a document that has been published by a third party, or if a different format – such as an A3 – is more beneficial for a particular item).

Circulation of meeting Minutes

37. Draft minutes and action points will be circulated by the HRB Secretary no later than 5 working days after the relevant HRB meeting.
38. The HRB Secretary will send letters to members confirming meeting action points, no later than 10 working days after the relevant meeting.
39. Any proposed amendments to the minutes may be raised with the Secretary, or at the following HRB meeting. The Chair's decision on minutes' content is final.

Terms of Reference for the
National Agencies’
Incident Management Reference Group (IMRG)

December 2017

‘Building a resilient National Security System’

1. Purpose & Brief

Purpose

This document details the terms of reference for the National Agencies' Incident Management Reference Group (IMRG). This group is one of the committees reporting to the Hazard and Risk Board (HRB)as part of the National Security System.[1] Synergies exist with some of the other National Security committees such as the National Exercise Programme (NEP).

The purpose of IMRG is to provide an information sharing forum for central government agencies that have, in emergency events, an Incident Management Team operating at a national level. The group is also intended to provide a 'joint voice' or incident management 'industry' group to represent the sector as well as an information sharing and support network.

Many agencies involved in the Group are working on similar issues and so the aim of the Group is to for members to be able to share initiatives and to be able to work 'smarter' together. As a conduit into the government agencies, the group will also work on various joint initiatives or deliverables as and when required. These initiatives may be self-generated or requested by HRB.

Objectives

The objectives of the Group include[2]:

1. Sharing IMT initiatives and experience that may be of relevance or interest to other members.
2. Sharing training and development opportunities for National Controllers or other IMT positions, including facilitating the coordination of exercises.
3. Sharing of lessons from live events or inter-agency exercises.
4. Assisting agencies by providing ideas and advice on agreed issues, such as the establishment of a national IMT cadre or ways in which best practice Planning and Intelligence could be developed and promulgated.
5. Act as an operational coordinating group for the National Security System (excluding Counter-Terrorism.)
6. Represent the incident management / emergency management sector as an industry group
7. Carrying out relevant work on behalf of the HRB in the interest of the wider state sector

[1] National Security System Handbook, 2016, pg 17

[2] Discussion during the meeting in Feb 2013 favoured this Group filling some of the coordination 'gaps' that are not addressed in other multi-agency forums.

8. Other objectives that may be agreed by the Group.

2. Structure

Membership

Membership is open to central government agencies that have a role to play in establishing and coordinating an Incident Management Team operating at national level. This includes but is not limited to:

- Department of Prime Minister and Cabinet
- Department of Corrections
- Fire and Emergency New Zealand
- Ministry of Business, Innovation & Employment
- Ministry of Civil Defence and Emergency Management
- Ministry of Culture & Heritage
- Ministry of Foreign Affairs & Trade

Membership cont.

- Ministry of Health
- Ministry for Primary Industries
- Ministry of Transport
- Ministry of Social Development
- New Zealand Customs Service
- New Zealand Defence Force
- New Zealand Search & Rescue Secretariat
- New Zealand Police
- New Zealand Transport Agency
- Maritime New Zealand
- Oranga Tamariki / Ministry for Vulnerable Children

More than one representative is permitted in order to build resilience into the group.

The representative from each agency should be a member of staff who is:

- Experienced in incident management
- Aware of the incident management initiatives ongoing within their own agency
- Able to influence incident management within their own

agency.

- Able to distribute IMRG material within their organisation.

Chair and Secretariat support

The role of Chair & Secretariat can be rotated between interested agencies

3. Meetings

Meeting frequency and location

The National IMT Group will meet two monthly. Each meeting will be hosted by a different agency, on a rotating basis.

Meeting format and Agenda

The meeting will follow a general template of:

- Introductions / Attendees
- Apologies
- Clarification of previous meeting notes and any action points
- Updates on any joint projects
- Presentations or topics to discuss or as agreed
- Agency updates relevant to the objectives
- General business
- Next meeting and venue

Each meeting will provide an opportunity for networking, normally through a 'morning tea' break occurring during the meeting. Host agencies will be responsible for providing this.

Agendas will be distributed by the secretariat at least five (5) days prior to the meeting.

Items for the agenda will ideally be with the chairperson at least two weeks before the meeting.

Meeting notes

Meeting notes (rather than formal minutes) will be distributed within one week of the meeting.

Costs

1. Agencies will meet their own costs of participation.
2. The Chair and secretariat will meet secretariat and associated costs.

3. The host of each meeting (rotating through agencies) will meet the costs of hosting the meeting and also any costs associated with liaison with the Chair and secretariat regarding the agenda etc.

4. Joint Initiatives or Deliverables

Projects

From time to time IMRG may be asked by HRB or of their own volution, to carry out research or complete projects on relevant issues. Sub-committees may be formed to work on such issues before presenting to IMRG for validation. This work can be presented to HRB for noting or seeking further action.

5. Record Keeping

Shared workspace

Meeting notes, agendas and any other relevant documents will be held within an IMRG shared workspace in EMIS hosted by the Ministry of Health. s9(2)(g)(ii)

6. Governance

The IMRG is a sub-committee of the HRB. Accordingly, the Chair is responsible for reporting back to the HRB on any initiatives assigned to it by the Board as well as provide an annual report.

DEPARTMENT *of the*
PRIME MINISTER *and* CABINET
Te Tari o Te Pirimia me Te Komiti Matua

Maritime Security Oversight Committee

Terms of Reference

June 2016

Vision

1. New Zealand's maritime interests are secure.

Principles

2. The maritime domain encompasses anything on, under, relating to, adjacent to, or bordering a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances that impact on New Zealand's interests.
3. New Zealand's maritime interests include sovereignty, resource management, law enforcement, maritime safety, environmental protection and the maritime economy.
4. The following principles will guide, and provide a framework for, the work carried out by the Maritime Security Oversight Committee (MSOC):

    - **Collaboration** - We ensure that we collaborate across agencies, including strategic policies, strategies and initiatives. Owners and operators of critical maritime infrastructure and resources are considered partners in achieving the security of New Zealand's maritime interests;
    - **Maritime domain awareness**[1] - establishing, understanding and maintaining an accurate and comprehensive national maritime operating picture (a single point of truth) is a priority activity;
    - **Protection of maritime interests** - New Zealand needs to undertake a range of activities to protect our sovereignty and sovereign rights, resources, critical infrastructure and the marine environment to reduce the incidence and impact of any intentional or accidental activity or harm;
    - **Management of New Zealand's maritime interests** - New Zealand needs to maintain an ability to mitigate or eliminate a detected maritime security threat.

