DEPARTMENT OF THE
PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

18 August 2021

[redacted]

Reference: OIA-2020/21-0753

Dear [redacted]

Official Information Act request relating to Counter-terrorism system capability review

I refer to your Official Information Act 1982 (the Act) request, received by the Department of the Prime Minister and Cabinet (DPMC) on 7 July 2021. You requested:

> *"…a copy of the counter-terrorism system capability review. Please include advice, briefings, reports, aides memoire and memos related to the findings of the review and proposed priority actions..."*

I note the timeframe for responding to your request was extended by 10 working days to allow for further consultation to be undertaken. Following this, I am now in a position to respond.

A search of information relevant to your request held by the National Security Group within DPMC was undertaken. Please find copies of the following documents enclosed:

Item	Date	Document Description/Subject
1.	June 2020	Countering Terrorism and Violent Extremism System Capability Review: Paper 1 and CT / CVE System Capability Landscape
2.	19 June 2020	CT Strategy Implementation Plan - 2020
3.	1 April 2021	Counter-Terrorism Work Programme 2021
4.	11 November 2020	Cover Sheet for SIB Item 4
5.	11 November 2020	Counter-Terrorism System Capability Review
6.	11 November 2020	Counter-Terrorism System Capability Review: Proposed Priority Development Initiatives

Some information has been withheld in these documents under the following sections of the Act:

- section 6(a), as the making available of that information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand;
- section 9(2)(a), to protect the privacy of natural persons;
- section 9(2)(ba)(i), protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied;

- section 9(2)(f)(iv), to maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials;
- section 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any public service agency or organisation in the course of their duty; and
- Section 9(2)(g)(ii), to maintain the effective conduct of public affairs through the protection of such Ministers, members of organisations, officers, and employees from improper pressure or harassment.

You will note two parts of the *Counter-Terrorism System Capability Review* are enclosed. Two further items comprise this Review. I have decided to withhold these parts in full under sections 6(a), 9(2)(ba)(i), and 9(2)(g)(i) of the Act, as outlined above.

Three of the items enclosed: *Cover Sheet for SIB Item 4, Counter-Terrorism System Capability Review,* and *Counter-Terrorism System Capability Review: Proposed Priority Development Initiatives,* were prepared for the Security and Intelligence Board (SIB). In addition to these three items, a fourth document, *CVE System Capability Landscape,* was also presented to SIB. I have decided to withhold this document in full under sections 6(a), 9(2)(ba)(i), and 9(2)(g)(i) of the Act as outlined above. If you are interested, some information about SIB can be found online at: https://dpmc.govt.nz/our-programmes/national-security-and-intelligence-oversight/national-security-governance-structure/odesc-governance-boards.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on DPMC’s website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely

[redacted]

Tony Lynch
Deputy Chief Executive,
National Security Group

ODESC
Officials' Committee for Domestic and External Security Coordination

Counter-Terrorism Coordination Committee
ctcc@dpmc.govt.nz

Countering Terrorism and Violent Extremism

System Capability Review

Paper 1: Capability landscape and development opportunity themes

June 2020

Contents

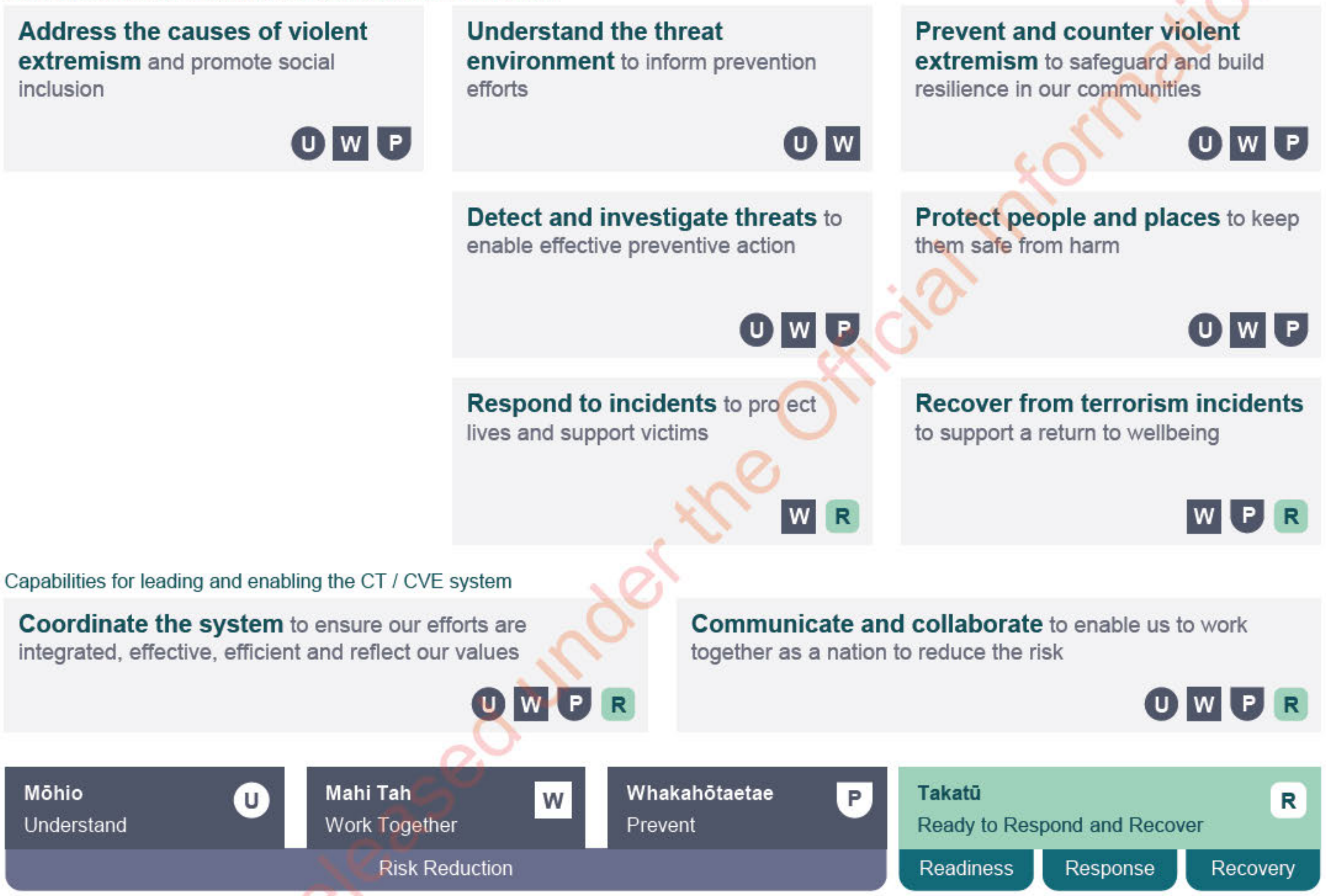
Figures

Executive summary

'Business capabilities' are expressions of what organisations must be able to do in order to implement their strategies and deliver target outcomes.

This paper presents a system view comprising 9 headline and 37 second-order capabilities, then proposes areas for further investigation and evaluation.

Capability landscape – headline level



Core capabilities for countering terrorism and violent extremism

Address the causes of violent extremism and promote social inclusion U W P

Understand the threat environment to inform prevention efforts U W

Prevent and counter violent extremism to safeguard and build resilience in our communities U W P

Detect and investigate threats to enable effective preventive action U W P

Protect people and places to keep them safe from harm U W P

Respond to incidents to protect lives and support victims W R

Recover from terrorism incidents to support a return to wellbeing W P R

Capabilities for leading and enabling the CT / CVE system

Coordinate the system to ensure our efforts are integrated, effective, efficient and reflect our values U W P R

Communicate and collaborate to enable us to work together as a nation to reduce the risk U W P R

Development opportunities

Strengthening shared foundations

What **Better connect information, expertise and effort**, both within government and more widely…

How …through **increasing engagement, understanding and collaboration**…

Why **…to enhance the inclusiveness and effectiveness of our work to protect our communities from terrorism and violent extremism**

Key opportunity themes:

- stakeholder relationship management
- public communication
- capability management and joint ventures
- threat assessment, discovery and investigation
- community understanding and representation in the workforce
- workforce CT / CVE awareness
- information access and sharing

Next steps

Apply a structured approach to evaluate existing capabilities and the nature of challenges, then set out development objectives (3-4 year horizon).

1 Introduction

1.1 Purpose

The Counter-Terrorism System Capability Review ('the review') was commissioned to provide the Counter-Terrorism Coordination Committee (CTCC) with:

- a high-level view of system capabilities for countering terrorism and violent extremism (CT / CVE)[1]
- options for enhancing those capabilities.

The review's objectives are to:

- support the CTCC to ensure CT / CVE capabilities across government are integrated, effective, efficient and reflect New Zealand's values
- inform the CTCC's response to the findings of the Royal Commission of Inquiry into the Attack on Christchurch Mosques[2]
- inform future versions of the CTCC's annual work programme
- potentially, provide agencies with information to support the development of investment cases and Budget bids, in particular to demonstrate alignment to system priorities.

This paper presents a system view of capabilities and proposes candidates for development.

It has been kept at the RESTRICTED level to facilitate sharing. In some areas this has meant limiting the amount of detail presented.

