Controller and Auditor-General
Tumuaki o te Mana Arotake

B.29 [16w]

Governance of the National Security System

Photo acknowledgement:
mychillybin © Karen Williamson

Governance of the National Security System

Presented to the House of Representatives under section 20 of the Public Audit Act 2001.

November 2016

ISBN 978-0-478-44252-6

Contents

Auditor-General's overview

National security arrangements are probably not matters that most New Zealanders would think about often, but they are important to all of our lives. Although a level of secrecy is needed, the National Security System needs to strike the right balance between secrecy and transparency if we are to trust it.

My Office carried out a performance audit to provide assurance to Parliament and the public about the effectiveness of governance arrangements for the National Security System.

We looked at the governance arrangements for responding to national security events, identifying and managing risks, and building national resilience. We used the eight elements of good governance published in our recent report, *Reflections from our audits: Governance and accountability,* to assess governance.

As part of our audit, we examined two examples of how the National Security System responded to recent threats. These were the threat to contaminate infant milk formula with 1080 poison (Operation Concord) and the response to terrorist attacks in Paris in November 2015. We also observed the first day of an exercise (Exercise Tangaroa) simulating a national response to a tsunami.

In my view, the governance arrangements for responding to national security events and emergencies are well established, fundamentally sound, and fit for purpose. The response to Operation Concord was an example of the National Security System working well.

The "response" side of the National Security System

The right people come together and there are strong, trusting, and respectful relationships between them. This provides a solid platform for effective governance and enables the National Security System to respond well. The National Security Systems Directorate[1] generally supports the response side of the system well and is providing better support over time.

There is a National Exercise Programme, which allows the main parties to practise responding and learn lessons. This contributes to ensuring that all-of-government responses to national security events and emergencies are governed effectively.

The "governance" side of the National Security System

New governance arrangements were introduced in 2014. Since then, the governance of how national security risks are managed and how our national resilience is strengthened has started to improve. The right people are on the various boards that make up the "governance" side of the National Security System and their strong, trusting, and respectful relationships are enabling the

1 The National Security Systems Directorate is a business unit in the Department of the Prime Minister and Cabinet, which serves as the secretariat for the National Security System.

new governance arrangements to mature quickly. The National Security Systems Directorate is providing more strategic support for governance.

Getting to a world-class national security system

The Department of the Prime Minister and Cabinet (DPMC) aspires to have a world-class national security system. New Zealand's security system has some of the characteristics of a world-class system. For example, the system can quickly mobilise a network of people and there are clear frameworks for managing the response to national security events and emergencies.

DPMC is making further improvements as it works towards a world-class national security system. In our view, those further improvements are needed. The work under way to define national security risks is particularly important, and clearer and stronger accountabilities for risk management and reporting are needed.

Information flows, particularly for classified information, need to improve throughout the National Security System. For the System to be more resilient and operate in a sustained and seamless way, it also needs to be supported by processes that better identify, record, and transfer institutional knowledge. Lessons identified from activating the National Security System and exercises need to be recorded and applied more consistently. People coming into the National Security System also need to be inducted deliberately and methodically.

DPMC has responded positively to our recommendations and has already talked to us about its plans to address them.

I thank the staff of DPMC and the other agencies, including the many chief executives we interviewed, for their time and co-operation with our audit. It is reassuring to know that New Zealand can call on an experienced, dedicated, and resolute network of people to come together constructively and quickly when needed, to help ensure our national security.

Lyn Provost
Controller and Auditor-General

24 November 2016

Our recommendations

The National Security System needs to be flexible, agile, and effective in responding to national security events and emergencies. It also needs to be resilient, because the risks it manages and the personnel involved in governing and operating the System change over time.

We recommend that the Department of the Prime Minister and Cabinet:

1. sharpen the focus of governance of the management of national security risks and of national resilience-building by:
   - using the work it is doing to define national security risks to establish clear accountabilities for governance of the management risks, and reporting regularly against the accountabilities; and
   - rationalising the number of subgroups beneath the main governance boards and clarifying lines of accountability between the subgroups and the boards.
2. strengthen the resilience of the National Security System by:
   - enabling easier and more efficient information flows, particularly of classified information, throughout the System;
   - capturing institutional knowledge to build a knowledge bank that people in the System can draw on for future responses;
   - capturing and applying lessons from activations of the System and exercises more methodically; and
   - introducing more methodical induction, training, and development of people moving into different roles in the System.

1 Introduction

1.1 In this Part, we discuss:

- why we did our audit;
- who and what we audited;
- how we carried out our audit;
- what we did not audit; and
- the structure of this report.

Why we did our audit

1.2 The Department of the Prime Minister and Cabinet (DPMC) has a strategic objective to ensure that national security priorities, the civil defence emergency management system, and the intelligence system are well led, well co-ordinated, and well managed.

1.3 The National Security System (the System) provides the platform for governance of national security. The System needs to be governed effectively so it can prepare for, and respond to, national security events and emergencies well.

1.4 New Zealand takes a holistic and integrated approach to managing national security risks. Known as "the 4Rs", this approach includes:

- Reduction — identifying and analysing long-term risks and taking steps to eliminate these risks if practicable, or if not, to reduce their likelihood and the magnitude of their impact;
- Readiness — developing operational 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.[2]

1.5 Given the importance of national security to all of us, we considered it important to provide assurance to Parliament and the public about the effectiveness of the governance arrangements for the System.

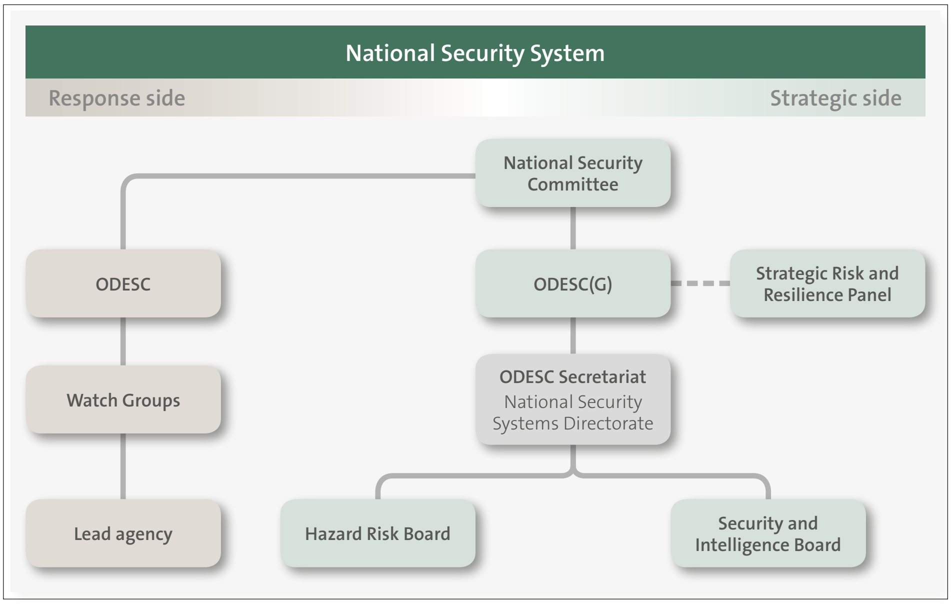
Who and what we audited

1.6 We carried out a performance audit to assess how well the System is governed. People working in the System refer to a "response" side and a "governance" side. We looked at the governance arrangements for both. Referring to governance arrangements for the governance side of the System could be confusing. For ease of reading, we refer to a response side and a strategic side (see Figure 1).