Purpose

5. The primary function of MSOC is to support the Hazard Risk Board through effective oversight of national maritime security arrangements, namely:

- Overseeing the implementation of the national maritime security strategic framework (known as Te Kaitiakitanga o Tangaroa, Guardianship of New Zealand's maritime waters);
    - ○ Aligning of strategies contained in the maritime component(s) of the accountability documents for the agencies involved;
    - ○ Developing a shared awareness and understanding of New Zealand's maritime interest and any activity that impacts upon them;
    - ○ Effective coordination of planning, investment and operational activity amongst agencies.

[1] Maritime Domain Awareness is the effective understanding of anything in the global maritime environment that could impact on New Zealand's security, safety, economy or the environment.

6. MSOC also acts as a Board of Directors for the National Maritime Coordination Centre.

Members

7. MSOC will be Chaired by the Secretary of Transport and will include deputy-secretary level representatives from the following agencies:

   Core membership: (Accountable agencies leading lines of work)

   - Ministry of Transport
   - Department of Conservation
   - Department of the Prime Minister and Cabinet
   - Maritime New Zealand
   - Ministry for Primary Industries
   - Ministry of Business, Innovation & Employment
   - Ministry of Defence
   - Ministry of Foreign Affairs and Trade
   - New Zealand Customs Service
   - New Zealand Defence Force
   - New Zealand Police

Wider membership: (*ex officio*)

- Government Communications Security Bureau
- GEOINT New Zealand
- National Maritime Coordination Centre
- New Zealand Security Intelligence Service

8. Agencies within MSOC will be responsible for the ownership of certain deliverables. These will be agreed by the Committee.
9. Other agencies, non-government organisations, and private sector entities will be invited according to the agenda.

Expectation of members

10. Members of MSOC must ensure the committee acts in a manner consistent with this Terms of Reference.
11. Members are expected to regularly attend meetings and support MSOC related work outside of meetings.
12. MSOC will operate as a collective, rather than operating as committee of individuals representing various constituencies. Members are expected to examine issues before MSOC from a strategic viewpoint, support a consensus decision-making approach and support and endorse the decisions of the MSOC.
13. Members are appointed as individuals with knowledge and expertise of the maritime security sector. They are expected to use their networks to understand and communicate the views of the sector, but are expected to govern on behalf of all stakeholders.

14. The Chair of MSOC is expected to:

    - Facilitate meetings;
    - Manage communications;
    - Ensure the objectives of MSOC are achieved;
    - Build good working relationships with members and the wider maritime security sector.

Committee performance

15. The Chair of MSOC is required to report to the Hazard Risk Board on the performance of the Committee on a regular basis, typically annually.

Meetings

16. MSOC meets quarterly with additional meetings called by the Chair if needed. Consideration of issues and related decisions can be made outside of formal meetings as required.

17. Meetings will follow an agenda which, along with supporting papers, is to be circulated a week in advance of the relevant meeting to allow MSOC to operate effectively.

18. Minutes of meetings and a record of decisions made will be kept and confirmed at the next meeting of MSOC.

Secretariat

19. The MSOC secretariat is currently provided by the National Security Systems Directorate of the Department of the Prime Minister and Cabinet. It acts as a co-ordination and liaison point for MSOC.

20. The secretariat is supported by the Joint Maritime Advisory Group (JMAG).

Joint Maritime Advisory Group

21. MSOC and the secretariat are supported by the Joint Maritime Advisory Group (JMAG). JMAG is a standing multi-agency group responsible for driving the various all-of-government maritime security work streams.

22. Membership of JMAG will be senior officials from MSOC agencies. Additional agencies may be included to reflect the interests and expertise across the sector.

NATIONAL EXERCISE PROGRAMME
INTERAGENCY CAPABILITY BUILDING

National Exercise Programme Planning and Coordination Team Terms of Reference

Purpose

This document details the Terms of Reference for the inter-agency National Exercise Programme (NEP) Planning and Coordination Team, including the background; role; objectives; membership; expectations for team members; governance and reporting; meetings; costs; and review cycle.

Background

The National Exercise Programme (NEP) builds capability across government through a coordinated series of inter-agency readiness activities that underpin the resilience of New Zealand's national security system.

The Officials' Committee for Domestic and External Security Coordination (ODESC) approved the establishment of the NEP in 2013. ODESC noted that this programme built on the experiences of the Police-led build up to the 2011 Rugby World Cup (RWC11) and that it would provide the basis for building Government capacity in the lead up to the major events that were to occur during 2015.

ODESC also agreed that a series of activities pertinent to the hosting of major events in New Zealand in 2015 would be developed to build on the 'lessons learned' from the RWC11, with a view to establishing a programme for sustaining all-of-government security response capability up to and beyond 2015. This led to the establishment of the NEP and the creation of supporting Objectives and Key Performance Indicators (KPIs) – not threat-specific and enduring across all national-level exercises (attached as Annex A).

ODESC directed that future activities will, where possible, incorporate and /or build on existing exercises being held by agencies to meet their own individual capacity building requirements.

Role

The role of the NEP Planning and Coordination Team is to maintain oversight of nationally significant exercises developed within the NEP framework approved by ODESC in 2013; to support national exercising consistency and reduce duplication of effort; and to provide guidance to agency-led exercise writing and planning groups. It plays a critical part in ensuring that all national exercises are designed to a high standard and that information is communicated in a timely manner in order to facilitate good exercise planning amongst all agencies.

The NEP Planning and Coordination Team also serves as a platform for connectivity, mentoring and relationship-building between agencies.

Objectives

The objectives of the NEP Planning and Coordination Team are:

- To ensure there is coordination of effort, and that efficiencies on resource sharing and capacity building are being effectively and efficiently managed across government.

- To assist lead agencies in developing exercises that are based on scenarios which would require a National Security System activation, in order to test the roles and responsibilities, communications and complex decision-making which is required in those activations.[1]

- To ensure that the Interagency NEP Objectives remain fit for purpose and usable.

- To make sure exercises are designed to allow both lead and support agencies to exercise appropriately against the Interagency NEP Objectives.

- To ensure that all of the Interagency NEP Objectives are being exercised across the NEP exercise cycle – that is, while each exercise may not focus on meeting all of the objectives, subsequent exercises should ensure those that have not been practiced are incorporated into planning and development.

- To maintain progressive exercise development, using the 'crawl, walk, run' methodology across the programme, to ensure that agencies are not jumping straight into the "big ones" without the proper training and information base being built along the way.

- To work closely with the Incident Management Reference Group, the National Security System Training and Development Group and the DPMC National Risk Unit to ensure that:

    - Issues/lessons learned surfaced at IMRG can be incorporated into the NEP as needed.
    - Training opportunities are made known to agencies to assist in preparing for exercises and are linked up with lessons learned.
    - The government's risk management priorities are being incorporated appropriately.

- To ensure that inter-agency exercises developed for the four-year NEP cycle are in line with the priorities for the National Security System as a whole, as well as with other strategic priorities and commitments.

- To ensure that the interagency NEP exercise documentation/templates remain fit for purpose, accessible and usable.