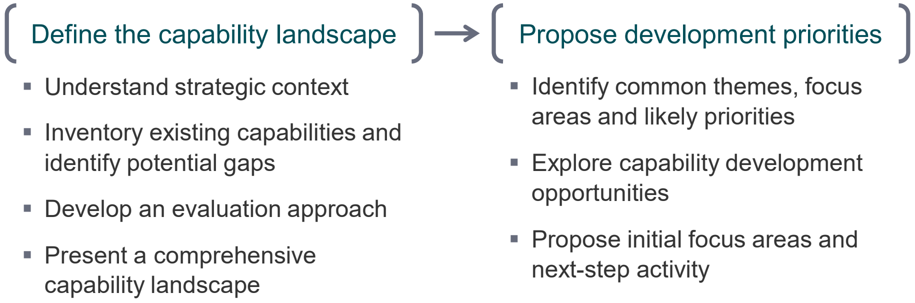
Further context is provided in Annex 1.

1.2 Approach

The review began in February 2020. A structured approach was adopted to help ensure a balanced range of views is represented, including those of agencies not traditionally seen as central to countering terrorism and violent extremism.

Progress was disrupted by the Covid-19 lockdown, ongoing challenges in engaging with agency representatives who were working on Covid response, and the second extension of the time available for the Royal Commission of Inquiry. In response, consultation was limited to agency representatives and the approach was adjusted to refocus this stage and paper on:

- developing, for the first time, a shared view across all capabilities required to counter terrorism and violent extremism
- identifying shared priorities for development.



Define the capability landscape → Propose development priorities

- Understand strategic context
- Inventory existing capabilities and identify potential gaps
- Develop an evaluation approach
- Present a comprehensive capability landscape

- Identify common themes, focus areas and likely priorities
- Explore capability development opportunities
- Propose initial focus areas and next-step activity

Figure 1: Updated stage approach.

A working group representing a subset of CTCC and social sector agencies was convened to support opportunity identification.

[1] Terrorism and violent extremism are not conflated here. Terms are linked because the capabilities required to counter them are essentially the same.

[2] christchurchattack.royalcommission.nz

2 Capability landscape

The model presented in this section is designed to inform system-level decisions on capability investment and management, both now and into the future.

2.1 Modelling approach

‘Business capabilities’ are expressions of what[3] organisations must be able to do to implement their strategies and deliver target outcomes. They may be:

- deployed individually or in combination to fulfil business functions
- defined to multiple levels of detail. Modelling in this paper is limited to two tiers so as to maintain its focus at the system level.

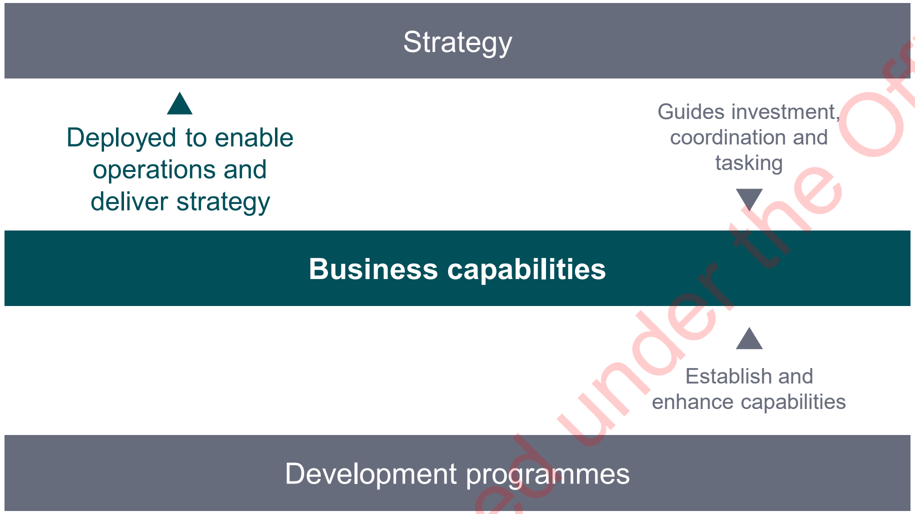

Strategy
Deployed to enable operations and deliver strategy
Guides investment, coordination and tasking
Business capabilities
Establish and enhance capabilities
Development programmes

Figure 2: Capability-strategy relationship.

In order to deliver value successfully and sustainably, capabilities:

- require a well-understood stakeholder and ‘customer’ base that is effectively supported to derive value from them
- must be comprehensive and coherent, effectively integrating people, competencies, processes, information, technology, facilities, equipment and other resources
- should be operated by the parties best placed and most appropriate to deliver them
- require active governance and coordination.

Capability modelling is an appropriate approach for establishing a system-level view of CT / CVE activity as capability-based design:

- recognises capabilities may be deployed for different purposes at different times, supporting agencies to be flexible to respond to evolving priorities in line with New Zealand’s ‘all hazards, all risks’ approach to national security risk management
- supports capability sharing in a range of forms and degrees of formality
- facilitates the identification of opportunities and priorities for enhancement, including where partners can assist each other.

The modelling approach aligns to commonly accepted standards for business capability architecture, with some adjustments to support shared understanding across the range of agencies working in different parts of the system. These include:

- emphasising the use of plain-English, objective-focused labelling
- allowing repetition to support clarity.

[3] Rather than *how* functions are delivered.

2.2 Capability landscape

Figure 3 presents the proposed system capability model. Each component is described further in Annex 2.

Core capabilities: **Countering terrorism and violent extremism**

We have capabilities to…

Address the causes of violent extremism
…and promote social inclusion

- Engage and work effectively with our communities
- Develop, support and promote social inclusion and resilience programmes

U W P

Understand the threat environment
…to inform prevention efforts

- Research, assess and report strategic trends, threats, risks and mitigations
- Understand terrorist and violent extremist ideologies
- Understand the drivers, processes, indicators and implications of radicalisation

U W

Prevent and counter violent extremism
…to safeguard and build resilience in our communities

- Challenge terrorist and violent extremist narratives
- Support at-risk groups to resist radicalisation
- Support people with violent extremist ideologies to disengage
- Counter the means and support that enable terrorism
- Reduce terrorist and violent extremist content, and address its consequences

U W P

Detect and investigate threats
…to enable effective preventive action

- Specify and communicate intelligence requirements
- Generate and manage leads
- Conduct security intelligence and criminal investigations
- Understand the capabilities and intentions of those with terrorist and violent extremist ideologies
- Generate and disseminate intelligence reporting
- Manage residual risks

U W P

Protect people and places
…to keep them safe from harm

- Protect, support and enable individuals, communities and other groups at increased risk of being targeted
- Secure events, locations and infrastructure at increased risk of being targeted
- Disrupt threats and illegal activity

U W P

Respond to incidents
…to protect lives and support victims

- Respond rapidly and proportionately to incidents
- Manage incident consequences
- Support decision-makers
- Manage public and targeted communications
- Manage offenders

W R

Recover from terrorism incidents
…to support a return to wellbeing

- Support the welfare and recovery of victims, families, communities and organisations
- Improve system preparedness

W P R

Enabling capabilities: **Leading and enabling the CT / CVE system**

We have capabilities to…

Coordinate the system
… to ensure our efforts are integrated, effective, efficient and reflect our values

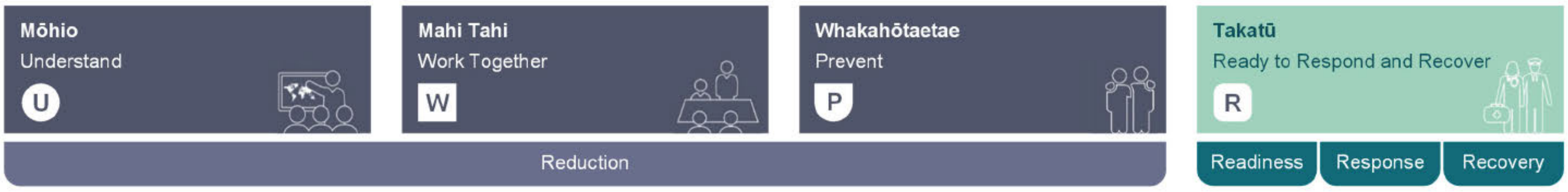
- Set strategic priorities and plans
- Coordinate functions, capabilities and change
- Monitor and review system performance
- Administer legislation and regulation
- Advise and support decision-makers

U W P R

Collaborate and communicate
… to enable us to work together as a nation to reduce the risk

- Manage stakeholder relationships and engagement
- Deliver public information and guidance
- Build internal system awareness and understanding
- Share and leverage system capabilities
- Contribute to international efforts
- Manage, share and utilise information / data

U W P R



Mōhio
Understand
U

Mahi Tahi
Work Together
W

Whakahōtaetae
Prevent
P

Takatū
Ready to Respond and Recover
R

Reduction

Readiness | Response | Recovery

Figure 3: CT / CVE system capability landscape.