2 From the *National Security System Handbook*. See dpmc.govt.nz/national-security.

1.7 We wanted to know whether governance structures on the response side enable responses to national security events and emergencies to be managed effectively. We also wanted to know whether governance structures on the strategic side contribute to national resilience-building and risk management.

Figure 1
The National Security System, response side and strategic side



1.8 DPMC is responsible for co-ordinating and supporting the System, as well as providing risk management advice to the Government. Support for the System is largely delivered by DPMC's Security and Intelligence Group. Within this group, the National Security Systems Directorate (the Directorate) has specific responsibility for:

- co-ordinating all-of-government responses to national security events; and
- providing support to the strategic side.

1.9 In its 2014/15 annual report, DPMC said that it will work to ensure that New Zealand has world-class processes for identifying and dealing with national security events and emergencies, and for building national resilience.

1.10 We considered DPMC's desire to have a world-class system as we carried out our audit and measured DPMC against that high standard.

How we carried out our audit

1.11 To assess how well the System is governed, we used the eight elements of good governance published in our recent report, *Reflections from our audits: Governance and accountability*.

1.12 The eight elements of good governance are:

- set a clear purpose and stay focused on it;
- have clear roles and responsibilities that separate governance and management;
- lead by setting a constructive tone;
- involve the right people;
- invest in effective relationships built on trust and respect;
- be clear about accountabilities and transparent about performance against them;
- manage risks effectively; and
- ensure that you have good information, systems, and controls.

1.13 We looked at whether these elements were in place for the System, and whether they were providing effective governance of the System. Governance of the System needs to enable agencies to work together in a co-ordinated way. Information also needs to flow through the System effectively and efficiently.

1.14 We interviewed staff involved in the governance of the response side and the strategic side of the System. We also reviewed and analysed relevant documents, mostly from DPMC.

1.15 We looked at two examples of recent responses to assess the response side of the System. Figure 2 sets out background information about each response, the main agencies involved, and the duration of the response.

Figure 2
The National Security System responses that we selected as examples for our audit

Example	Reason for system activation	Key agencies involved	Duration of response
Operation Concord	Fonterra and Federated Farmers received anonymous letters threatening to contaminate infant formula and other formula products with 1080 poison.	Ministry for Primary Industries New Zealand Police Ministry of Foreign Affairs and Trade Ministry of Health	November 2014 to March 2015
Paris attacks	A series of terrorist attacks, including several suicide bombings and mass shootings, took place in Paris in November 2015. It was initially uncertain whether the attacks posed a threat to New Zealand or whether they would have other implications that might affect the country, so the System was activated to consider possibilities.	Ministry of Foreign Affairs and Trade New Zealand Police New Zealand Defence Force	November 2015

1.16 We also observed governance meetings that DPMC convened to co-ordinate responses to two national security events that took place during our audit. We did not fully assess how the responses to these events were governed because the responses were not completed when we wrote this report. However, our observations about the responses have contributed to our overall audit findings.

1.17 As part of our assessment of governance of the strategic side of the System, we observed the first day of Exercise Tangaroa. Exercise Tangaroa was a national exercise to test New Zealand's preparations for, response to, and recovery from a nationally significant tsunami.

1.18 In late 2013, the strategic side of the System was reorganised. Our performance audit was the first external review of that relatively new structure.

1.19 We looked at the boards involved in the strategic side of the System. We looked at how the boards have been operating since the new structure was established. These boards are described in Part 2, and they are:

- the Officials' Committee for Domestic and External Security Coordination (Governance);
- the Security and Intelligence Board;
- the Hazard Risk Board; and
- the Strategic Risk and Resilience Panel.

1.20 For each of the boards, we:

- interviewed members of the board;
- reviewed the terms of reference and charter;
- analysed meeting agendas, minutes, and action points; and
- reviewed documents produced for and by the boards to enable them to fulfil their governance function.

1.21 We assessed how the Directorate supports both sides of the System. We looked at how the Directorate co-ordinates responses to national security events, and how it supports the boards on the strategic side of the System to fulfil their governance functions.

1.22 Our work included reviewing policy and accountability documents and internal review documents. We also interviewed Directorate staff and members of the various groups and boards that they support on the response and strategic sides of the System.

What we did not audit

1.23 For the two examples we examined – Operation Concord and the Paris attacks – we did not form a view on whether the right response was decided on. Our focus was on the effectiveness of the governance arrangements behind each response.

1.24 Similarly, we did not form a view on whether the strategic side of the System focuses on the right risks.

1.25 We did not audit the work of subcommittees and working groups reporting to the boards on the strategic side of the System. Our focus was on how clear the lines of governance and accountability were between the boards and these subcommittees and working groups.

1.26 Some agencies have specific roles in responding to national security events. For example, the Ministry of Civil Defence and Emergency Management has a specific role in the event of a civil emergency and the Ministry of Health has a specific role in the event of a pandemic. We did not audit these agencies.

Structure of this report

1.27 In Part 2, we describe the structure of the System. We explain the governance arrangements for the response side and the strategic side in more detail.

1.28 In Part 3, we examine the effectiveness of governance of responses to national security events and describe the aspects of effective governance we observed. We also discuss our observations about the two examples we looked at – Operation Concord and the Paris attacks.

1.29 In Part 4, we examine the effectiveness of the arrangements that govern national security risks and resilience-building (the strategic side of the System). We describe some of the improvements already under way and those that could still be made.

1.30 In Part 5, we discuss how governance needs to continue to improve throughout the System as a whole for it to be a world-class national security system.

2 The National Security System and how it is governed

2.1 In this Part, we discuss:

- what national security is;
- the governance arrangements for responses to national security events and emergencies – the response side of the System; and
- the governance arrangements for managing national security risks and national resilience-building – the strategic side of the System.

What is national security?

2.2 DPMC's *National Security System Handbook* describes national security as the condition that permits the citizens of a state to go about their daily business confidently and free from fear, and to be able to make the most of opportunities to advance their way of life. This condition requires a resilient national security system that is:

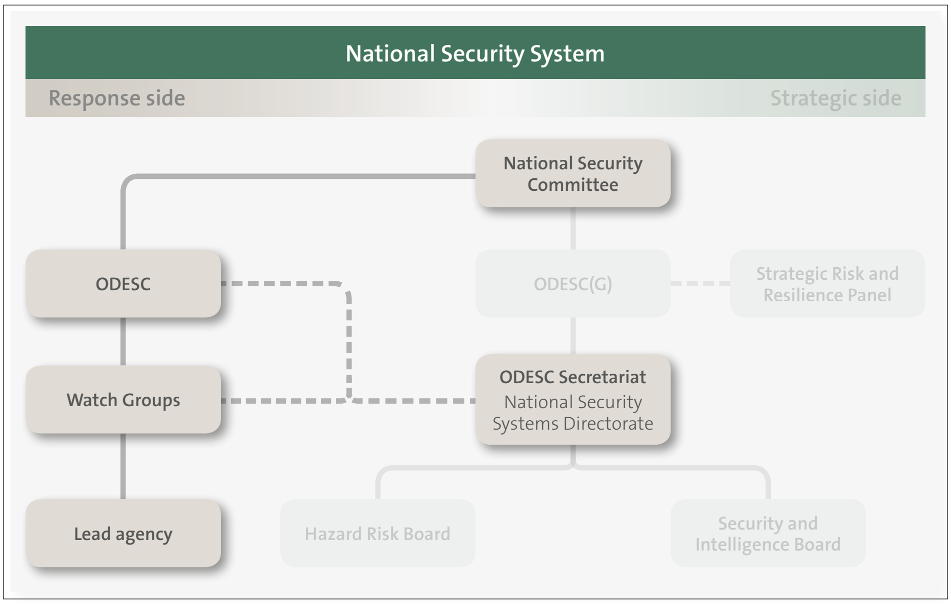
- well led;
- strategically focused;
- co-ordinated;
- cost-effective;
- accountable;
- geared to risk management; and
- responsive to any challenges that arise.

2.3 New Zealand takes an "all hazards, all risks" approach to national security. This means that the System includes all risks to national security, whether internal or external, human or natural. Such risks can include state and armed conflict, transnational organised crime, cyber-security incidents, natural hazards, biosecurity events, and pandemics. In New Zealand, national security is centrally co-ordinated.

Governance arrangements for the response side

2.4 When the System is activated in response to a national security event or emergency, the response side governs and manages the response (see Figure 3). This happened, for example, with the threat to contaminate infant milk formula with 1080 poison, the *TS Rena* grounding, and the Pike River Mine disaster.

Figure 3
The response side of the National Security System



2.5 The response side of the System has been in place since 1987. It has a simple structure that has not changed significantly since it was introduced. There are three levels of governance in the response side of the System:

- The **National Security Committee** is chaired by the Prime Minister. It oversees the national security and intelligence sector, including policy and legislative proposals. The Committee co-ordinates and directs national responses to crises or circumstances (either domestic or international) that affect national security. It includes Ministers with relevant portfolio responsibilities. The National Security Committee reports to Cabinet and has the power to act without further reference to Cabinet in some circumstances.
- The **Officials' Committee for Domestic and External Security Coordination** (ODESC) is chaired by the Chief Executive of DPMC and involves chief executives from a range of agencies, selected by the Chairperson as circumstances require. ODESC's role is to provide strategic direction and co-ordination for the all-of-government response to an event. ODESC reports to the National Security Committee.
- **Watch Groups** are usually chaired by DPMC's Deputy Chief Executive Security and Intelligence or a delegated official from the Directorate and are made up of senior officials from relevant agencies. DPMC may call a Watch Group to monitor a potential, developing, or actual crisis. Watch Groups are responsible for ensuring ongoing, high-level co-ordination between agencies and for co-ordinating assessments and advice up to ODESC.

2.6 The aim of the response structure is to provide a co-ordinated, all-of-government response that identifies and manages risks, is timely, minimises harm, and uses resources appropriately.

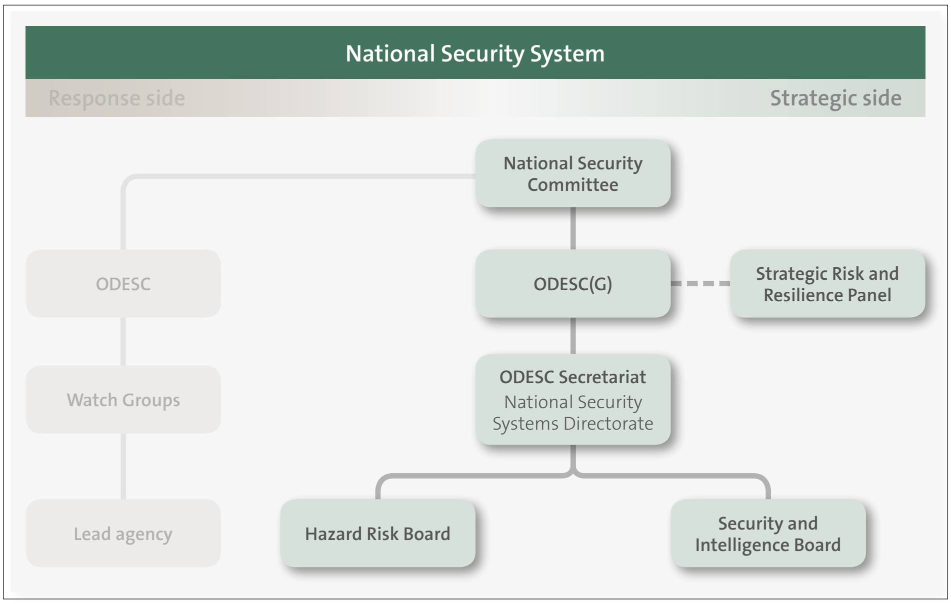
2.7 DPMC activates the System at the request of, or in discussion with, the chief executive of the lead agency.[3] There are several reasons why the System can be activated. According to the *National Security System Handbook*, these include:

- increasing risk, or a disaster or crisis, affects New Zealand interests;
- when active or close co-ordination or extensive resources are required;
- when the crisis might involve risk to New Zealand's international reputation;
- when an issue is of large scale, high intensity, or great complexity;
- to assist with co-ordinating multiple, smaller, simultaneous events; and
- to assist with the early co-ordination of an emerging issue that might meet the above criteria in the future and would benefit from proactive management.

Governance arrangements for the strategic side

2.8 The strategic side of the System focuses on risk management and building national resilience (see Figure 4). This structure has existed since late 2013, and DPMC describes it as a work in progress.

Figure 4
The strategic side of the National Security System



3 For any national security risk (or major element of such a risk), a lead agency is identified. The lead agency is the agency with the primary mandate for managing a particular hazard or risk.

2.9 The strategic side of the System includes several boards, committees, and subcommittees and working groups. We looked at the governance boards on this side of the System. They are:

- the Officials Committee for Domestic and External Security Coordination (Governance), or **ODESC(G)**;
- the **Security and Intelligence Board**;
- the **Hazard Risk Board**; and
- the **Strategic Risk and Resilience Panel**.

2.10 ODESC(G) is the primary governance board overseeing New Zealand's national resilience-building and risk management. ODESC(G) is a different board to the group of officials that meet as ODESC in a response. The similarity of the names causes confusion for some people involved in the System.

2.11 The purpose of ODESC(G) is to ensure that capability and systems are in place to identify major risks facing New Zealand and that suitable arrangements are made throughout government to efficiently and effectively mitigate and manage those risks. ODESC(G) is chaired by the Chief Executive of DPMC. Its members include DPMC's Deputy Chief Executive Security and Intelligence, the Solicitor-General, and Chief Executives from the State Services Commission, the Treasury, the New Zealand Police, the New Zealand Defence Force, the Ministry of Foreign Affairs and Trade, the Ministry for Primary Industries, the Ministry of Defence, and the Ministry of Health. ODESC(G) reports to the National Security Committee.