- To build capability by sharing of lessons identified from individual agencies' events and exercises, and to ensure visibility of lessons learned from NEP exercises for incorporation into exercise planning for both future NEP exercises and agency internal exercises.

Membership

The NEP Planning and Coordination Team has representatives from the following agencies:

- Department of Prime Minister and Cabinet (as Chair NEP)
- New Zealand Police
- Ministry of Civil Defence & Emergency Management
- New Zealand Defence Force
- New Zealand Customs
- Fire and Emergency New Zealand
- Ministry of Health

[1] This is to distinguish from individual agency exercises, which often require multiple government agencies to participate, but which do not necessarily meet the criteria for a National Security System response (found on page 12 of the "National Security System Handbook, August 2016".

- Ministry of Primary Industries
- Ministry of Foreign Affairs and Trade
- Ministry of Transport
- Maritime New Zealand
- Ministry of Social Development
- Ministry of Business, Innovation and Employment
- New Zealand Search and Rescue Council

Other agencies will be included should they be designated the lead for an NEP exercise, and/or for their expertise as required.

Expectations for members

Ideally, the representative from each agency should be a member of staff who is:

- Experienced in exercise planning
- Aware of the exercise activity within their own agency in the context of their agency's overall priorities; and
- Able to influence exercise planning and development within their own agency.

Members of the NEP Planning and Coordination Team will:

- Seek to provide continuity of membership through attendance at monthly meetings;
- Identify timing changes, priority changes and resource constraints for their NEP exercises as early as possible to inform decision-making;
- Be willing to contribute to the work of the planning team (within and outside of planning team meetings), including the debate and decision making;
- provide expert guidance within the planning team when an issue which falls under their particular area of expertise is under discussion;
- contribute to the debate in the capacity of a well-informed professional where the issue does not fall within their expertise;
- ideally have the authority to make decisions and commit resources to the exercise on behalf of their agency;
- Not be an exercise player, if possible, but seek to undertake roles such as Exercise Control during the exercises; and
- Come prepared to share lessons learned from their individual agency exercises to incorporate into NEP exercise planning as relevant.

Reporting

The NEP Planning and Coordination Team will report to the Hazard Risk Board annually on the overall progress on national capacity building through the NEP series of exercises. Other reports will be provided as needed (for example, for strategic direction regarding the four-year exercise cycle, themes from lessons learned regarding agencies' capability etc).

Formal reporting on specific exercise development progress is the responsibility of the lead agency. Exercise updates will be communicated to all participating agencies by the lead agency, but can also be distributed through the NEP Chair.

Meetings

Meetings will be held monthly. There will be four governance meetings per year, chaired by DPMC (as Chair of the NEP). The other meetings will be planning meetings, chaired by the agencies who have the lead for the next two-three exercises to occur within the cycle.

A forward agenda will be developed by the NEP Chair to help guide lead agencies in developing agendas for the planning meetings, but the goal is for lead agencies to drive those agendas, to identify issues for discussion that will meet the specific planning needs for their upcoming exercises.

Costs

Agencies will meet their own costs of participation. The host of each meeting (rotating through agencies) will meet the costs of hosting the meeting and also any costs associated with liaison with the Chair and secretariat regarding the agenda etc.

Resources

The following documents provide useful ready reference for the NEP Planning and Coordination Team:

- The CDEM Exercises – Director's Guideline for Civil Defence Emergency Management [DGL 010/09] for exercise planning.
- The Guide to the National Civil Defence Emergency Management Plan 2015 – sets out the arrangements and roles and responsibilities of agencies for the national management, or support to local management, of civil defence emergencies.
- National Counter Terrorism (CT) Plan (2006). Hardcopy available only.
- National Contingency Plans (e.g. Mass Arrivals Control and Processing Plan, Mass Casualties Plan etc).

Review

These Terms of Reference will be reviewed by the NEP Planning and Coordination Team every two years. They will be submitted for consideration and agreement by the Hazard Risk Board members to ensure appropriate oversight is maintained.

ANNEX A - INTERAGENCY NATIONAL EXERCISE PROGRAMME OBJECTIVES (2013)

National Objectives	Training Objectives	Key Performance Indicator
NO 1.0 Lead a coordinated interagency response to major security incidents including overseas agencies where necessary.	**TO 1.1** Identify threat of major security incident.	**KPI 1.1.1** Incident identified as a major incident requiring the significant involvement by more than one agency.
	TO 1.2 Activate coordination centres at all required levels in accordance with standard operating procedures.	**KPI 1.2.1** Lead agency activates a coordination centre in accordance with standard operating procedures.
		KPI 1.2.2 Key stakeholders are identified and informed of the activation(s).
		KPI 1.2.2 Liaison arrangements are activated in accordance with standard operating procedures.
	TO 1.3 Develop an effective action plan in accordance with standard operating procedures.	**KPI 1.3.1** Planning processes are followed by the lead agency as established in standard operating procedures.
		KPI 1.3.2 The systems, processes and resources are appropriate for developing the action plan.
		KPI 1.3.3 Threats and associated risks are embedded in the action plan.
		KPI 1.3.4 Where appropriate, legal and policy frameworks are used to support the action plan.
	TO 1.4 Coordinate a critical incident in accordance with the lead agency's emergency plan, the action plan, CIMS, and legal/policy frameworks.	**KPI 1.4.1** Liaison arrangements are maintained as required throughout the duration of the response.
		KPI 1.4.2 Response is managed in accordance with plans and within mandated frameworks.
		KPI 1.4.3 The systems, processes and resources are appropriate for implementing the action plan.
		KPI 1.4.4 Lead agency is able to delegate tasks to support agencies within legal frameworks.
		KPI 1.4.5 Agencies carry out the delegated tasks in a timely manner in accordance with standard operating procedures.
		KPI 1.4.6 As appropriate, implement site, local, regional and national levels of coordination.
	TO 1.5 Lead coordination centres in accordance with standard operating procedures.	**KPI 1.5.1** Lead agency manages an interagency coordination centre.
		KPI 1.5.2 Lead agency is able to sustain an operational response for the length of time required.
		KPI 1.5.3 Lead agency is able to reconstitute following a response to a major security incident.
	TO 1.6 Effective activation of specialist functional groups.	**KPI 1.6.1** Identify relevant specialist groups, such as SAC, JIG etc, and activate these groups in accordance with standard operating procedures.
NO 2.0 Support a coordinated Interagency response to major security incidents including overseas agencies	**TO 2.1** Support identification of threat of major security incident.	**KPI 2.1.1** Agency supports the identification of a threat as a major incident requiring the significant involvement by more than one agency.
		KPI 2.1.2 Agency identifies contributing hazards from within its sphere of expertise.