6(a), 9(2)(ba)(i), 9(2)(g)(i)

[redacted]

6(a), 9(2)(ba)(i), 9(2)(g)(i)

[redacted]

6(a), 9(2)(ba)(i), 9(2)(g)(i)

[redacted]

6(a), 9(2)(ba)(i), 9(2)(g)(i)

[redacted]

6(a), 9(2)(ba)(i), 9(2)(g)(i)

[redacted]

6(a), 9(2)(ba)(i), 9(2)(g)(i)

[redacted]

4 Next steps

Evaluate capabilities → Assess solution options → Inform work programmes

Evaluate capabilities

- Establish a structured approach for evaluating capabilities (a candidate has been developed)
- Confirm the scope for evaluation – all 1st level, all 2nd level or a subset of 2nd level based on opportunity themes
- Assess existing capabilities and the nature of challenges faced
- Set out target maturity levels (3-4 year horizon)

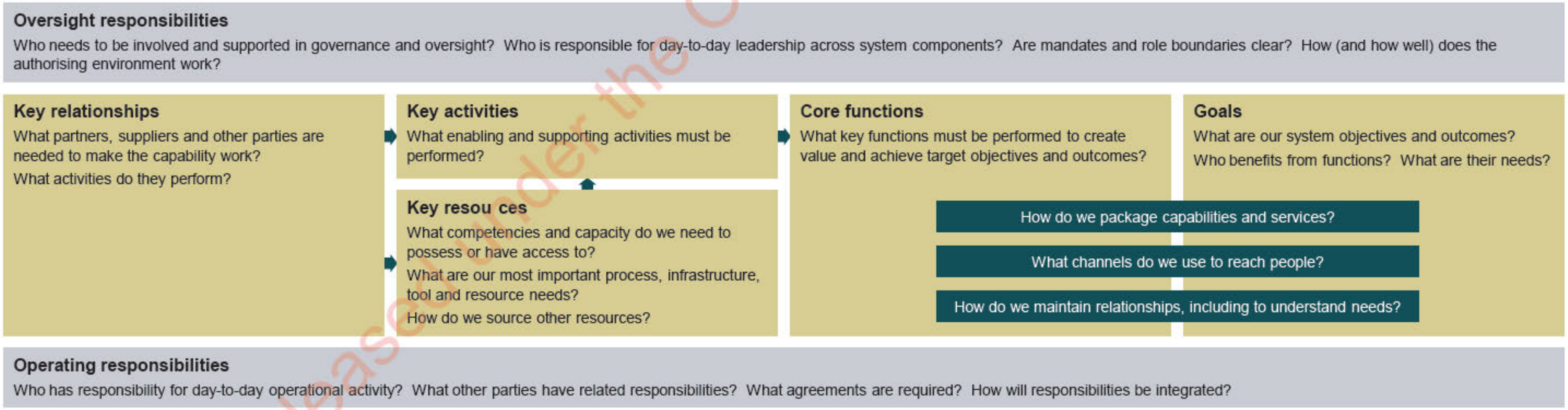
Assess solution options

- Reconcile evaluation results and opportunity theme areas, then translate results into more discrete and actionable candidate initiatives
- Specify delivery options, focusing on coherent, joined-up system solutions
- Establish an options assessment approach and criteria
- Assess options, ensuring counter-factual arguments are addressed
- Confirm conclusions and recommendations

Inform work programmes

- Specify enabling initiatives, e.g. in the form of pre-business case scoping briefs
- Confirm funding and delivery channels (e.g. via the annual CTCC work programme versus individual agency initiatives)
- Support agencies to demonstrate investment alignment to agreed CT system needs and possibly to the Living Standards Framework
- Establish right-sized monitoring and evaluation mechanisms for implementation and operation

When evaluating capabilities and options consider…



Oversight responsibilities
Who needs to be involved and supported in governance and oversight? Who is responsible for day-to-day leadership across system components? Are mandates and role boundaries clear? How (and how well) does the authorising environment work?

Key relationships
What partners, suppliers and other parties are needed to make the capability work?
What activities do they perform?

Key activities
What enabling and supporting activities must be performed?

Key resou ces
What competencies and capacity do we need to possess or have access to?
What are our most important process, infrastructure, tool and resource needs?
How do we source other resources?

Core functions
What key functions must be performed to create value and achieve target objectives and outcomes?

Goals
What are our system objectives and outcomes?
Who benefits from functions? What are their needs?

How do we package capabilities and services?

What channels do we use to reach people?

How do we maintain relationships, including to understand needs?

Operating responsibilities
Who has responsibility for day-to-day operational activity? What other parties have related responsibilities? What agreements are required? How will responsibilities be integrated?

Figure 4: Candidate next steps.

Annex 1: System context

National security system

New Zealand takes an 'all hazards, all risks' approach to managing all types of national security risks. Known as the 4Rs, this approach encompasses:

- **Reduction**. Identifying and analysing long-term risks and taking steps to eliminate them if possible, or if not, to reduce their likelihood and the magnitude of their impact.
- **Readiness**. Building operational response systems and capabilities before an emergency happens.
- **Response**. Taking action immediately before, during or directly after a significant event.
- **Recovery**. Using coordinated efforts and processes to bring about immediate, medium-term and long-term regeneration.

Relevant integrated control frameworks include the:

- *Coordinated Incident Management System*. New Zealand's modular framework of principles, structures, functions, processes and terms for coordinating and controlling the response to natural disasters and other emergencies of any scale.[6]
- *National Security System Handbook*. Sets out arrangements regarding the governance of national security and for responding to a potential, emerging or actual national security crisis.[7]
- *Counter-Terrorism Handbook*. Guides the initial 'response' phase following a terrorism incident.[8]

Cabinet's **External Relations and Security Committee** (ERS) oversees the national intelligence and security sector.

The **Officials' Committee for Domestic and External Security Coordination** (ODESC) is responsible for governance, risk management and operational coordination of national security in its broad sense.

The ODESC **Security and Intelligence Board** (SIB) supports the ERS, working to build a cohesive and effective security and intelligence sector.

The SIB's **Counter-Terrorism Coordination Committee** coordinates and risk manages CT / CVE activity, primarily through:[9]

- supporting strategic CT decision-making and action
- coordinating and driving inter-agency CT work, particularly through the national CT work programme.

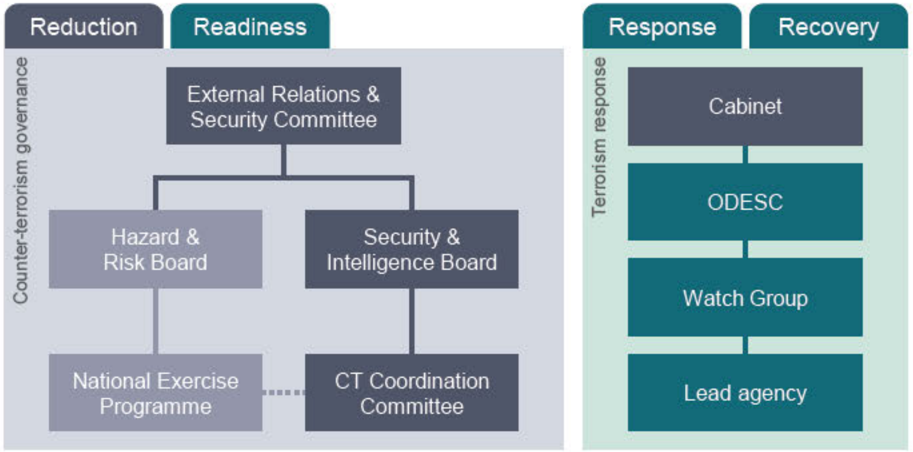

Reduction
Readiness
Response
Recovery
Counter-terrorism governance
External Relations & Security Committee
Hazard & Risk Board
Security & Intelligence Board
National Exercise Programme
CT Coordination Committee
Terrorism response
Cabinet
ODESC
Watch Group
Lead agency

Figure 5: CT system governance.

[6] *Coordinated Incident Management System*, 3rd Edition, NEMA, August 2019, UNCLASSIFIED.

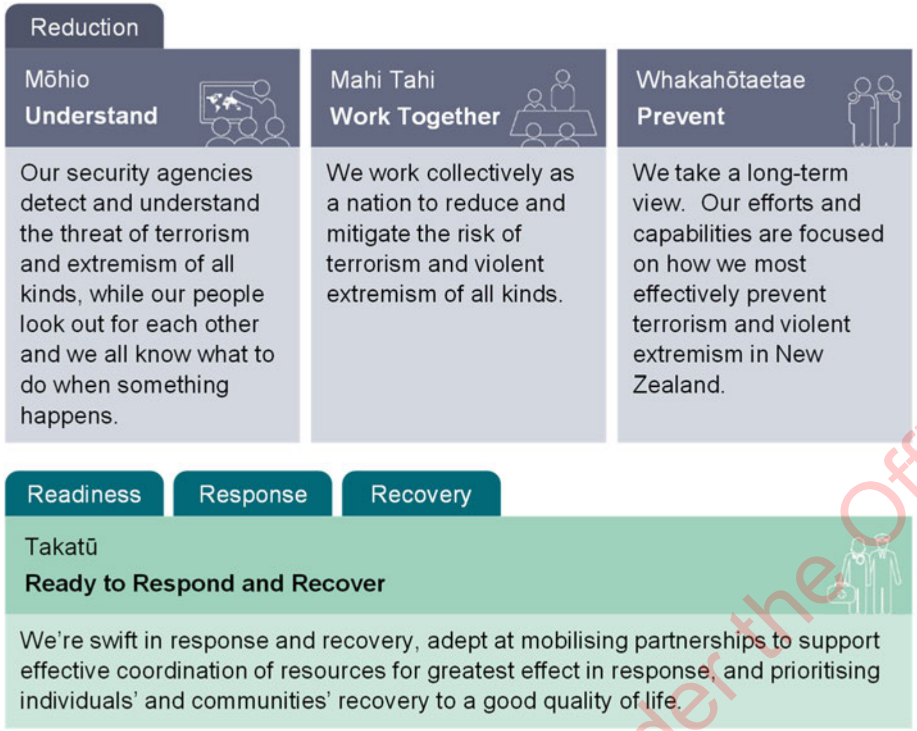
[7] *National Security System Handbook*, DPMC, August 2016, UNCLASSIFIED.