2.12 The Security and Intelligence Board focuses on external threats and intelligence issues. Its purpose is to build a high-performing, cohesive, and effective security and intelligence sector through appropriate governance, alignment, and prioritisation of investment, policy, and activity. It is chaired by DPMC's Deputy Chief Executive Security and Intelligence, and its members include Chief Executives from DPMC, the Government Communications Security Bureau, the Ministry of Foreign Affairs and Trade, the Ministry of Defence, New Zealand Customs, the New Zealand Defence Force, the New Zealand Police, the Ministry of Business, Innovation and Employment, and the New Zealand Security Intelligence Service. The Security and Intelligence Board reports to ODESC(G).

2.13 The sorts of matters that the Security and Intelligence Board considers include:

- the national security workforce;
- implementing New Zealand's intelligence priorities;
- New Zealand's overseas peacekeeping commitments;
- intelligence and security relationships; and
- counter-terrorism.

2.14 The Hazard Risk Board focuses on a range of hazards and risks, and also has a focus on the overall health of the System. According to the *National Security System Handbook*, the purpose of the Hazard Risk Board is "to build a high performing and resilient National Security System able to manage civil contingencies and hazard risks through appropriate governance, alignment, and prioritisation of investment, policy and activity".

2.15 The Hazard Risk Board is also chaired by DPMC's Deputy Chief Executive Security and Intelligence, and its members include Chief Executives or their delegates from DPMC, the New Zealand Police, the Ministry of Health, the Ministry for Primary Industries, the Ministry of Transport, the New Zealand Defence Force, the Ministry of Foreign Affairs and Trade, the New Zealand Fire Service, and the Ministry of Civil Defence and Emergency Management.

2.16 The sorts of matters that the Hazard Risk Board considers include:

- managing major transport risks and clarifying national arrangements for managing a major transport accident;
- search and rescue capabilities, limitations, readiness, and risks;
- security risks of highly hazardous substances;
- enabling effective oversight of the System's capability, including professional development and the National Exercise Programme; and
- improvements to the System after Operation Concord.

2.17 The Strategic Risk and Resilience Panel is an independent panel that was set up to provide challenge and advice to ODESC(G). According to the National *Security System Handbook*, the purpose of the Strategic Risk and Resilience Panel is "to provide a rigorous and systematic approach to anticipating and mitigating strategic national security risks."

2.18 The Strategic Risk and Resilience Panel has nine members who were selected by the Chairperson of ODESC(G) for their expertise in a wide range of areas in both the public and private sectors. Panel members are independent and do not represent any agencies.

Effectiveness of governance of responses to national security events

3

3.1 In this Part, we discuss:

- how well the response side of the System responded during Operation Concord and after the November 2015 terrorist attacks in Paris;
- the aspects of effective governance that helped the System respond well; and
- ways to improve the governance of the response side of the System.

Summary of our findings

3.2 The response side of the System is fundamentally sound. It has provided an effective and co-ordinated, all-of-government response to recent events. We consider it to be fit for purpose.

3.3 Operation Concord was an example of the System responding at its best. Those involved with Operation Concord, and the response to the Paris attacks, worked together effectively to manage risks.

3.4 The response side of the System is flexible in the way it responds to different types of events. We saw and heard of other times when this side of the System responded well when activated.

3.5 The right people come together to respond. Strong, trusting, and respectful relationships between the people involved in responses provide a solid platform for effective governance, and enable the System to respond well. The Directorate generally supports the response side of the System well and is providing better support over time.

3.6 Some improvements are needed to enhance the governance of responses:

- The roles and accountabilities of the lead agency and DPMC, and the lines of accountability between Watch Groups, ODESC, and Ministers, in a response need to be more clearly defined.
- Better induction processes are needed so that new people involved in the System can quickly learn what is required of them.
- Lessons from activations of the System need to be identified, recorded, and applied in a more methodical way to enable the System to learn and mature quickly and effectively.

3.7 DPMC has some of these improvements under way already.

The National Security System has responded well in the past

3.8 We looked at two examples of recent system activations to assess the response side of the System: Operation Concord and the Paris attacks. Operation Concord was the name given to the response to the threats to contaminate infant formula with 1080 poison received by Fonterra and Federated Farmers in November 2014. The Paris attacks were a series of terrorist attacks in that city, including several suicide bombings and mass shootings, in November 2015.

3.9 For each example, we reviewed:

- meeting agendas and minutes of ODESC and Watch Group meetings;
- communication between Watch Groups, ODESC, the National Security Systems Directorate, and Ministers;
- situation updates from lead agencies;
- documents relating to reviews of each response after the response was deactivated.

3.10 Overall, we found that the System responded well in both examples. The response side of the system was activated promptly, and the different agencies worked effectively together until the response was deactivated.

Figure 5
Examples of effective responses to security threats

Example: Operation Concord

On 27 November 2014, Fonterra received an anonymous letter threatening to contaminate infant and other formula products with 1080 poison. Federated Farmers received a similar letter the next day. Both letters were accompanied by a sachet of infant formula that tested positive for 1080 poison. After receiving the letters, Fonterra and Federated Farmers both immediately informed the Police.

The System was activated the day the first threat was received. A Watch Group convened that evening and met weekly after that. The day after the first threat was received, a meeting of ODESC was called, and it then met fortnightly. Watch Group and ODESC meetings continued regularly between November 2014 (when the threat was received) and March 2015 (when a public announcement about the threats was made).

Elements of effective governance in Operation Concord

The System responded quickly to the threat, provided sound direction for the response, and ensured that the appropriate agencies were working together.

The following elements of effective governance helped enable the response:

- The roles of the lead agency and DPMC were clear.
- The purposes of the meetings were clear.
- The right people were involved in Watch Groups and ODESC, and members demonstrated a willingness to share information, debate issues, provide resources, and work together.
- Information flowed effectively into and out of ODESC and Watch Group meetings, and up to the responsible Minister when necessary.

Example: Paris attacks

On 13 November 2015, several suicide bombings and mass shootings took place throughout Paris, resulting in the deaths of 130 people. Most of the casualties came from the attack on the Bataclan theatre, where gunmen carried out a mass shooting and took hostages.

The System was briefly activated in response to the attacks. It was initially uncertain whether the attacks posed a threat to New Zealand or could otherwise affect the country, so the System was activated to consider possibilities. This was an example of the System activating in response to a potential threat and quickly deactivating when the threat was gone.

Elements of effective governance in the response to the Paris attacks

The System responded quickly to this event. The first Watch Group was convened on a Saturday afternoon, the second Watch Group meeting was on the following Sunday, and the System was deactivated on the following Monday when the potential threat to New Zealand was considered to be over.

The following elements of effective governance helped to enable the response:

- The Watch Groups had a clear purpose, and responsibilities for action items were made clear at both Watch Group meetings.
- The right people attended the Watch Group meetings.
- Agencies represented on the Watch Groups demonstrated a willingness to work together and share responsibility for tasks.
- The Directorate effectively supported the response, by organising meetings, co-ordinating contact with Ministers and Cabinet, and collating relevant information.
- Situation updates flowed regularly from the Ministry of Foreign Affairs and Trade to other relevant agencies and to Ministers.
- Information flowed effectively into Watch Group meetings from agencies, and from the Watch Groups to ODESC.
- Watch Group members carried out their assigned tasks.