where necessary.	**TO 2.2** Activate coordination centres at all required levels in accordance with standard operating procedures.	**KPI 2.2.1** Support agency activates a coordination centre, where required, in accordance with standard operating procedures.
		KPI 2.2.2 Lead agency and other key stakeholders are identified and informed of the activation(s).
		KPI 2.2.2 Liaison arrangements are activated in accordance with standard operating procedures.
	TO 2.3 Support the development of an action plan in accordance with standard operating procedures.	**KPI 2.3.1** Support agency contributes to the lead agency planning processes as established in standard operating procedures.
		KPI 2.3.2 Threats and associated risks identified by the support agency are embedded in the action plan.
		KPI 2.3.3 Support agency develops an action plan to detail the tasks assigned to it by the lead agency.
		KPI 2.3.4 Where appropriate, legal and policy frameworks are used to support the action plan.
	TO 2.4 Support a critical incident in accordance with the lead agency's emergency plan, the action plan, CIMS, and legal/policy frameworks.	**KPI 2.4.1** Liaison arrangements are maintained as required throughout the duration of the response.
		KPI 2.4.2 Response is supported in accordance with plans and within mandated frameworks.
		KPI 2.4.3 The systems, processes and resources are appropriate for implementing the action plan.
		KPI 2.4.5 Agencies carry out the delegated tasks in a timely manner in accordance with standard operating procedures.
		KPI 2.4.6 As appropriate, implement site, local, regional and national levels of support.
	TO 2.5 Support coordination centres in accordance with standard operating procedures.	**KPI 2.5.1** Support agencies are able to support the inter-agency coordination centre as required by the lead agency.
		KPI 2.5.2 Support agencies are able to sustain an operational response for the length of time required.
		KPI 2.5.3 Support agencies are able to reconstitute following a response to a major security incident.
	TO 2.6 Support activation of specialist functional groups.	**KPI 2.6.1** Identify relevant specialist groups, such as SAC, JIG etc, and support the activation of these groups in accordance with standard operating procedures.
NO 3.0 Conduct effective high level All of Government decision making.	**TO 3.1** DESC activated and effective within acceptable period of time.	**KPI 3.1.1** DES, ODESC and Watch Groups (DESC) established as appropriate in a timely manner in accordance with standard operating procedures.
		KPI 3.1.2 Relevant DESC Groups provide strategic direction to relevant agencies, allowing comprehensive operational planning as required.
		KPI 3.1.3 Decisions are communicated to key stakeholders in a timely manner in accordance with standard operating procedures.
		KPI 3.1.4 Relevant DESC groups monitor and evaluate decisions throughout the incident.
	TO 3.2 Effective consultation of key stakeholders in the decision making process.	**KPI 3.2.1** Management of all domestic and international stakeholders as appropriate.

NO 4.0 Effectively manage information horizontally and vertically.	**TO 4.1** Incident information is effectively managed and communicated by all agencies involved in the response.	**KPI 4.1.1** A strategic communication plan is developed and implemented.
		KPI 4.1.2 Accurate information is communicated internally in a timely manner in accordance with standard operating procedures.
		KPI 4.1.3 Information is communicated across domestic and international stakeholders in a timely manner in accordance with standard operating procedures.
		KPI 4.1.4 Information is appropriately stored.
		KPI 4.1.5 Public information/messaging is coordinated and consistent across agencies.
		KPI 4.1.6 All agencies have the appropriate equipment and resources to manage information effectively.
	TO 4.2 Support requirements are effectively communicated.	**KPI 4.2.1** International or domestic support requests are effectively managed.
	TO 4.3 When required, secure communications are deployed and effectively established within a multi agency domain.	**KPI 4.3.1** Appropriate agencies have the equipment, resources and procedures to manage classified information effectively.
	TO 4.4 Intelligence products effectively fused from various sources and promulgated in a timely manner to relevant stakeholders.	**KPI 4.4.1** Intelligence products accurately disseminated to key stakeholders over a correctly classified medium.
NO 5.0 Implement business continuity arrangements during a response to a major security (all hazards) incident.	**TO 5.1** Agency is able to continue to effectively meet essential business as usual outputs.	**KPI 5.1.1** Essential and non essential business outputs are identified.
		KPI 5.1.2 Agency has, or is able to acquire from other agencies, the capacity needed to meet essential business requirements whilst simultaneously meeting incident resource requirements.
		KPI 5.1.3 Business activities are adjusted and communicated as per business continuity plans.
NO 6.0 Integrate previous lessons identified from interagency activities in order to engender a culture of continuous improvement.	**TO 6.1** Continuous improvement processes are implemented.	**KPI 6.1.1** Inter agency capability building Information is collected and shared with relevant agencies by the lead agency to allow continuous improvement across government.
		KPI 6.1.2 During the development of inter agency exercises, previous lessons identified are integrated by the lead agency.
		KPI 6.1.3 Best practices are discussed and shared across agencies.
	TO 6.2 Evaluation and post activity reporting of the inter agency outcomes is undertaken.	**KPI 6.2.1** Evaluation is coordinated by the lead agency against relevant national objectives.
		KPI 6.2.2 Supporting agencies provide relevant information to the post activity reporting.
		KPI 6.2.3 Post activity reports, with lessons identified for inter agency capability building, are stored in a central location by a central agency (DPMC).

		KPI 6.2.4 Corrective actions, identified in post activity reports, are implemented by the appropriate agency and in collaboration with other agencies where necessary.
NO 7.0 Further develop collaborative relationships, to enhance interagency knowledge and understanding; creating capability and resilience across the security (all hazards) sector.	**TO 7.1** Agencies share information to engender an all hazards, all of government approach to incident management.	**KPI 7.1.1** Information is shared and utilised across agencies to assist in relationship and resilience building.
		KPI 7.1.2 Best practices are discussed and shared across agencies.

National Security System Training and Development Group (NSSTDG) Terms of Reference

Background

DPMC established the National Security System Training and Development Group (NSSTDG) in late 2015 to bring an 'All of Government (AoG)' approach to readiness activities associated with Training & Development. Having a competent and capable response workforce with the appropriate skills, experience and relationships contributes to a strong National Security System (NSS) and is fundamental to the resilience of the overall system.

In 2017 the Hazard Risk Board (HRB) signed off on recommendations made by the NSSTDG to lift the efficiency and effectiveness of training across the sector. These recommendations included that:

- Staff working in a response have a level of competency appropriate to their role;
- Agencies engage in consistent CIMS training and assessment;
- Agencies will support the use of existing CIMS unit standards and engage with Skills to support their review and ongoing development of new unit standards as appropriate;
- Unit standards in Planning, Intelligence and Logistics are prioritised for development;
- Work would continue to further develop and embed the NSSTDG Training and Development framework

The NSSTDG meets on a monthly basis and is chaired by the Workforce Team within the National Emergency Management Agency (NEMA).

Purpose and Role

Broadly, the NSSTDG exists to build the capability and capacity of the National emergency management workforce so that the New Zealand Government can respond efficiently and effectively in times of national response.