[8] *Counter-Terrorism Handbook*, DPMC, October 2019, RESTRICTED

[9] *Counter-Terrorism Coordination Committee Terms of Reference*, October 2019, IN-CONFIDENCE.

National counter-terrorism strategy

The national counter-terrorism strategy[10] and supporting work programme emphasise threat reduction whilst also preparing for incident response.



Reduction

Mōhio
Understand

Our security agencies detect and understand the threat of terrorism and extremism of all kinds, while our people look out for each other and we all know what to do when something happens.

Mahi Tahi
Work Together

We work collectively as a nation to reduce and mitigate the risk of terrorism and violent extremism of all kinds.

Whakahōtaetae
Prevent

We take a long-term view. Our efforts and capabilities are focused on how we most effectively prevent terrorism and violent extremism in New Zealand.

Readiness | Response | Recovery

Takatū
Ready to Respond and Recover

We're swift in response and recovery, adept at mobilising partnerships to support effective coordination of resources for greatest effect in response, and prioritising individuals' and communities' recovery to a good quality of life.

Figure 6: Risk reduction-focused strategy.

A range of traditional (e.g. law enforcement, security intelligence, safety regulators) and non-traditional agencies (including from the social, health and education sectors) are partnering to deliver the strategy.

[10] *Countering Terrorism and Violent Extremism: National Strategy Overview*, September 2019, UNCLASSIFIED.

Annex 2: Capability descriptions

The descriptions presented here were developed to:

- help clarify capability scope and boundaries (they are illustrative and not necessarily complete)
- inform ongoing evaluation and prioritisation.

Core capabilities

Seven core capability areas are presented. The first – *address the causes of violent extremism* – includes capabilities most often led by agencies in the social sector (though not always – for instance the NZ Police is active in this space). While CT / CVE benefits should accrue from work in this area, they will often be secondary to other social outcomes being sought and may not be made explicit. The remaining six areas are more often deployed directly towards countering terrorism and violent extremism.

Address the causes of violent extremism

Engage and work effectively with our communities
The ability to (see also page 22):

- understand community views, needs and expectations of government and the CT / CVE system
- build and maintain social licence to operate in this often sensitive domain, including through being seen to de iver on commitments
- provide communities with the information they need to engage with the system, and support them to do so
- maintain the trust and confidence required for individuals and communities to feel safe and willing to proactively engage with agencies, for example when they observe concerning behaviours.

Develop, support and promote social inclusion and resilience programmes
The ability to identify, develop, deliver, evaluate and / or support (e.g. through funding) social inclusion and community resilience initiatives that will help address causes of violent extremism, including through:

- fostering recognition, acceptance, participation and positive interactions
- addressing prejudice, unfairness and discrimination.

Understand the threat environment

Research, assess and report strategic trends, threats, risks and mitigations
The ability to:

- develop, maintain, evaluate and share baseline views of the terrorism and violent extremism threat-scape both within and relevant to New Zealand
- plan, direct and conduct strategic CT / CVE analyses, including of historic cases and outcomes to help inform future investigation targeting
- research and forecast ‘over the horizon’ threat sources and vectors before they manifest
- identify, assess, reassess and communicate threat types and their implications as they emerge over time
- research, develop and share information on effective counter-measures
- explore and review information requirements to support the above
- effectively manage risk frameworks, individual risks, and associated communication and effort integration
- provide threat and risk assurance information.

Understand terrorist and violent extremist ideologies

The ability to identify and assess existing, emerging and evolving ideologies. This includes understanding ideological 'cultural' elements such as sources of inspiration, phraseology, symbology and modes of dress.

Understand the drivers, processes, indicators and implications of radicalisation

The ability to inform threat and risk management through understanding:

- behavioural and other indicators associated with violent extremism
- motivations and pathways to radicalisation and mobilisation
- links between radicalisation risk and potentially related vulnerability factors, for example mental illness
- the practical implications of offshore influences on radicalisation
- relationships between crime, criminal relationships and violent extremism.

Prevent and counter violent extremism

Challenge terrorist and violent extremist narratives

The ability to work with, within and on behalf of communities to challenge terrorist and violent extremist ideologies and hate speech (links to the capability to eliminate relevant objectionable content – see page 18), and to promote social inclusiveness.

This includes the ability to identify, develop and utilise appropriate communication content, channels and spokespeople (links to enabling communications management capabilities – see page 22).

Support at-risk groups to resist radicalisation

The ability to identify, educate and support individuals and groups who may be vulnerable to self-radicalisation or targeted for recruitment by terrorist or violent extremist groups. This includes the ability to:

- identify, design and implement effective resilience support mechanisms in cooperation with communities
- manage the risk of inadvertent alienation and / or stigmatisation.

Support people with violent extremist ideologies to disengage

The ability to identify, design and apply appropriate tailored interventions and case management to support the disengagement, rehabilitation and community reintegration of individuals known to follow extremist ideologies. This includes the ability to assess the nature and degree of risk posed by such individuals (links to the ability to conduct investigations – see page 18).

Counter the means and support that enable terrorism

The ability to detect and neutralise access to mechanisms, training and materiel enabling terrorism, for example through anti-money laundering controls, border controls and firearm access controls.

This includes the ability to:

- identify and formally designate terrorist entities to enable the criminalisation and disruption / suppression of recruitment, participation and support activities, including in accordance with foreign policy and international obligations
- administer and disseminate designation information
- exercise powers pursuant to the formal designation of terrorist entities.

Reduce terrorist and violent extremist content, and address its consequences

The ability to identify, detect and prevent the dissemination of, or otherwise limit exposure to, objectionable material relevant to terrorism and violent extremism.

The ability to identify and evaluate actual and anticipated consequences of hate speech and violent extremist content, then to design, apply and evaluate interventions to address those consequences (may link to social inclusion and resilience programmes – see page 16).

This may also include supporting activities such as liaison, monitoring, assessment, case management and enforcement.

Detect and investigate threats

Specify and communicate intelligence requirements

The ability to identify, prioritise and communicate clear and actionable requirements that drive and inform criminal and security intelligence discovery, investigation and analysis.

Generate and manage leads

The ability to effectively generate, record and triage enquiry and lead information:

- proactively, e.g. through focused discovery initiatives
- reactively, e.g. as a result of border screening, reporting by the public, or reporting by partner agencies (domestic or international)
- on a 24*7 basis when necessary, e.g. due to international travel or in reaction to social media activity suggesting an attack is imminent.

This includes, or will be dependent on, supporting capabilities to:

- develop lead source channels and triggers (links to collaboration and communication capabilities – see page 22)
- source, manage and analyse information, including complex datasets (see page 23).

Conduct security intelligence and criminal investigations

The ability to manage full investigation lifecycles from lead development, prioritisation and tasking through to reporting and potential handover for disruption and / or prosecution – all in a timely and efficient manner. This includes supporting capabilities such as:

- overt and covert information and evidence collection methods, e.g. observation, liaison, interviewing, surveillance, technical operations, online operations, forensics, research and more
- processing, analysis and decision-making – including in specialist domains such as financial intelligence
- case management and record-keeping
- compliance monitoring and management.

Understand the capabilities and intentions of those with terrorist and violent extremist ideologies

The ability to evaluate and report on the influences, capabilities, motivations and intentions of individuals and groups identified as following or espousing terrorist or violent extremist ideologies. This includes threats within New Zealand and threats to New Zealanders and New Zealand's interests overseas.

Generate and disseminate intelligence reporting

The ability to generate and deliver reporting that:

- has impact, i.e. it meets well-understood audience needs and is clear and actionable
- is timely and delivered via appropriate channels to all those with a valid need-to-know – this includes the ability to generate and disseminate threat warnings on a 24*7 basis when necessary
- is appropriately access controlled.

Manage residual risks

The ability to ensure individuals and groups assessed as being of interest / concern are not permanently ‘forgotten’ once an investigation is complete, including through maintaining records and incorporating appropriate triggers to inform future lead discovery work – all within the bounds of legislation and policy governing the retention and management of historic / closed records.

The ability to ensure residual risk management is well integrated with wider CT / CVE threat and risk management (see page 16).

Protect people and places

Protect, support and enable individuals, communities and other groups at increased risk of being targeted

The ability to:

- understand who may be at increased risk domestically and offshore, including through ensuring there are effective channels for managing incoming information
- develop and issue relevant advice, guidance and direct interventions (e.g. funding community-led initiatives) through appropriate channels and with understanding of audiences and their needs (see page 22)
- provide protective security measures when it is appropriate to do so directly
- review and adjust protective measures over time.