Aspects of effective governance of responses

The right people come together to respond

3.11 Overall, the right people are involved in responses. Watch Group and ODESC membership varies depending on the nature of the response. When a Watch Group is called, the Directorate informs the relevant agencies, and they decide who to send to represent them. Members of Watch Groups are usually senior officials who are able to commit resources and agree actions on behalf of their organisations.

3.12 Watch Groups can be large. One Watch Group that we observed involved more than 30 people. There are several reasons why Watch Groups can be large. Sometimes, agencies send representatives from throughout their organisation, including response staff, policy staff, and communications staff. Inviting a wide variety of people means that it is more likely that the right people are there from the start in a time-critical response.

3.13 However, this can also cause problems, because large Watch Groups can be unwieldy and difficult to manage. They can delay progress and be an inefficient use of resources. A balance between ensuring appropriate representation at meetings and not having too many people must be struck. The Directorate is mindful of this when sending out invitations to meetings.

3.14 We saw that, when an ODESC meets, the chief executives from relevant agencies generally attend. This shows that chief executives prioritise attendance at these meetings. When ODESC and Watch Groups meet, the purpose of the meetings is clear. For the examples we looked at, the purpose of Watch Group and ODESC meetings was stated in the records of meetings.

3.15 We observed some ODESC and Watch Group meetings during our audit. For these meetings, the purpose of the meeting was stated when the meeting invite was sent out and again at the beginning of the meeting. In our view, this helped people understand their roles in the response.

Strong relationships mean people work together well to respond

3.16 Strong, trusting, and respectful relationships between the people involved in responses provide a solid platform for effective governance and enable the System to respond well. In the examples we observed, the people involved in responses generally had strong pre-existing relationships. People were open and worked together constructively. This was encouraged and facilitated by the chairpersons of the meetings, and there was constructive challenge and rigorous debate of issues.

3.17 Strong relationships need to be supported by good processes. These processes need to enable and not constrain the agility and flexibility of the System, but also provide continuity for the System to operate effectively over time. For example, it is important to have knowledge management systems and information repositories so that institutional knowledge is not lost when people leave the System (see Part 5).

Accountabilities are clear

3.18 During an incident, Watch Groups are accountable to ODESC and ODESC is accountable to Ministers. Within this accountability framework, specific accountabilities depend on the circumstances of the response and are agreed when Watch Groups and ODESC meet. When accountabilities are agreed at these meetings, they appear to be clear, assigned, understood, and actioned.

The Directorate generally supports the response side well and is providing better support over time

3.19 The Directorate generally provides effective support for Watch Groups and ODESC. For example, in the Operation Concord and Paris attacks examples, the Directorate facilitated information flows between Watch Groups, ODESC, and Ministers. The Directorate also provided support such as risk analysis to help decision-makers consider how to respond.

3.20 As it matures and learns from experience, the Directorate is providing better support for responses. Although we were told of occasions where the Directorate's support for Watch Groups could have been better, most of the people we talked to told us that they had seen improvements over time.

3.21 The Directorate is making ongoing improvements to how it supports the response side of the System. For example:

- The Directorate introduced standard agendas for Watch Groups and produced a *National Security System Handbook* so that officials working within the System are clear about roles, responsibilities, and the purpose of the System. The *National Security System Handbook* has been published on the DPMC website with the intention that it should be available as a resource for all.
- After Operation Concord, the Directorate introduced standard operating procedures for how it supports the response side of the System, including how it prepares to support Watch Groups and ODESC before they meet. The Directorate considers that these standard operating procedures are a way to capture and apply best practice and lessons identified in responses. For example, during Operation Concord, a need for enhanced internal co-ordination before Watch Group and ODESC meetings was identified. The Directorate trialled a new process during an exercise in 2015. The process was found to be useful so has become a standard operating procedure. This is a good example of the Directorate making ongoing improvements.

Ways to improve governance of the response side

Greater clarity is needed on the roles and accountabilities of the lead agency and DPMC in a response

3.22 People generally understood their roles and responsibilities in responses. Those involved in previous responses are clearer about their roles and responsibilities than new people coming in. However, there is occasionally confusion about the distinction between the role of the lead agency and the role of DPMC.

Better induction is needed for new people involved in responses

3.23 New people involved in the System do not always clearly understand what is expected of them. Better induction processes are needed to ensure that new people are able to get up to speed quickly.

3.24 Examples of improvements already made to help improve knowledge throughout the System include developing the *National Security System Handbook* and the officials' courses that DPMC and Victoria University of Wellington have developed.

More systematic identification, recording, and application of lessons is needed

3.25 The response side of the System needs to improve the way that lessons are identified and actioned. There is a process for debriefing after activations of the System, and some lessons have been identified, recorded, and applied. However, lessons from activations and exercises could be collated and co-ordinated in a more systematic and comprehensive way. Particularly, so that lessons identified in one context are considered for application throughout the System.

3.26 Developing a process that records and applies all the lessons identified from responses and exercises should support the System to learn and mature quickly and effectively. DPMC has work under way to identify how to improve the way lessons are identified, recorded, and applied.

Effectiveness of governance of national security risks and resilience-building

4

4.1 In this Part, we discuss:

- how governance of national security risks and resilience-building is maturing over time; and
- improvements under way and improvements that could be made.

Summary of our findings

4.2 Governance of national security risks and resilience-building on the strategic side is maturing. Many of the members of ODESC(G) and the two main governance boards (the Security and Intelligence Board and the Hazard Risk Board) said to us that the current governance structures for the strategic side of the System were an improvement on the previous structures and were providing better governance over time.

4.3 The right people are coming together with greater purpose. Strong, trusting, and respectful relationships established over time between members of ODESC(G) and its boards are enabling the governance of national security risks and national resilience to mature quickly.

4.4 The Directorate is providing more strategic support for improving governance over time. Also, the National Exercise Programme helps the System to be prepared. Allowing the main players to practise responding, and to learn lessons, should help ensure that governance of all-of-government responses to national security events and emergencies is effective.

4.5 Some improvements are under way and others can be made for governance of the strategic side of the System to continue to mature quickly and to be fully effective. The work to define national security risks is particularly important for ODESC(G) to be more effective as the overall governance body for overseeing management of national security risks and resilience-building.

4.6 Clearer and stronger accountabilities are needed throughout the strategic side of the System. Identifying risks is also important to achieving this by providing a better framework for delegating accountabilities for risks from ODESC(G) to the boards and subgroups, and reporting against the delegated accountabilities. Work to achieve this is under way.

How governance of national security risks and resilience-building is maturing over time

4.7 In contrast to the governance structures for the response side of the System, which have remained significantly unchanged since they were introduced, the governance structures for the strategic side have changed over time. Governance of national security risks and resilience-building through the most recently introduced structures is maturing.

The current governance structures provide a better platform for effective governance

4.8 In 2013, DPMC carried out an internal review of the arrangements for co-ordinating national security and intelligence priorities. Also in 2013, the State Services Commission completed a Performance Improvement Framework (PIF) review of DPMC. The PIF review's findings about governance of national security risks and resilience-building included that DPMC needed to ensure:

- that appropriate governance was in place and roles and responsibilities were clear to mitigate and manage risk in new threat areas, including through further refining and rationalising the governance structures so that they were targeted to deal with specific risks and responsibilities; and
- that appropriate co-ordination and leadership of the roles and responsibilities of all relevant agencies.