Specifically, the NSSTDG will support and promote the work that the Workforce Team is undertaking to:

a) Deliver on the government's recommendations from the *Ministerial Review, Better responses to natural disasters and other emergencies* - focus area #4: Building the capability and capacity of the Emergency Management Workforce.

b) Progress 'The Enabling Consistent CIMS Practice' project in accordance with Hazard Risk Board recommendations and system need.

Note that the NSSTDG's focus is on training and development that contributes to readiness for response. This focus on response is aligned to the *Ministerial Review, Better responses to natural disasters and other emergencies.*

Responsibilities

The NSSTDG will support and promote the work that the Workforce team and the National Emergency Management Agency (NEMA) is undertaking to:

1. Enhance the capability and capacity of a trained workforce to support National Security System responses
2. Professionalise the role of emergency management through professional standards and accreditation
3. Develop a recognised career path for emergency managers
4. Increase the use of CIMS by central government agencies, departments and crown entities
5. Progress 'The Enabling Consistent CIMS Practice' project in accordance with Hazard Risk Board recommendations and system need.

Group Composition

Membership is open to all interested central government agencies, departments and Crown entities. A list of those agencies represented on the NSSTDG as at 1 April 2020 is contained in Appendix 2.

The skills and capabilities of those who attend support the effectiveness of the group. A list of the skills and capabilities required in attendees is contained in Appendix 3.

New agencies may be invited to join NSSTDG. This will be documented appropriately and noted in any future refresh of this Terms of Reference.

Agency representation:

- Agencies are asked to send one representative to NSSTDG sessions but, if space allows, two people from the same agency can attend.
- Sharing agency representation between two agency staff and alternating/sharing attendance at NSSTDG sessions is acceptable.
- Sending an array of different representatives to each session is discouraged as it impacts on the ability of the group to progress work and maintain consistency.

Member's role

In attending the NSSTDG, members support the Workforce team and the work relating to the Emergency Management System Reform-related work programmes by:

- Providing their agency perspective and representing the needs and expectations of their agency;
- Providing subject matter knowledge, expertise and free and frank advice;
- Championing improved capability development for response, disseminate relevant information and provide their agency with a national perspective;
- Supporting each other in progressing the kaupapa of the NSSTDG

It is expected that NSSTDG members:

- Keep abreast of what the group is working on even if they are unable to attend a session
- Come to NSSTDG sessions prepared. If preparation in advance is required for any NSSTDG session, this will be emailed in advance.

- Attend NSSTDG regularly

Frequency of meetings

- The NSSTDG meets monthly or as/when required.
- To further projects or particular areas of work, smaller sub-working groups or focus groups can be formed. Membership on these groups is voluntary and welcomed.

Reporting

- The NSSTDG is a Hazard Risk Board Committee.
- Reporting and work programme updates will be provided as/when required to boards or groups that require updates, such as HRB, the Incident Management Reference Group (IMRG), the CIMS Steering Group or the National Security System weekly update.
- The NSSTDG monthly update provides a monthly update to a distribution list of parties who have interest in the work that is being done by the NSSTDG.

Circulation of meeting notes

A summary of each working group, including updates and action points, will be provided, post working group, to all on the distribution list.

Appendix 1: Member agencies

Membership is comprised of the following agencies:

Member Agencies

- Ara Poutama - Department of Corrections
- Department of Conservation
- Ministry of Education
- Department of Internal Affairs
- Department of the Prime Minister and Cabinet
- Fire and Emergency New Zealand
- Land Information New Zealand
- Maritime New Zealand
- Ministry of Business, Innovation & Employment
- Ministry of Foreign Affairs and Trade
- Ministry of Health
- Ministry for Primary industries
- Ministry of Social Development
- Ministry of Transport
- New Zealand Customs
- New Zealand Defence Force
- New Zealand Police
- New Zealand Search and Rescue Secretariat
- The Electoral Commission
- Ministry for the Environment
- New Zealand Transport Agency
- Worksafe

Appendix 3:

Individual level skills required to enable and enhance participation:

The skills and capabilities of those who attend support the effectiveness of the group. NSSTDG members should possess the following skills and capabilities:

- Learning and Development – learning design, development, delivery and evaluation and/or;

- People Capability Development / Workforce – broad knowledge and/or experience of building people or workforce capability within and /or across organisations and/or;

- Emergency and/or Incident Management knowledge and practical application and/or;

- Knowledge of home agency systems / processes / capabilities that support response and;

- Networking ability and influence – is connected and can influence effectively upwards, downwards and across, in home agency and during working groups.

ODESC
Officials' Committee for Domestic
and External Security Coordination

Counter-Terrorism Coordination Committee (CTCC) Terms of Reference

Purpose

The Counter-Terrorism Coordination Committee (CTCC) coordinates and drives activity across the counter-terrorism (CT) system, to implement the national *Counter-Terrorism Strategy* (CT Strategy).

Context

The CTCC was established by DPMC in 2015, to bring together the significant pieces of CT work being led by different agencies across government, and to collectively deliver improvements to the CT system at a national level. New Zealand's first national CT Strategy was agreed by Cabinet in September 2019, with the aim of "*bringing our nation together to protect all New Zealanders from terrorism and violent extremism*".

Role of the CTCC

The CTCC is responsible for ensuring the National Security System (NSS) delivers the vision, outcomes and commitments set out in the CT Strategy. The key responsibilities of the CTCC are therefore to implement the CT Strategy by:

a. **Supporting strategic CT decision-making and action**, including by providing advice and recommendations to the Security and Intelligence Board (SIB) on:

- The CT Strategy, to ensure it remains relevant and fit for purpose.
- CT risk management practice (across the 4Rs aspects of the CT Strategy), including governance gaps and opportunities for improvement.
- Specific CT-related priorities for action (such as significant CTWP adjustments).

b. **Coordinating and driving inter-agency CT work**, including:

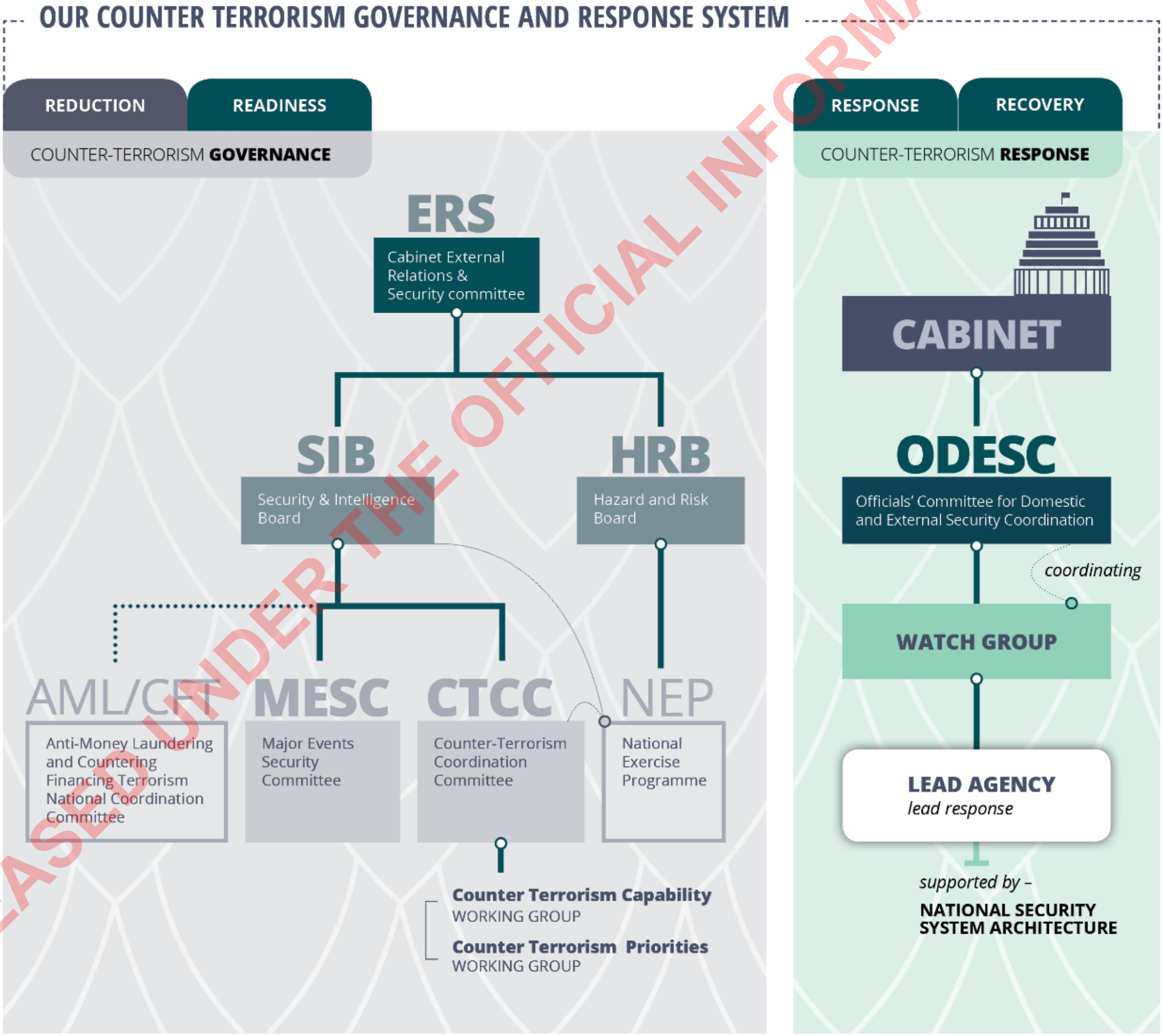
- Maintaining a comprehensive and cohesive CT Work Programme (CTWP), to deliver strategy objectives.
- Developing appropriate performance measures to monitor CTWP progress, and using these indicators to report regularly to the Security and Intelligence Board (SIB).
- Managing and de-conflicting risks, issues and interdependencies relating to the delivery of individual CTWP elements.
- Prioritising and coordinating the resourcing of priority CT system work streams where required (acknowledging that agencies retain authority and responsibility for allocating their own resources).

CTCC member agencies, in their roles as individual CTWP element owners, are responsible for ensuring each element:

- Remains aligned to the CT Strategy.
- Is delivered in the most efficient and effective way, using appropriate performance indicators.
- Takes into account connections to other CTWP elements, as well as the broader NSS as appropriate.
- Are appropriately resourced.

Governance and reporting to the Security and Intelligence Board

The CTCC is a sub-committee of SIB. It provides advice and assurance to SIB about CT systems risks, priorities, projects and resourcing requirements. CTCC reporting to SIB will take the form of a regular report-back, and risks and issues will be escalated on an as-required basis.


OUR COUNTER TERRORISM GOVERNANCE AND RESPONSE SYSTEM
REDUCTION
READINESS
COUNTER-TERRORISM GOVERNANCE
RESPONSE
RECOVERY
COUNTER-TERRORISM RESPONSE
ERS
Cabinet External Relations & Security committee
SIB
Security & Intelligence Board
HRB
Hazard and Risk Board
AML/CFT
Anti-Money Laundering and Countering Financing Terrorism National Coordination Committee
MESC
Major Events Security Committee
CTCC
Counter-Terrorism Coordination Committee
NEP
National Exercise Programme
Counter Terrorism Capability WORKING GROUP
Counter Terrorism Priorities WORKING GROUP
CABINET
ODESC
Officials' Committee for Domestic and External Security Coordination
coordinating
WATCH GROUP
LEAD AGENCY
lead response
supported by –
NATIONAL SECURITY SYSTEM ARCHITECTURE

Sub-groups of the CTCC

Working groups reporting to and accountable to CTCC will be established by as required. There are two enduring CTCC working groups:

a. The **Counter-Terrorism Capability Working Group (CTCWG)**, an ad hoc sub-committee responsible for enhancing New Zealand's readiness to respond to a terrorist incident.

b. The **Counter-Terrorism Priorities Working Group**, is responsible for recommending updates to the CTWP to address New Zealand's CT risks and vulnerabilities. This working group is also responsible for sector coordination of the National Security and Intelligence Priority (NSIP) on CT, reporting in parallel on this aspect to the National Intelligence Coordination Committee (NICC).

Membership

The CTCC is chaired by the Counter-Terrorism Strategic Coordinator. Membership of CTCC will comprise representatives of NSS agencies operating in the CT system, with agency attendees to be confirmed in consultation with the Chair and to be of an appropriately senior level.

CTCC meeting arrangements

The CTCC will meet at least quarterly – and significantly more often if required – with meetings aligned to the SIB meeting schedule where possible. Every second meeting will include social sector agencies, and the CTCC will allow for other external groups to present and discuss CT-related issues. The National Security Group (NSG) within DPMC will provide secretariat services.

The Chair will set the meeting agenda with a focus on strategic issues and risks, and interdependencies across work streams. Work streams with a RAG status of Red will be reviewed at each meeting. Members can add items to the agenda by advising the Chair.

All papers for consideration must be lodged with the Secretariat at least five working days prior to the meeting, and will be circulated electronically to members at least three working days before the meeting. The purpose of all papers should be identified in the agenda as being for *information*, *discussion* or *decision-making*.

Prior to each meeting, members should ensure that they:

- Read and understand the papers to be taken as read and any other papers submitted.
- Have formed a position on any decisions required by the CTCC.
- Prepare any feedback or questions.