Secure events, locations and infrastructure at increased risk of being targeted

The ability to mitigate risk through identifying, assessing, prioritising and addressing factors making events, places and infrastructure (physical and digital) vulnerable to, and / or targets for, attack. Examples include crowded places, major events, transport systems, utilities and border control spaces.

This includes the ability to collaborate and share vulnerability and response information with all parties having protective security responsibilities, including those in the community and private sectors.

Disrupt threats and illegal activity

The ability to perform law and regulatory enforcement activities, e.g.:

- monitoring and enforcing compliance, e.g. with control orders
- issuing warnings
- exercising statutory powers of detention and arrest
- disrupting and prosecuting criminal activities, e.g. relevant acts of preparation, planning, recruitment, participation in a terrorist group (including international travel in order to participate) financing terrorism, etc.

This capability is closely related to the countering of means and support for terrorism (see page 17) and the elimination of objectionable material (page 18).

Respond to incidents

Respond rapidly and proportionately to incidents

The ability to effectively sustain an agreed level of capacity and readiness to respond to suspected or known terrorist attacks how, when, where and at the scale required. This includes testing plans and demonstrating preparedness through inter-agency personnel mobility (supporting surge capacity), scenario planning, cross-training and exercises (links to system monitoring – see page 21).

The ability to immediately respond to a terrorism incident in one or more locations in order to:

- preserve life and safety
- develop situational awareness
- prevent escalation, neutralise threats and apprehend offenders
- contain situations, e.g. via evacuation, fire management, hazardous material identification and neutralisation, location security, tightened border controls...

This includes the ability to rapidly assess needs, to structure, manage and integrate a response, and to equip and scale it up as required.

Manage incident consequences

The ability to understand and manage the immediate consequences of an incident, possibly while elements of the initial response continue. This may include, for example, the ability to:

- treat and / or identify victims
- extend physical security measures
- address the risk of follow-up, copycat and / or revenge attacks
- restore essential services and ensure their continuity
- shelter, feed and support displaced people (welfare management, logistics management)
- provide support to New Zealanders overseas
- coordinate offers or requests for international support
- inform and support foreign missions to fulfil their obligations to their nationals affected by an incident in New Zealand.

Support decision-makers

The ability to provide information, advice and support that enables right-sized governance and oversight of the response to an incident, including in accordance with the Coordinated Incident Management System, National Security System and National CT Handbook as applicable.

Manage public and targeted communications

The ability to, in a timely fashion:

- coordinate the provision of appropriate and clear information and safety messages to the public through suitable channels
- identify, engage and communicate with groups requiring additional information and support, in particular those targeted by an attack
- monitor media activity and liaise with media organisations
- monitor and manage communications through diplomatic channels and international media.

Manage offenders

The ability to:

- build and prosecute criminal cases (links to the ability to conduct investigations – see page 18)
- manage suspects in custody and monitor those released subject to conditions.

Recover from terrorism incidents

Support the welfare and recovery of victims, families, communities and organisations

The ability to understand the needs of affected individuals, communities and organisations, and to work appropriately with and for them, in order to:

- support them to navigate the aftermath of an incident
- address longer-term physical, psychological, social, financial, economic and / or environmental consequences.

Effective support should also prevent further victimisation and / or address the risk of survivors themselves becoming radicalised.

Improve system preparedness

The ability to review and apply experience to improve the CT / CVE system. This includes ensuring learnings inform policies, processes, doctrine, education, incident readiness (see page 20) and future system reviews (see below).

Enabling capabilities

Enabling capabilities are foundational. They may be deployed to manage the system or in support of any core capability

Coordinate the system

Set strategic priorities and plans

The ability to develop, test, consult on, approve, report and evaluate strategic priorities, risk thresholds and plans (e.g. incident response and recovery plans) across the CT / CVE system.

Coordinate functions, capabilities and change

The ability to:

- plan, coordinate and integrate functions and capabilities at the system level
- agree how agencies will work together and with community groups and other organisations to manage prevention, protection and response work appropriately and effectively
- define, agree, communicate and operationally manage agency responsibility boundaries and transition / handover points
- collectively set expectations and share information between agencies on an ongoing basis to help manage the risk activities come into conflict or that capabilities are unnecessarily duplicated
- identify inter-organisational and international collaboration, secondment and training / cross-training needs and opportunities (links to shared capability operation – see page 23)
- plan, deliver and integrate new capabilities and capability enhancements, both through incremental improvement and more substantial / structured change initiatives
- ensure system-level coordination is right-sized and does not impose unnecessary overheads on agencies.

Monitor and review system performance

The ability to:

- specify, track and report appropriate success criteria and assurance information
- inform and support oversight bodies
- plan, run and review exercises (links to maintaining response readiness – see page 20)
- translate learnings into system improvements.

Administer legislation and regulation

This includes the implementation and proactive stewardship of legislative and regulatory frameworks to provide assurance they uphold the rule of law, remain fit-for-purpose and are consistent with democratic rights and freedoms.

Advise and support decision-makers

The ability to provide policy, legal and technical advice that is timely, evidence-based and of high quality. This includes ensuring there is consistency with:

- the Treaty of Waitangi
- human rights, criminal justice and cyber security policy
- New Zealand's international obligations.

Collaborate and communicate

Manage stakeholder relationships and engagement

The ability to:

- identify, develop and manage enduring and effective domestic and international partnerships and stakeholder relationships across the public (central and local government), community, academic and private sectors
- understand stakeholder information and support needs
- understand how stakeholders may contribute to countering terrorism and violent extremism, including parties not traditionally seen as working in this domain
- establish and manage formal agreements where these are appropriate
- effectively and sustainably coordinate engagement and consultation, demonstrating openness, accountability and system integration.

Deliver public information and guidance

The ability to sustainably identify, develop and deliver (through appropriate channels, including via third parties) appropriate audience-specific and public communications and guidance regarding, for example (not limited to):

- the domestic and international threat environment
- how to stay safe
- how to respond to incidents
- accessing assistance
- recognising signs of radicalisation
- how to report concerns
- protective security obligations and solutions, including educating people for whom parties have a duty of care.

Build internal system awareness and understanding

The ability to ensure agencies possess the awareness and capability (including cultural and diversity competencies and representation) required to:

- design and deliver public services that are inclusive, respectful, relevant to community needs, informed by Te Tiriti o Waitangi, and reflect New Zealand's values
- work sensitively and effectively with and on behalf of communities, for example (not limited to) ethnic, faith and LGBTQI+ communities
- build baseline understanding of CT / CVE issues within the government workforce.

Share and leverage system capabilities

The ability to:

- share knowledge of agency capabilities that may be made available to others
- share expertise and resources across the system, including to help meet surge demand
- establish, provision, manage and govern capabilities as shared services when appropriate, to drive system effectiveness and / or efficiency improvements.

Contribute to international efforts

The ability to lead or otherwise meaningfully contribute to international CT / CVE initiatives that align to New Zealand's values, including via:

- engagement, cooperation and advocacy, including through participation in multi-lateral fora
- meeting United Nations reporting requirements
- secondments and deployments
- providing and / or funding capability development programmes.

Manage, share and utilise information / data

The ability to:

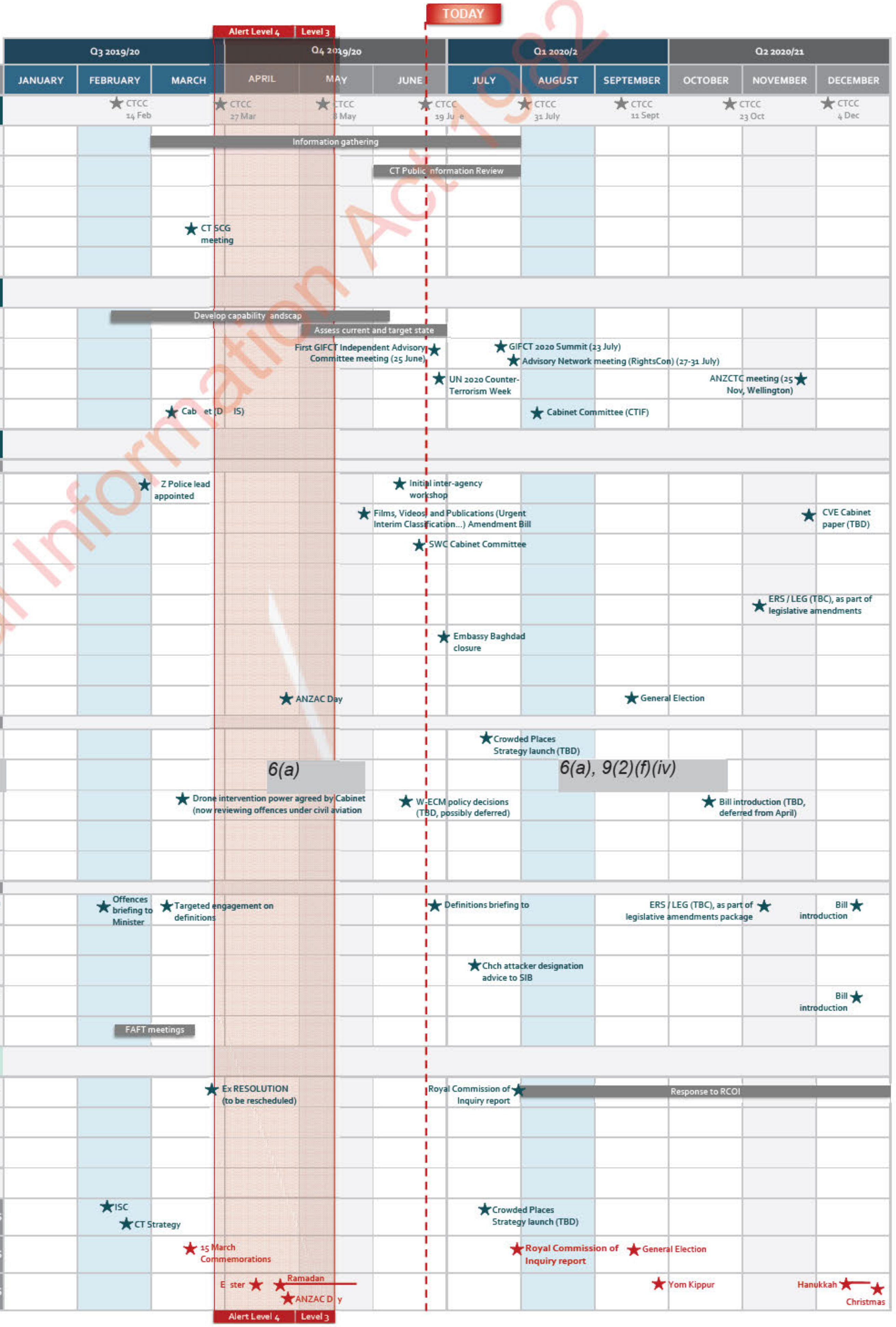
- identify information requirements and sources
- secure and manage holdings
- maintain appropriate cross-system awareness of available holdings
- manage appropriate access, collaboration sharing and transfer within and between domestic and international organisations
- agree and utilise standards to support cross-system understanding and sharing
- link, 'mine' and analyse large and complex datasets.