4.9 After the reviews, the current structures for governance of national security risks and resilience-building (see Figure 4) were introduced in late 2013. Many of the members of ODESC(G), the Security and Intelligence Board, and the Hazard Risk Board told us that the current governance structures for the strategic side of the System are an improvement on the previous structures and are providing better governance over time.

4.10 Under the current structures, responsibilities are split more clearly between traditional security threats such as terrorism and broader threats to national security such as tsunamis, food safety failures, or pandemics. The current structures provide a basis for co-ordination and leadership of activities to mitigate and manage these different kinds of risk.

The right people are coming together with greater purpose

4.11 ODESC(G), the Security and Intelligence Board, and the Hazard Risk Board generally include the right people from the right organisations. Most of the members of ODESC(G) and its boards who we spoke to thought that their membership was appropriate. The membership of the boards has been refined over time. For example, the Security and Intelligence Board recently agreed to bring in a member from the Ministry of Business, Innovation and Employment, and the Hazard Risk Board brought in a member from the New Zealand Fire Service about 12 months ago.

4.12 A balance needs to be struck between broad representation on the boards and keeping them to a suitable size so they are effective as governance bodies. Some of the people we spoke to thought that there could be some useful additions to the boards, but most agreed that additional people could be brought in as required to prevent the boards from becoming too large. There is flexibility to allow officials who would not normally attend meetings to attend when needed.

4.13 Various documents set out the purpose of ODESC(G) and its boards. These include Cabinet papers, terms of reference, and the *National Security System Handbook*. It is important that these documents are kept up to date. The purposes of the boards are well documented. However, continued work is needed to ensure that the purposes of these boards are well understood by members.

4.14 The Security and Intelligence Board and the Hazard Risk Board have found better focus during the last 12 months because national security risks have been better defined and they have been better supported by the Directorate. Governance through the boards has gained momentum and is becoming more strategic, forward looking, and focused on defined risks.

4.15 In our view, the Security and Intelligence Board is the most mature as a governance body. It is widely viewed by people involved in the System as providing good co-ordination and leadership for the security and intelligence sector. The Board is operating constructively and is valued as a critical governance body by members.

4.16 The Hazard Risk Board is becoming more effective in its governance role over time. Recently, the Board adopted six focal areas, and dashboards were created to help track the progress of work against them. These improvements are helping the Board to be focused and purposeful.

4.17 ODESC(G) is the least mature as a governance body, partly because it has not had a set of clearly defined risks to focus its governance role on. The Strategic Risk and Resilience Panel is providing valuable independent advice to ODESC(G) on defining national security risks. We discuss the status of work on defining national security risks and the importance of this work for enabling better governance by ODESC(G) in paragraphs 4.31-4.33.

Strong relationships are enabling governance to mature quickly

4.18 The strong, trusting, and respectful relationships between members of ODESC(G) and its boards are enabling governance of national security risks and national resilience to mature quickly. The members of ODESC(G) and its boards are part of the network of people who are also sometimes called on when the response side of the System is activated. Most of the people we spoke to said that the relationships between people involved in the System were one of the System's main strengths.

4.19 We observed a meeting of the Security and Intelligence Board and of the Hazard Risk Board, and interviewed most of the members of the boards individually. We saw and heard that the tone of board meetings was constructive, and there appeared to be a good level of trust and respect between members.

4.20 There was good rapport between members at the meetings we observed, and we heard considered, focused, and collaborative discussion of issues. We also observed active listening and participation by board members. We heard support from members for jointly resourcing initiatives.

4.21 The Security and Intelligence Board, which meets monthly, is a particularly cohesive board. Chief executives give priority to attending board meetings.

4.22 The established and constructive relationships between members of the boards mean that the boards are well positioned to continue to become more effective in their governance roles and to do this quickly.

The Directorate is maturing in providing more strategic support over time

4.23 Members of ODESC(G) and its boards mostly see the Directorate as a small directorate that provides good and improving secretariat support for them. For example, the Directorate:

- developed dashboards and focal areas to help the Hazard Risk Board to target its efforts better;
- improved the timeliness of distribution of papers for meetings of the boards by introducing standard operating procedures, which outline time frames for collecting and sending out papers; and
- sends out weekly updates to members of the boards to keep them informed of activities and developments throughout the System between meetings.

4.24 A recent survey by DPMC showed that a notable minority of members of boards were not satisfied with the support they received from the Directorate. Some of the people we interviewed also told us that they experience variation in the Directorate's overall support for their board. For example, some papers are still late on occasion.

4.25 The Directorate needs to be more proactive in facilitating the boards to be strategic and forward looking. This is increasingly happening. For example, the Directorate has initiated senior officials' groups, which help set future agendas for the Security and Intelligence Board and the Hazard Risk Board. Directorate staff also told us that they have received extra resourcing to increase staff numbers. Additional capacity within the Directorate should help it to provide more strategic support.

The National Exercise Programme helps the System to be prepared

4.26 Cross-agency exercises were held before the National Exercise Programme was set up. Those exercises were in response to emerging issues or in preparation for major events, such as the Rugby World Cup.

4.27 The National Exercise Programme was set up in 2013 and more formally plans exercises between agencies on an all-hazards basis to help ensure that New Zealand has the capability to effectively respond to national security events on- and offshore. The National Exercise Programme is designed to help officials confidently follow best practice crisis-management processes. It complements, but does not replace, agency-readiness programmes.[4]

4.28 The Hazard Risk Board oversees the National Exercise Programme, which operates on a four-year time frame. The 2015-19 programme uses a philosophy known as "crawl-walk-run". Each year, there is at least one "run" exercise conducted to fully test the System in a realistic national security scenario. The "run" exercise is preceded by two "walk" exercises to help prepare for the "run" exercise.[5] Exercise Tangaroa is an example of a "run" exercise that took place in August 2016.

4.29 We observed how governance of co-ordination of the all-of-government response was practised by DPMC and agencies on the first day of Exercise Tangaroa. This involved simulating activation of the response side of the System, calling and running a Watch Group meeting, calling and running an ODESC meeting, and organising a National Security Committee meeting. There will be a formal debrief of the exercise as part of the National Exercise Programme. We have summarised our observations here. They are our views and do not replace the formal debriefing that DPMC will carry out.

4 For more information on the National Exercise Programme, see www.dpmc.govt.nz/sig/nep.

5 "Walk" exercises generally do not involve the same scenario as the "run" exercise. At the national level, exercises are designed to test and strengthen officials' capability to operate in the System when responding to national security events, almost regardless of the type of scenario.

Figure 6
About Exercise Tangaroa

Exercise Tangaroa

Exercise Tangaroa was a national inter-agency exercise designed to test New Zealand's arrangements for preparing for, responding to, and recovering from a nationally significant tsunami.

This was an all-of-government exercise led by the Ministry of Civil Defence and Emergency Management (which is the lead agency for geological, meteorological, hazards, and infrastructure failure emergencies).