CTCC members should be prepared to represent the views of their agency at meetings. Members should also look to demonstrate the following values and behaviours:

- Debating difficult issues, and coming out with clear and agreed decisions focused on delivering the CT Strategy.
- Working as a unified team.

- Prioritising system interests above the interests of individual agencies, and not straying into day-to-day operational issues.

Following each meeting, members should ensure that they:

- Complete any actions assigned to them.
- Communicate relevant CTCC decisions to their respective agencies and teams.

CYBER SECURITY STRATEGY CO-ORDINATION COMMITTEE

Terms of Reference - 2019

Purpose

This Terms of Reference defines the role of the Cyber Security Strategy Co-ordination Committee (CSSCC) to implement New Zealand's Cyber Security Strategy 2018 (the Strategy) through a more joined-up approach.

Mandate

Cabinet has agreed that relevant agencies implement the Strategy by establishing a CSSCC and Co-ordinator [CAB-18-MIN-0562].

The focus of the CSSCC is to plan, monitor, and govern the annual work programme for joint-agency and cross portfolio cyber security projects. The CSSCC will maintain strong links and coordinate with relevant government institutions including the Government Chief Digital Officer and the Government Chief Information Security Office. The CSSCC's focus will be on implementing the government's strategy for cyber security across New Zealand, rather than a focus on cyber security in government alone.

While the CSSCC will be informed about agency-specific projects, it is not intended to make decisions about agencies' business-as-usual work or projects.

As part of Cabinet's direction to relevant agencies, the CSSCC will apply the Strategy's new guiding principles for how agencies will work together during the planning, conduct, and assessment of projects and initiatives to give effect to the Strategy. These principles are:

- Working with others in a way that:
  - builds and maintains trust
  - is people-centric, respectful, and inclusive
  - balances risk with being agile and adaptive
  - uses our collective strengths to deliver better results and outcomes, and
  - is open and accountable.

The CSSCC will also need to ensure that agencies work more with other organisations, including those outside ICT and cyber security, and participate in events to get broader input and engagement with people, businesses, and community organisations. It is also anticipated that the CSSCC will provide oversight of any co-design projects undertaken to tackle shared policy, technology, and service problems.

Government's expectations for how cyber security agencies will work together and implement the Strategy are set out in detail in the 'Delivering the Strategy: working together more effectively' section and Appendix A of the Refresh of New Zealand's Cyber Security Strategy Cabinet paper [CAB-18-MIN-0562].

Governance

The CSSCC will report to and seek guidance from the Security Intelligence Board where appropriate.

Membership

Membership of the CSSCC will reflect the agencies tasked with improving and regulating New Zealand's 'as a whole' cyber security and in particular those agencies involved in joint projects to address cross-sector issues.

The following agencies be standing members of the CSSCC:

- Department of the Prime Minister and Cabinet, National Security Group (Chair)
- Department of the Prime Minister and Cabinet, National Cyber Policy Office
- Department of Internal Affairs
- Government Communications Security Bureau
- Ministry of Business, Innovation and Employment
- Ministry of Defence
- Ministry of Foreign Affairs and Trade
- Ministry of Justice
- New Zealand Defence Force
- New Zealand Police
- State Services Commission

Agency representatives should be senior officials with decision making authority, with regard to their agency's cyber security functions.

Other agencies may attend the CSSCC where matters being considered directly affect their agencies. It is also expected that a wider group of agencies and their component business units will be involved in work that the CSSCC has oversight for.

Meetings

The CSSCC will meet at its discretion. The National Cyber Policy Office (NCPO) of the DPMC will act as the secretariat (a Cyber Security Co-ordinator, if funded, will lead secretariat support functions). An agenda will be circulated ahead of the meeting to allow members to nominate items for discussion. Ideally agenda items should be of a strategic, cross-cutting nature, related to decision-making required to implement the Strategy. Relevant background papers for discussion should also be circulated ahead of meetings. The NCPO will provide brief minutes and record follow-up action steps for each meeting.

A working level group will also meet, as required, to ensure clarity of roles and responsibilities, provide agencies an opportunity to raise current cyber-related priorities, implementation issues and updates, communication initiatives and provide relevant operational updates. This will be called the Cyber Coordination Group (CCG). This group's membership will be as broad as required to coordinate across joint agency projects and will report to the CSSCC.

Other working level cyber security joint-agency groups and committees established or maintained to implement Strategy objectives and will report to the CSSCC. The CSSCC will approve the membership, mandate and terms of reference (if any) of any working groups. The mix of working groups is expected to change over time in line with project initiation and completion, and the business needs and capacity of agencies.

Priorities

New Zealand's Cyber Security Strategy 2018 will be the primary driver for the CSSCC's priorities. The Strategy sets out five priority areas for improving New Zealand's Cyber security:

- Strong and capable cyber security workforce and ecosystem
- Cyber security aware citizens
- Internationally active
- Resilient and responsive New Zealand
- Proactively tackle cybercrime

These priorities are set out in more detail in *New Zealand's Cyber Security Strategy 2018* and DEV-18-SUB-0256.

Foreign Interference Coordination Committee (FICC) Terms of Reference

s6(a)

[redacted]

s6(a)

[redacted]

s6(a)

[redacted]

MAJOR EVENTS SECURITY COMMITTEE

TERMS OF REFERENCE

Purpose

The purpose of this Terms of Reference is to describe the role, responsibilities, governance structure, and membership of the Major Events Security Committee (MESC).

Role

MESC is responsible for providing security advice to ODESC concerning major events which have a national interest and ensuring that New Zealand security support for approved major events is appropriate to the risk.

Responsibilities

- Providing strategic planning and policy advice to ODESC for major event security;
- Identifying major events that may require New Zealand government interagency security support;
- considering threat level advice for those events identified for further consideration;
- considering the security measures being put in place by the host country of those events identified for further consideration;
- considering the risk assessment for those events identified for further consideration;
- producing a consular emergency response plan;
- determining the mitigation required to reduce residual risk levels for those events to a level acceptable to the New Zealand Government;
- recommending to ODESC the mitigation measures required to reduce the residual risk associated with a specific event to a level acceptable to the New Zealand Government;
- identifying lessons learned from supported major events; and
- providing a post event report to ODESC

Governance Arrangements

MESC is a sub-committee of the Security and Intelligence Board (SIB) and accordingly the chief executives forum is responsible for approving and prioritising MESC's work programme. MESC will report to SIB annually.

Membership

MESC is chaired by an official from the National Security Systems Directorate (NSSD) of DPMC. The Chair of MESC is responsible for coordinating the committee's work programme and reporting to SIB.

MESC will be comprised of officials from government agencies that have a role to play in a major event's security support. The core agencies of the committee are DPMC, MFAT, NZ Police, NZSIS, CTAG, GCSB, NZDF' with other agencies co-opted as and when required.

s6(a), s(6)(d) .