ODESC
Officials' Committee for Domestic and External Security Coordination

Counter-terrorism Coordination Committee
ctcc@dpmc.govt.nz

CT STRATEGY IMPLEMENTATION PLAN - 2020

Work Stream	Goal	Lead	CTCC Review	Status	Risk / Issues & Comments
REDUCTION Mōhio - Understand	We detect and understand the threat, while our people look out for each other and we all know what to do when something happens.				
Information Access and Sharing	Appropriate information is available to agencies to proactively identify terrorist and violent protest threats and manage residual risk.	NZSIS & DPMC	TBD	🟨	DPMC / NZSIS-led information gathering underway (delayed due to COVID-19).
Public Information	New Zealanders have the information they need to be aware, engaged, and know what to do to stay safe.	DPMC	TBD	🟨	CT Comms Working Group established to manage action plan, and cordinating with RCOI Response Steering Group (RSG). DPMC comms staff in place.
Strategic Threat Assessment	CTAG to develop and introduce an annual New Zealand Terrorism Threat Environment assessment, to inform priority and risk discussions.	CTAG	-	Complete	Published Dec 2019, unclassified version to be published in the NZSIS Annual Report.
CT NSIP Implementation	Fully implement the structures to support the implementation of the CT NSIP under the updated framework.	DPMC	Post RCOI	🟩	NSIP Qs agreed, SCG last met in March. Light touch NSIPs review isunderway, CT will be considered as part of this after RCOI report.
Risk Profile	Update the Terrorism Risk Profile.	DPMC	2021	Complete	Signed off by SIB in June 2019.
Mahi Tahi - Work Together	We work collectively as a nation to reduce and mitigate the risk.				
CT System Capability Review	Review of cross-system CT capabilities to inform the CT Work Programme and capability development options.	DPMC	Jun-20	🟩	DPMC-led review delayed due to COVID-19 but initial phase scheduled to complete at end of June. Ongoing agency input required.
Christchurch Call	Lead the Christchurch Call to Action to eliminate terrorist and violent extremist content online.	MFAT	TBD	🟩	Priorities are engaging with newly independent GIFCT, crisis response mechanisms, understanding algorithmic outcomes and research landscape.
International CT Engagement and Posture	Support the efforts of the international community to counter terrorism and violent extremism at the global, regional and national levels.	MFAT	TBD	🟨	Heavy COVID-19 impact. Some forums now being held virtually, potentially in person in coming months. Risk for NZ if unable to contribute appropriately.
International Deployments	Cabinet to confirm Middle East and other deployments.	NZDF & MFAT	TBD	🟨	Defeat ISIS Cabinet paper approved. CTIF Cabinet paper scheduled for Cabinet in August 2020.
Whakahōtaetae - Prevent	We focus our efforts and capabilities on effective, long-term prevention.				
Reduce the Threat					
Disengagement and MACIP	Establish a broader, more structured inter-agency model / programme for the case management of violent extremism risk individuals.	NZP	TBD	🟨	First inter-agency workshop held. Key milestones: establish criteria, approve case management pilot, explore risk assessment tool benefits.
CVE Online	Deliver CVE online content work programme via operational improvements, legislative change, and media content regulatory review.	DIA	TBD	🟨	Bill introduced on 26 May. DIA team established, key positions being filled, inter-agency planning underway. Research contract signed.
Social Inclusion	Progress and strengthen connections of government actions to build social inclusion.	MSD	TBD	🟨	Report-back on improving social inclusion lodged for consideration at Cabinet Social Wellbeing Committee (SWC) on 17 June.
Community Engagement	*[TBD]*	DPMC	TBD	🟩	Establishment of CTCC Community Engagement Subgroup agree at 19 June meeting.
Control Orders	Terrorism Suppression (Control Orders) Act passed in late 2019. Expand control orders to terrorism-related offenders (including FVPCA offenders).	MOJ	TBD	🟥	Policy development underway to expand control orders. Will be taken to Cabinet following the formation of the next Government.
FTF Planning	Agree policy and operational frameworks for managing New Zealand FTFs. Determine repatriation options.	DPMC	TBD	Complete	Frameworks agreed, but situation remains volatile. Limited repatriation options and no further planning will be undertaken at this stage.
Hate Speech	Ensure the incitement provisions in the Human Rights Act 1993 provide for adequate protection against hate speech.	MOJ	TBD	🟩	Policy development underway, decisions yet to be taken on possible timing for consultation on proposed changes.
Major Events	Support the Major Event Security Committee (MESC) to monitor and enable security planning by lead agencies.	DPMC	TBD	Ongoing	Focus is currently on the 2020 general election, America's Cup, and APEC 2021.
Address Vulnerabilities					
Crowded Places	Develop and role out a Crowded Places Strategy and guidelines for owners and operators.	NZP	TBD	🟩	Strategy developed and Crowded Places Advisory Group (CPAGNZ) established. Public engagement started, launch delayed by COVID-19.
Transport Security	Develop and implement work programme to address key security risks and vulnerabilities across the transport sector.	MOT & Sector	TBD	🟩	9(2)(f)(iv)
Drones	Implement effective legislative framework and capability to intervene in relation to unlawfully operated drones.	MOT & CAA	TBD	🟨	Policy work progressing well, but Civil Aviation Bill intro delayed (COVID-19). Being managed within wider Civil Aviation Bill project.
Border Systems	Use of border data (goods and passenger) to inform CT targeting and threat discovery. Procurement of technology/tools and trialling collaborative initiatives.	INZ & NZCS	TBD	🟨	COVID19 has hindered work in the passenger space, however has allowed for shift in focus to goods space.
Firearms Reform	Implement updated legislative framework to regulate the use and possession of firearms.	NZP	TBD	🟩	Arms Amendment Act and buy-back operation complete. Arms Legislation Bill in progress.
Disrupt Violent Extremist Activity					
CT Legislation (new offences; definition; extended COs)	Review of Counter Terrorism legislation to ensure offences and definition of terrorist offence are workable and fit for purpose	MOJ	TBD	🟥	Policy dvt and Bill drafting underway. Cabinet policy decisions and intro of Bills to the House will follow formation of a new government.
Terrorist Designations	Review and update as appropriate the terrorist designations framework and processes.	NZP	TBD	🟨	Review of framework at very early stages. Designation of Christchurch attacker under consideration by working group - advice to SIB in July.
Immigration National Security Screening (INSS) Project	Re-engineer National Security Screening to provide an agile system where risks from migrants can be tracked, measured and controlled.	INZ	TBD	🟨	Business case co-presented to INZ Business Change Board on 10 June.
NSI Proceedings	Create to a new regime for managing how national security information is used in proceedings	MOJ	TBD	🟨	Bill being drafted, though delayed due to competing priorities in PCO. Intro to the House will follow formation of a new government.
Terrorist Financing	Agree AML/CFT National Strategy and participate fully in FAFT mutual evaluation process in 2019-20.	MOJ	TBD	🟩	AML/CFT National Strategy released in December 2019. Feedback provided on first draft of FATF report - final due in February 2021
RECOVERY Takatū - Ready to Respond and Recover	We take a victim-centred approach, responding swiftly to protect lives and working in partnership to ensure recovery.				
Learning System	Respond to RCOI recommendations. Incorporate CT elements into any NSS centralised lessons management system. Run effective CT exercises.	DPMC	TBD	🟨	RCOI report delayed until 31 July. No progress on lessons management system. Ex RESOLUTION postponed due to COVID-19.
RESPONSE NZDF Support to Agencies	Clarify NZDF CT support to agencies under the Defence Act in the event of a terrorist incident.	MOD, NZDF NZDF	TBD	🟨	Currently working to understand gaps and opportunities.
READINESS CT Handbook Refresh	Review and publish the CT Handbook.	DPMC	-	Complete	Refresh completed in October 2019 and disseminated to agencies.
Threat Level System	Confirm changes to national terrorism threat level processes and decision-making.	DPMC & NZSIS	-	Complete	Signed off by Cabinet in Sept 2019.