Sequence of events for governance of the response (as the simulated emergency unfolded)

The Directorate activated the response system after the Ministry of Civil Defence and Emergency Management notified it of a potential tsunami threat just before 10am.

Co-ordinated by the Directorate, relevant elements of DPMC's Security Intelligence Group relocated to the National Crisis Management Centre in the basement of the Beehive to support governance of the response alongside where the operational management of the response by the Ministry of Civil Defence and Emergency Management had already started.

The Directorate convened a "co-ordination" meeting of DPMC staff to plan the sequence and timing of Watch Group, ODESC, and National Security Committee meetings for the day ahead. The Ministry of Civil Defence and Emergency Management's National Controller briefed staff on the situation.

A plan for DPMC's support to the governance of the response was determined at the co-ordination meeting, and tasks were assigned to those who attended.

Directorate staff notified relevant agencies of the Watch Group meeting by email and prepared an agenda for the meeting, based on their understanding of the issues requiring all-of-government support and attention, which became clearer as further information was received.

The Watch Group met at 12.30pm with the primary objective of supporting public safety and preservation of life. The issues discussed included a situation update from the National Controller, provision of support to the Ministry of Civil Defence and Emergency Management, impact on lifeline utilities, and issues to take to ODESC for a decision.

Actions from the Watch Group meeting were agreed and assigned.

Directorate staff sent out an email calling an ODESC meeting, prepared an agenda for the meeting, and recorded minutes from the Watch Group meeting.

ODESC met at 2.30pm and received a situation update from the National Controller before discussing the issues identified by the Watch Group.

The Chairperson of ODESC received advice from agencies and advised the Minister of Civil Defence of decisions needed from the National Security Committee.

The National Security Committee met by teleconference at about 3.15pm to discuss and agree on decisions to support the all-of-government response.

Impressions and observations

The exercise seemed quite real for those participating in it.

There was a sense of bringing as much organisation as possible to a response to an uncertain and unfolding situation.

The governance followed a planned sequence of events, through response structures (Watch Group, ODESC, and National Security Committee) that seemed to be understood by those organising and participating in them. This sequence of events seemed to fundamentally get the job of support and co-ordination of the all-of-government response done.

There were some glitches – for example, email distribution lists seemed inefficient to compile from different sources, and a few of the invited agencies did not send a representative to the Watch Group meeting.

Committing to action on the basis of uncertain, conflicting, and imperfect information is hard and requires judgement, and considered judgements were made.

Communication, including keeping the public informed, was recognised as important.

There was a focus on capturing lessons from the exercise from those participating in governance roles (at all levels) as the day unfolded.

We note that there were two more stages to the exercise: the response after the tsunami, followed by the management of the longer-term recovery two weeks later (desk-based stages that we did not observe).

A full report on the exercise, including lessons learned, is due in early 2017.

Improvements under way and others that could be made

4.30 Some improvements are under way and others could be made for governance of the strategic side of the System to continue to mature quickly and be fully effective.

More focused and proactive risk management

4.31 During the last 12 to 18 months, DPMC has been working with agencies across government and beyond to better identify and define national security risks and mitigations for these risks. This work is important because it will provide focus for the governance of the strategic side of the System and provide a forward-looking, proactive perspective for governance of national security risks and resilience-building on an ongoing basis. DPMC has identified risks and needs to clarify how that identification will be used to strengthen governance and management of risks through the strategic side of the System.

More focused purpose for ODESC(G)

4.32 The purpose of ODESC(G), as set out in its terms of reference, is "to identify major risks facing New Zealand and ensure that appropriate arrangements are made throughout Government to efficiently and effectively mitigate and manage them". Most members of ODESC(G) told us that ODESC(G) was not yet fulfilling this purpose or providing effective governance over the Security and Intelligence Board and the Hazards Risk Board.

4.33 This is partly because ODESC(G) does not yet have a clear set of risks to govern. The work to define national security risks should help members of ODESC(G) to be clearer about its purpose and enable ODESC(G) to be more effective as the overall governance body for overseeing management of national security risks and resilience-building.

Clearer accountabilities and better reporting against them

4.34 It is unclear how the Security and Intelligence Board and the Hazard Risk Board are accountable to ODESC(G). Some members of these boards did not have a good understanding of what they are accountable for or of how the boards report against their accountabilities.

4.35 What each of the boards is accountable for and who it is accountable to is set out in the board's terms of reference. However, there has not been a strong focus on monitoring and reporting against accountabilities using appropriate metrics. Reporting and accountability is primarily done informally by the chairpersons of the boards. The recent DPMC survey of board members showed that most believed that there could be better transparency and greater focus in reporting outcomes against accountabilities for the System as a whole. DPMC is working on strengthening its approach to monitoring and reporting through forward work programmes and dashboard performance reports.

4.36 A large number of subgroups sit beneath the Security and Intelligence Board and the Hazard Risk Board. In August 2016, the Directorate completed a stocktake to find out how many subgroups there are, what their terms of reference are, and who they report to.

4.37 Lines of accountability between the subgroups and the boards are not clear. There was some confusion among board members we interviewed about their roles and responsibilities for these subgroups, and about the roles and responsibilities of the subgroups.

4.38 Not being clear on accountabilities means that the boards cannot effectively govern the subgroups. DPMC has identified that the number of subgroups needs to be rationalised and that accountabilities and reporting against them need to be clearer. It has begun work to address this.

4.39 Recent work by DPMC has helped to strengthen some aspects of accountability on the strategic side of the System, such as identifying priorities and focal areas for the Security and Intelligence Board and the Hazard Risk Board and introducing dashboard reporting against them.

4.40 Clearer and stronger accountabilities are needed throughout the strategic side of the System. Identifying risks will help to clarify and strengthen accountabilities further by providing a better framework for delegating accountabilities for risks from ODESC(G) to the boards and subgroups, and reporting against the delegated accountabilities. When the identified risks are used in this way, the accountabilities of the boards and subgroups will need to be updated.

Recommendation 1

We recommend that the Department of the Prime Minister and Cabinet sharpen the focus of governance of the management of national security risks and of national resilience-building by:

- using the work it is doing to define national security risks to establish clear accountabilities for governance of the management risks, and reporting regularly against the accountabilities; and
- rationalising the number of subgroups beneath the main governance boards and clarifying lines of accountability between the subgroups and the boards.

5 Working towards a world-class system through continuous improvement

5.1 In this Part, we discuss:

- the attributes of the world-class system that DPMC aspires to:
- the attributes of the world-class system that the System displays now; and
- the main improvements that can be made to move the System closer to world class.

Summary of our findings

5.2 DPMC aspires to have a world-class national security system. The System currently displays some of the characteristics of a world-class system. For example, the System is able to quickly mobilise a network of people and has clear frameworks in place to manage the response to national security events and emergencies.

5.3 DPMC is making ongoing improvements to the System towards making it world class. Further improvements could be made. Information flows, particularly for classified information, need to be improved throughout the System. The resilience of the System needs to be supported by better identification and transfer of institutional knowledge, and more systematic induction of people coming into the System.