ODESC

Officials' Committee for Domestic and External Security Coordination

National Intelligence Coordination Committee (NICC) Terms of Reference

Purpose

The National Intelligence Coordination Committee (NICC) provides overarching guidance, coordination and oversight of the National Security and Intelligence Priorities (NSIPs).

Context

NICC is part of a broader governance system that supports national security sector agencies to operationalise the NSIPs.

The NSIPs articulate the Government's priorities for the national security and intelligence sector. They are used to ensure that intelligence, information and assessment insights are focused in areas where they're needed most, resulting in better-informed decision-making and policy advice.

This means ensuring providers of intelligence, information and assessment understand what customers need across all the NSIPs, that their response is coordinated and effective, and that intelligence products and activities have an impact on relevant decision-making and policy advice.

Role of NICC

NICC's key responsibilities are to:

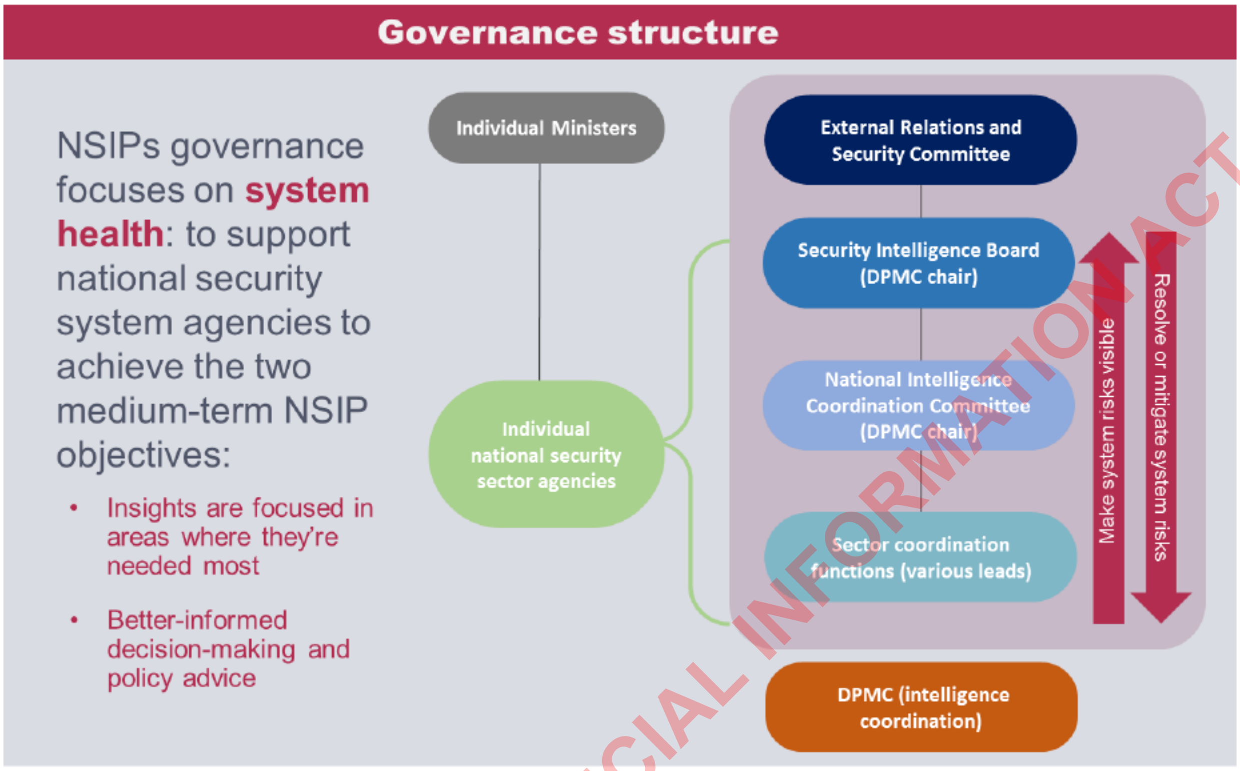
a. Manage system risks in relation to the NSIPs by:
   - i. Responding to gaps or issues with cross-agency coordination
   - ii. Responding to gaps or issues with resourcing that are not easily resolved at agency level
   - iii. Escalating identified system risks to the Security and Intelligence Board (SIB) where required and appropriate

b. Oversee the operationalisation of the NSIPs by:
   - i. Agreeing the appropriate sector coordination mechanisms for each NSIP
   - ii. Monitoring performance of sector coordination functions using agreed performance frameworks

c. Advise and consult on further development or refreshing of the NSIPs, and associated reporting to Ministers.

Governance and reporting to the Security and Intelligence Board

NICC is a sub-committee of the Security and Intelligence Board (SIB). It provides advice and assurance to SIB as required on system risks in relation to sector coordination and resourcing.



Governance structure

NSIPs governance focuses on **system health**: to support national security system agencies to achieve the two medium-term NSIP objectives:

- Insights are focused in areas where they're needed most
- Better-informed decision-making and policy advice

Individual Ministers
Individual national security sector agencies
External Relations and Security Committee
Security Intelligence Board (DPMC chair)
National Intelligence Coordination Committee (DPMC chair)
Sector coordination functions (various leads)
Make system risks visible
Resolve or mitigate system risks
DPMC (intelligence coordination)

Sub-groups of NICC

Sector Coordination Groups (SCGs) or other equivalent coordination mechanisms for individual NSIPs report to NICC. Where such groups also have other, broader responsibilities, they may also report to other governance structures as appropriate.

The National Intelligence Open Source Committee (NIOSC) is a sub-committee of NICC. Open source intelligence is a key information contributor to the NSIPs, and NIOSC looks at harnessing opportunities and mitigating potential risks to agencies that use open source intelligence, through leadership and coordination.

Meeting arrangements

s(6)(d), s9(2)(g)(ii) [redacted]

Papers are to be submitted to the Secretariat no later than six working days prior to a meeting date. The Secretariat is responsible for distributing papers to members five working days prior to the meeting.

Terms of Reference will be reviewed annually, in line with the annual review of the NSIPs.

Membership

NICC is chaired by DPMC's Manager, Intelligence Coordination. Members include representatives from the following agencies, at an appropriately senior level as decided by the Chair.

- NZ Customs (Intelligence)
- DPMC (Strategic Coordination, Policy, and Assessments)
- GCSB (Intelligence, Cyber and Policy)
- MBIE (Intelligence and Policy)
- Ministry of Defence (Policy Branch)
- MFAT (ISED)
- NZDF (NZDI and GEOINT NZ)
- NZ Police (Intelligence and Policy)
- MPI (Intelligence and Policy)
- NZSIS including CTAG (Intelligence and Policy)

Behaviours and values

NICC members operate as a collective. They represent the views of respective agencies at meetings, but they focus on the system rather than attending solely as representatives of their agencies. NICC members are expected to make constructive use of the variety of experience and perspectives in the room in debating the issues put before them and coming to a collective view.