Counter-Terrorism Work Programme 2021

CTCC 2021-04-01 – Item 4B

INITIATIVE	OVERVIEW	LEAD(S)	KEY WORKSTREAMS	RCOI RECS	NEXT KEY MILESTONE
Increase direct engagement and public communications	Lift capability and increase efforts to work with, within and on behalf of communities. Successful engagement and communication on matters relating to terrorism and violent extremism: ▪ Helps agencies build the trust and confidence that underpins our social licence to operate in often highly sensitive situations. ▪ Increases public understanding of the nature of threats and what people can do to protect themselves and others.	**DPMC** to lead strategic approach. **CTCC agencies** to lead public engagement and communication.	• RCOI engagement (DPMC) • Advisory Group on CT (DPMC) • Publish indicators and risk factors (NZSIS) • National Centre of Excellence (DPMC) • Coordinated public information (DPMC) • Annual CT Hui (DPMC)	- Rec 7 Rec 13 Rec 14 Rec 15 Rec 16	*9(2)(f)(iv)* [redacted]
Enhance stewardship of the CT / CVE system	Expand capability coordination and outcomes management: ▪ Enhance the identification, coordination and deployment of capabilities across the system to support efficient use of what are often specialist competencies and limited resources. ▪ Extend the CTCC work programme's Learning System workstream (including extending CT exercise programmes) to enhance system testing, reflection and lesson management.	**DPMC** to lead, through CTCC.	• New Intelligence and Security Agency (DPMC) • Clearer system roles and resp nsibilities (DPMC)	Rec 2 -	[redacted]
Grow workforce awareness and diversity	Continue and expand work to: ▪ Build baseline understanding of CT / CVE issues within the wider public sector, and depth of CT expertise across the workforce. ▪ Support and promote diversity, inclusion and cultural awareness within the national security workforce.	**DPMC** to lead, with diversity aspects led through National Security Workforce (NSW) programme.	• Grow workforce CT awareness (*TBD*) • Papa Pounamu (PSC) • NSW Programme (DPMC)	Rec 9 Rec 33 & 34 -	[redacted]
Enhance threat discovery and assessment	Expand capabilities and integration to: ▪ Assess and communicate the CT / CVE threatscape and associated vulnerabilities. ▪ Generate and investigate 'high quality' leads.	**NZSIS / CTAG** to lead.	• Threat discovery and leads (NZSIS) • Joint online threat discovery (NZSIS) • Single accessible reporting system (NZP) • Te Raranga (NZP)	- - Rec 12 Rec 42	[redacted]
Enhance information access, sharing and analysis	Enhance access to information to support threat identification and assessment, the provision of protective security advice, and the evidence used to inform investigations and interventions. **[This initiative is significantly broader than CT / CVE. It encompasses aspects across the national security system and the public sector, including the GCDO and GCISO roles.]**	**Recommend this requires stand-alone review / project sponsored by SIB.**	• Amend ISA wrt direct access agreements (DPMC) • Security clearances and access to information systems (NZSIS / GCSB)	Rec 10 Rec 11	[redacted]
Extend and support PCVE programmes	Develop a strategic approach to Preventing and Countering Violent Extremism (PCVE) with a focus on prevention and disengagement initiatives, then implement action plan across targeted areas.	**DPMC** to lead development of strategic approach. **CTCC agencies** to implement.	• P/CVE Strategic Framework (DPMC) • CVE online (DIA) • Disengagement (NZP)	Rec 4 Rec 41 -	[redacted]
Enhance protection of people and places	Continue and expand work to protect people and places, including enhancing CT legislation, addressing gaps in intervention capabilities, and building on the Crowded Places Strategy and Safer Communities Fund.	Lead(s) per key workstreams, including **MOJ, NZ Police and DIA.**	• Strengthen NZ's CT laws (MOJ) • Change hate speech legislation (MOJ) • Crowded Places Strategy (NZP) • Extend Safer Communities Fund (DIA) • *6(a)* [redacted]	Rec 18 Rec 40 - - -	[redacted]
Under-pinned by **Social cohesion**	*Existing work programme underway, under separate governance arrangements.*	*MSD lead through Social Cohesion Oversight Group.*	• *[Per social cohesion work programme]*	*[Various]*	[redacted]

Cover Sheet for SIB Item 4

Meeting Date	11 November 2020
Sponsoring Agency	Counter-Terrorism Coordination Committee
Item Title	CT Update: CT System Capability Review

Purpose

1. This item reports on the findings of the Counter-Terrorism Coordination Committee's (CTCC's) review of government capabilities for countering terrorism and violent extremism. SIB is asked to endorse the review's proposed priority development initiatives, as the basis of the next iteration of the CT Work Programme subject to any changes / additions that might arise from the Royal Commission of Inquiry's (RCOI's) report.

Recommendations

2. It is **recommended** that SIB:

   a. **Note** both the landscape view of system capabilities and the high-level capability maturity evaluations (Item 4C);

   b. **Note** the key capability challenge areas;

   c. **Endorse** the seven proposed priority development initiatives as the basis of the next iteration of the CT Work Programme, subject to the findings / recommendations of the Royal Commission of Inquiry; and

   d. **Note** the proposed cycle for future CT System Capability Reviews.

Comment

3. The CT System Capability Review was commissioned to provide an overview of capabilities for countering terrorism and violent extremism, and options for enhancement. As the first stage of the review, in June 2020 the CTCC ratified a system landscape view across CT / CVE capabilities. Two sets of recommendations for SIB were then endorsed by the CTCC at their most recent meeting on 22 October:

   - Assessed **key capability challenge areas**; and
   - Proposed **priority development initiatives**.

4. The CTCC is seeking SIB's endorsement of the seven proposed priority development initiatives, as the basis of the next iteration of the CT Work Programme. The finalisation of this Work programme will be subject to any changes / additions that might arise from the findings and recommendations of the RCOI's report. These will be considered by the

CTCC as part of the RCOI report response and the finalised CT Work Programme will be provided to SIB in early 2021 for agreement.

Papers accompanying this cover sheet

Item 4B	*Counter-Terrorism System Capability Review*
Item 4C	*CT / CVE System Capability Landscape and Evaluation Summary*
Item 4D	*Proposed Priority Development Initiatives*

Contacts

5. Primary: Andy George (CTCC Chair), *9(2)(a)*

6. Agency representatives:

DPMC	Andy George	Customs	*9(2)(g)(ii)*
GCSB	*6(a)*	NZDF	*9(2)(a)*
MBIE	Dylan Page	NZSIS	*6(a)*
MFAT	Ken Ryan	Police	*9(2)(a)*
MoD	*9(2)(a)*	JDGO	*6(a)*

11 November 2020

Members
Security & Intelligence Board

Counter-Terrorism System Capability Review

Purpose

1. This paper reports on the findings of the Counter-Terrorism Coordination Committee's (CTCC's) review of government capabilities for countering terrorism and violent extremism. SIB is asked to endorse the review's proposed priority development initiatives, as the basis of the next iteration of the CT Work Programme subject to any changes / additions that might arise from the Royal Commission of Inquiry's (RCOI's) report.

Background

2. The CT Work Programme agreed by SIB and overseen by the CTCC includes a 'CT system capability review' workstream. The review was commissioned to provide an overview of capabilities for countering terrorism and violent extremism, and options for enhancement. Its objectives were to:
    - Support the CTCC to meet the CT Strategy's goal that *'our capabilities across government are integrated, effective, efficient, and reflect our values'*;
    - Inform future iterations of the CTCC's annual work programme;
    - Inform the response to the findings of the Royal Commission of Inquiry into the Attack on Christchurch Mosques; and
    - Potentially, provide agencies with information to support the development of investment cases and Budget bids through demonstrating alignment to system priorities.

3. The review was led by DPMC and ran between February and August 2020. CTCC members and representatives of other agencies contributed through a series of meetings and group workshops, as well as through discussion at CTCC meetings.