The attributes of a world-class system

5.4 At the beginning of our audit, DPMC asked us to measure the System against a world-class standard. DPMC intends the System to be world class and seen as effective, efficient, and trusted by the officials involved in it and the Ministers who receive advice from it. DPMC sees a world-class system as enabling decision-makers to identify and respond appropriately to the national security issues confronting New Zealand.

5.5 National security systems throughout the world operate differently, and there is no obvious world-class standard for a national security system. However, there are many examples of what best practice looks like. Based on experiences here and overseas, DPMC identified that a world-class national security system is:

- resilient, forward-looking, risk-based, and able to learn lessons and adapt accordingly;
- swift in how it responds – it can mobilise partnerships and move information quickly;
- adaptable to events that are unexpected and/or complex;
- supported by good processes but has a degree of flexibility and is able to cope with a variety of responses;
- effective when making decisions in a strategic context;

- able to draw on good information quickly to promote understanding; and
- efficient in how it uses leadership effort and includes prioritisation mechanisms that make best use of resources.

The National Security System displays some of the attributes of a world-class system

5.6 The System currently displays some of the characteristics of a world-class system. For example, New Zealand is a small, well-connected nation, and the System is able to quickly mobilise a network of people. The System also has clear frameworks in place to manage crises, such as Watch Groups, ODESC, and the use of the Coordinated Incident Management System.[6]

5.7 New Zealand also applies elements of best practice in managing crises, such as "red teaming". Red teaming involves a multi-agency team subjecting a plan, ideas, and assumptions to rigorous analysis and challenge to improve the validity and quality of the final plan. This was used during Operation Concord. During this response, the response team also completed analysis of similar events internationally and sought advice from international partners to help with the response.

5.8 DPMC is making ongoing improvements to the System, both on the response side and the strategic side. Examples of continuous improvement include:

- defining risks to provide sharper focus and a forward-looking, proactive perspective for governance of national security risks and resilience-building;
- introducing the National Exercise Programme to prepare the System for responding to critical risks, including debriefing meetings after exercises and activations of the response side of the System, and work the Directorate intends to do to be more systematic in identifying, recording, and applying lessons from these debriefings;
- publication of the *National Security System Handbook* to improve understanding of how the System operates and roles in it, and other procedural improvements introduced by the Directorate; and
- the all-of-government strategic communications function, recently introduced to improve strategic communication during an event. The function helps the lead agency by managing the strategic communications, leaving the lead agency to focus on operational communications.

6 As described in the *National Security System Handbook*, New Zealand's "Coordinated Incident Management System" (CIMS) is a framework of consistent principles, structures, functions, processes and terminology that agencies can apply in an emergency response. It enables agencies to plan for, train and conduct responses in a consistent manner, without being prescriptive. CIMS relates to the management of a response; the ODESC structure sits above this if the situation is significant or complex enough to demand a coordinated strategic response at the national level.

Moving the National Security System closer to world class

5.9 Although the System is evolving and maturing, further improvements could be made for it to be world class. These should strengthen the resilience of the System and enable it to operate in a seamless and sustained way.

Information flows throughout the System can be improved

5.10 Effective governance on both the response and the strategic sides of the System requires relevant information to flow efficiently between the different people involved.

5.11 We saw examples of good information flow on the response side of the System when examining our two examples. In both examples, information flowed from lead agencies into Watch Groups, and between Watch Groups and ODESC. Information was also shared to provide co-ordinated advice to Ministers. Although there were issues with information flows very early in the Operation Concord response, these were quickly sorted out.

5.12 On the strategic side of the System, meeting minutes also showed that relevant information flowed between ODESC(G) and the boards, and to the boards from subgroups, within the limitations of unclear accountabilities.

5.13 However, information (both classified and non-classified) does not always flow efficiently on either the response or the strategic side of the System. Directorate staff told us that they consider that this is the biggest issue to resolve for the System to be more effective. Many people we spoke to also told us that information does not always flow well throughout the System.

5.14 Although there is scope to improve the flow of non-classified information through the System, the flow of classified information is of particular issue. Classified information is information that people can access only if they have a specific level of security clearance.

5.15 There are several barriers to the easy and effective flow of classified information:

- the lack of a simple way to transmit classified information that all people with the appropriate clearance are able to access, and no consolidated information repository that everyone with the appropriate level of security clearance can access;
- limited staff throughout the System with appropriate clearances to access classified information, which is a particular problem for some agencies; and
- the current manual process for confirming that people attending meetings and receiving information have the appropriate security clearance, which is labour-

intensive and trust-based, and could be simpler and more efficient. Work is under way to find a solution for this.

5.16 As well as the issue of how classified information flows through the System, the Directorate has recognised that the way information flows from the boards to agencies on the strategic side of the System can be constrained. The Directorate is seeking to improve these information flows with several new initiatives. For example, the Directorate has recently started sending out a weekly "all hazards" update, which provides situational awareness throughout government.

Better knowledge management and induction to the System

5.17 The System relies on the institutional knowledge and established relationships of an experienced network of people. That network changes over time as people move in and out of the System.

5.18 Sustained and seamless operation of the System needs to be supported by better capture and transfer of institutional knowledge, such as knowledge of the circumstances or scenarios the System has responded to, and how it has responded, in the past. This would provide a "knowledge bank" that people in the System could draw on where relevant in future responses.

5.19 How people are inducted, trained, and developed in their roles in the System also needs to be more methodical. One person we interviewed described induction to the System, and understanding their role in it, as learning "by osmosis". Recently developed, tertiary-led officials' courses provide people with a useful introduction to the System. These courses are run several times a year. More methodical induction and development to build on this training is needed to bring people into the System quickly and effectively.

5.20 Given the recent changes to the architecture of the System, the diagram depicting the System needs to be updated, including the names of some of the boards so that people can clearly distinguish them and their roles.

Recommendation 2

We recommend that the Department of the Prime Minister and Cabinet strengthen the resilience of the National Security System by:

- enabling easier and more efficient information flows, particularly of classified information, throughout the System;
- capturing institutional knowledge to build a knowledge bank that people in the System can draw on for future responses;
- capturing and applying lessons from activations of the System and exercises more methodically; and
- introducing more methodical induction, training, and development of people moving into different roles in the System.

About our publications

All available on our website

The Auditor-General's reports are available in HTML and PDF format on our website – **www.oag.govt.nz**. We also group reports (for example, by sector, by topic, and by year) to make it easier for you to find content of interest to you.

Our staff are also blogging about our work – see **blog.oag.govt.nz**.

Notification of new reports

We offer facilities on our website for people to be notified when new reports and public statements are added to the website. The home page has links to our RSS feed, Twitter account, Facebook page, and email subscribers service.

Sustainable publishing

The Office of the Auditor-General has a policy of sustainable publishing practices. This report is printed on environmentally responsible paper stocks manufactured under the environmental management system standard AS/NZS ISO 14001:2004 using Elemental Chlorine Free (ECF) pulp sourced from sustainable well-managed forests. Processes for manufacture include use of vegetable-based inks and water-based sealants, with disposal and/or recycling of waste materials according to best business practices.

Office of the Auditor-General
PO Box 3928, Wellington 6140

Telephone: (04) 917 1500
Facsimile: (04) 917 1549

Email: reports@oag.govt.nz
Website: www.oag.govt.nz