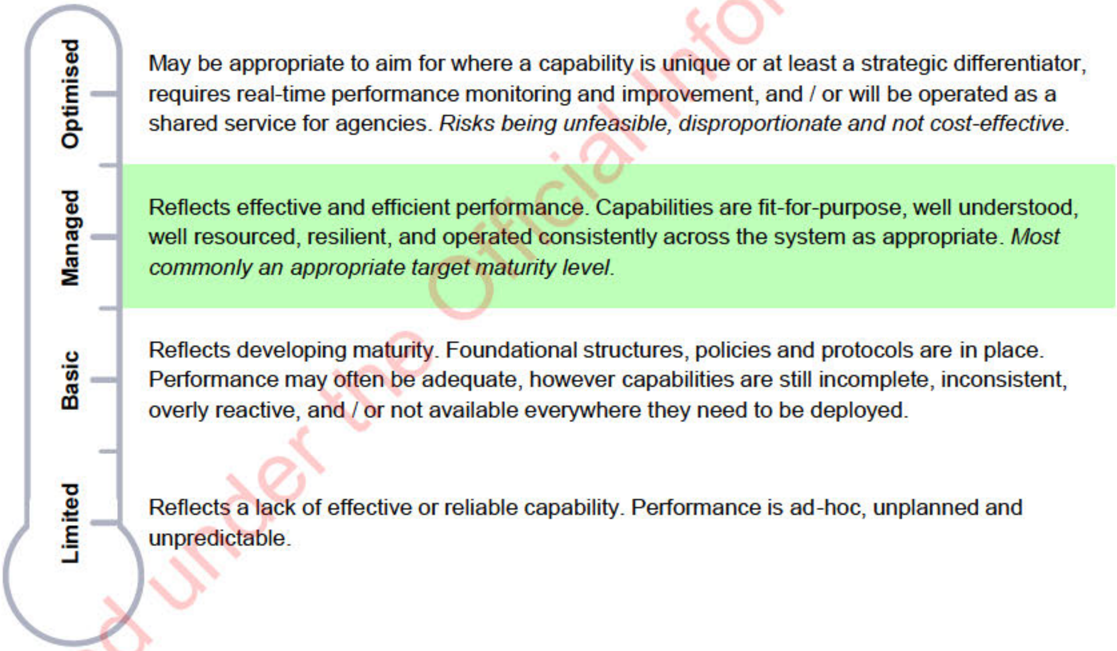
4. As the first stage of the review, in June 2020 the CTCC ratified a system landscape view across CT / CVE capabilities, consisting at the top level of seven core capabilities and two enabling capabilities (Item 4C, with high-level capability maturity evaluations for each). Two sets of recommendations for SIB were then endorsed by the CTCC at their most recent meeting on 22 October:
    - Assessed **key capability challenge areas**; and
    - Proposed **priority development initiatives**.

Capability evaluation

5. A structured qualitative approach was adopted. It was light-touch, informed by workshop discussions and reviews of papers provided. Agencies were not asked to provide detailed evidence.

6. Assessments applied a capability maturity model spanning four dimensions:
   - **Capability management** (design, configuration, oversight, authorising environment outcome monitoring);
   - **Resourcing** (personnel capacity, competency management, asset availability);
   - **Collaboration** (activity integration, interoperability, process performance); and
   - **Information management** (accessibility, quality, management, sharing, IT support).

7. Current and target maturity ratings were assigned to all 37 second-order capabilities, based on the four dimensions noted above and the levels presented in Figure 1 below. The thermometer diagrams in Item 4C represent average results for each of the nine capability groups. Maturity levels of the second-order capabilities within each of those groups can vary widely.



May be appropriate to aim for where a capability is unique or at least a strategic differentiator, requires real-time performance monitoring and improvement, and / or will be operated as a shared service for agencies. *Risks being unfeasible, disproportionate and not cost-effective.*

Reflects effective and efficient performance. Capabilities are fit-for-purpose, well understood, well resourced, resilient, and operated consistently across the system as appropriate. *Most commonly an appropriate target maturity level.*

Reflects developing maturity. Foundational structures, policies and protocols are in place. Performance may often be adequate, however capabilities are still incomplete, inconsistent, overly reactive, and / or not available everywhere they need to be deployed.

Reflects a lack of effective or reliable capability. Performance is ad-hoc, unplanned and unpredictable.

Figure 1: Capability maturity levels.

Key capability challenge areas

8. *6(a)* [redacted]

6(a)

[redacted]

Proposed priority development initiatives

9. Based on these key capability challenge areas, seven candidate initiatives were endorsed by the CTCC as priorities to develop capability across the system. The initiatives are detailed in Item 4D and summarised below (not in any priority order):

Increase public communications and direct engagement	***DPMC*** *to lead strategic approach;* ***CTCC agencies*** *to lead public communications and engagement.*
Enhance stewardship of the CT / CVE system	***DPMC*** *to lead, through CTCC.*
Grow workforce awareness and diversity	***DPMC*** *to lead, with diversity aspects led through National Security Workforce programme.*
Enhance threat discovery and assessment	***NZSIS / CTAG*** *to lead.*
Enhance information access, sharing and analysis	***[Significantly broader than CT; requires stand-alone review / project sponsored by SIB.]***
Extend and support PCVE programmes	***DIA and DPMC*** *to lead development of strategic approach;* ***CTCC agencies*** *to implement.*
Enhance protection of people and places	*Lead(s)* ***TBD****.*

Figure 2: Summary of proposed priority initiatives. levels.

10. **Social inclusion** remains a key enabler for delivering the *CT Strategy*, but is not included in these proposed priority development initiatives as it has its own work programme led by MSD and governed separately to the CTCC and SIB. It is proposed that the CTCC continues to receive regular updates from MSD on the progress of the social inclusion

work programme and maintain strong linkages to ensure CT / CVE components are reflected within it.

Next steps – the CT Work Programme

11. The CT System Capability Review has been deliberately timed to ensure that it has been completed and considered / endorsed by SIB prior to the RCOI's report. This:

    - Has ensured that the review process represents the collective view of CTCC agencies without being directly influenced by the RCOI's findings; and
    - Will enable the RCOI's recommendations to be considered against a CT capability landscape and set of development priorities that have already been established by the CTCC and SIB.

12. If endorsed by SIB, the seven priority development initiatives summarised above will form the basis of the next iteration of the CT Work Programme, subject to any changes / additions that might arise from the findings and recommendations of the RCOI's report. These will be considered by the CTCC as part of the RCOI report response and the finalised CT Work Programme will be provided to SIB in early 2021 for agreement.

13. The CTCC has endorsed an annual cycle of capability maturity evaluations to assess the progress being made and inform future updates to the CT Work Programme. A full CT System Capability Review will be conducted every three years.

Recommendations

14. It is **recommended** that SIB:

    a. **Note** both the landscape view of system capabilities and the high-level capability maturity evaluations.

    b. **Note** the key capability challenge areas.

    c. **Endorse** the seven proposed priority development initiatives as the basis of the next iteration of the CT Work Programme, subject to the findings / recommendations of the Royal Commission of Inquiry.

    d. **Note** the proposed cycle for future CT System Capability Reviews.

2020-11-11 SIB Item 4D

Counter-Terrorism System Capability Review: Proposed Priority Development Initiatives

INITIATIVE	OVERVIEW	LEAD(S)	COMMENTS
Increase public communications and direct engagement	Lift capability and increase efforts to work with, within and on behalf of communities. Successful communication and engagement on matters relating to terrorism and violent extremism: ▪ Helps agencies build the trust and confidence that underpins our social licence to operate in often highly sensitive situations. ▪ Increases public understanding of the nature of threats and what people can do to protect themselves and others.	**DPMC** to lead strategic approach. **CTCC agencies** to lead public communications and engagement.	*6(a)* [redacted]
Enhance stewardship of the CT / CVE system	Expand capability coordination and outcomes management: ▪ Enhance the identification, coordination and deployment of capabilities across the system to support efficient use of what are often specialist competencies and limited resources. ▪ Extend the CTCC work programme's Learning System workstream (including extending CT exercise programmes) to enhance system testing, reflection and lesson management.	**DPMC** to lead, through CTCC.	[redacted]
Grow workforce awareness and diversity	Continue and expand work to: ▪ Build baseline understanding of CT / CVE issues within the wider public sector, and depth of CT expertise across the workforce. ▪ Support and promote diversity, inclusion and cultural awareness within the national security workforce.	**DPMC** to lead, with diversity aspects led through National Security Workforce (NSW) programme.	[redacted]
Enhance threat discovery and assessment	Expand capabilities and integration to: ▪ Assess and communicate the CT / CVE threatscape and associated vulnerabilities. ▪ Generate and investigate 'high quality' leads.	**NZSIS / CTAG** to lead.	[redacted]
Enhance information access, sharing and analysis	Enhance access to information to support threat identification and assessment, the provision of protective security advice, and the evidence used to inform investigations and interventions. **[This initiative is significantly broader than CT / CVE. It encompasses aspects across the national security system and the public sector, including the GCDO and GCISO roles.]**	**Recommend this requires stand-alone review / project sponsored by SIB.**	[redacted]
Extend and support PCVE programmes	Develop a strategic approach to Preventing and Countering Violent Extremism (PCVE) with a focus on prevention and disengagement initiatives, then implement action plan across targeted areas.	**DIA and DPMC** to lead development of strategic approach. **CTCC agencies** to implement.	[redacted]
Enhance protection of people and places	Continue and expand work to protect people and places, including enhancing CT legislation, addressing gaps in intervention capabilities, and building on the Crowded Places Strategy and Safer Communities Fund.	Lead(s) **TBD**, agencies include **MOJ, NZ Police, DPMC and DIA**.	[redacted]
Plus **Social inclusion**	*Existing work programme underway, under separate governance arrangements.*	***MSD** lead through Social Inclusion Oversight Group.*	[redacted]