



# Managing Threats to Domestic Security

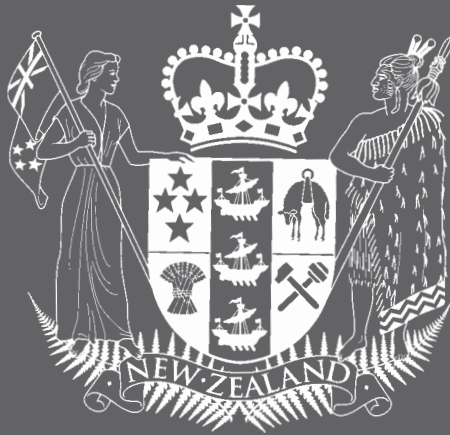
Report of the  

---

**Controller and Auditor-General**

*Tumuaki o te Mana Arotake*

**The Audit Office**  
**Private Box 3928, Wellington**  
**Telephone: (04) 917 1500**  
**e-mail: *reports@oag.govt.nz***  
**web site: *www.oag.govt.nz***



# **Report of the Controller and Auditor-General**

*Tumuaki o te Mana Arotake*

## **Managing Threats to Domestic Security**

**October 2003**

*This is the report of a performance audit carried out under the authority of section 16 of the Public Audit Act 2001.*

ISBN 0-478-18109-4

## Foreword

The attacks in the United States of America on 11 September 2001 have heightened world awareness of the risks to domestic security – especially the risk of terrorist attacks designed to cause mass casualties. The bombings in Bali in October 2002 further confirmed that the security environment has changed, and that countries need to adapt to meet new security challenges.

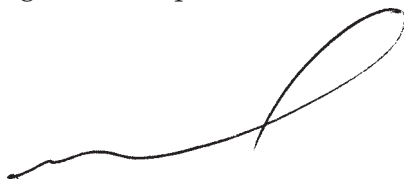
New Zealand is not immune to these changes. It is important – for the country's own protection and well-being, and to meet international obligations – that New Zealand adapts to meet the new security environment in the most effective way possible. Unless security measures keep pace with those being adopted elsewhere, New Zealand risks attracting terrorist attention, and could unwittingly provide a 'safe haven' for terrorists and terrorist activities.

In this audit, we set out to provide assurance to Parliament and the public that threats to domestic security are being adequately managed. Our unique mandate as auditor of the public sector enabled us to examine the wide range of arrangements in place to identify and respond to domestic security threats.

I am pleased to report that New Zealand has taken, and is continuing to take, steps to ensure that it is meeting current "international best practice" in relation to domestic security.

I was impressed by how favourably the audit was received by the agencies involved, and I thank their staff for the very positive and willing assistance given to my auditors and their contribution to this report.

In particular, I thank the staff of the Domestic and External Security Secretariat, for their efforts in helping to co-ordinate the audit and the agencies' responses.



K B Brady  
Controller and Auditor-General  
20 October 2003



## Contents

|   | <i>Page</i> |
|---|-------------|
| <b>Glossary of Abbreviations</b>  | <b>6</b>    |
| <b>Summary</b>  | <b>7</b>    |
| Background to Our Audit   | 7           |
| Purpose of Our Audit  | 8           |
| Overall Findings  | 8           |
| <b>Part One – Introduction</b>  | <b>13</b>   |
| What Is Domestic Security?  | 15          |
| Why Domestic Security?  | 16          |
| What Did We Do?   | 17          |
| <b>Part Two – The Context for Domestic Security</b>                                       | <b>21</b>   |
| Policy Dimensions of Domestic Security  | 23          |
| What Is Driving the International Response?   | 27          |
| New Zealand's Response  | 29          |
| Who Is Responsible for Domestic Security?   | 31          |
| <b>Part Three – Developing a Co-ordinated Response</b>                                    | <b>35</b>   |
| Key Findings  | 37          |
| Effectiveness of the DESC Structure for Domestic Security                                 | 38          |
| A Domestic Security Strategy  | 41          |
| Assessing and Obtaining Resources for Domestic Security                                   | 46          |
| <b>Part Four – Determining Intelligence Needs and<br/>Co-ordinating Information Flows</b> | <b>49</b>   |
| Key Findings  | 52          |
| The Fundamentals of Intelligence Co-ordination  | 53          |
| Agencies' Use of Intelligence   | 53          |
| Meeting General Intelligence Needs  | 54          |
| Co-ordinating the Flow of Intelligence  | 57          |
| Providing Effective Analysis of Information and Intelligence                              | 61          |



|   | <i>Page</i> |
|---|-------------|
| <b>Part Five – Assessing the Capability to Respond</b>              | <b>63</b>   |
| Key Findings  | 65          |
| Setting Day-to-day Capability Expectations                          | 66          |
| Monitoring Against Day-to-day Capability Expectations               | 71          |
| Planning and Monitoring the Capability to Respond to Events         | 73          |
| A Stock-take of Capabilities for Responding to Events               | 80          |
| <br><b>Appendices</b>   |             |
| 1 United Nations Security Council Resolution 1373                   | 84          |
| 2 List of International Anti-terrorist Conventions                  | 88          |
| 3 Legislative Activity Since September 2001                         | 90          |
| 4 Additional Funding for Domestic Security After September 11, 2001 | 91          |
| <br><b>Figures</b>  |             |
| 1 The Security Spectrum   | 16          |
| 2 Three-phase Policy Framework for Domestic Security                | 25          |
| 3 Who's Who in Domestic Security                                    | 32          |
| 4 Funding Framework for Domestic Security                           | 47          |
| 5 Co-ordination of Maritime Intelligence                            | 58          |
| 6 New Zealand Aviation Security                                     | 68          |
| 7 New Zealand Maritime Security                                     | 69          |
| 8 Obligations of Exporters to the United States of America          | 71          |
| 9 Simulation – <i>The Virus has Landed 02</i>                       | 76          |



## GLOSSARY OF ABBREVIATIONS

### Glossary of Abbreviations

|                                |   |
|--------------------------------|---|
| <b>AvSec</b>                   | Aviation Security Service (a separate function of the Civil Aviation Authority) |
| <b>CAA</b>                     | Civil Aviation Authority  |
| <b>CIMS</b>                    | Co-ordinated Incident Management System   |
| <b>CLAG</b>                    | Combined Law Agencies Group   |
| <b>Customs</b>                 | New Zealand Customs Service   |
| <b>CSI</b>                     | Container Security Initiative   |
| <b>CTG</b>                     | Counter Terrorist Group of the New Zealand Defence Force                        |
| <b>DES</b>                     | Cabinet Committee on Domestic and External Security<br>Co-ordination            |
| <b>DESS</b>                    | Domestic and External Security Secretariat                                      |
| <b>DESC</b>                    | Domestic and External Security Co-ordination                                    |
| <b>DPMC</b>                    | Department of the Prime Minister and Cabinet                                    |
| <b>EAB</b>                     | External Assessments Bureau   |
| <b>FIRC</b>                    | Foreign Intelligence Requirements Committee                                     |
| <b>GCSB</b>                    | Government Communications Security Bureau                                       |
| <b>ICAO</b>                    | International Civil Aviation Organisation                                       |
| <b>Immigration<br/>Service</b> | New Zealand Immigration Service (a division of the<br>Department of Labour)     |
| <b>IMO</b>                     | International Maritime Organisation   |
| <b>ISO</b>                     | International Organization for Standardization                                  |
| <b>JIG</b>                     | Joint Intelligence Group  |
| <b>MAF</b>                     | Ministry of Agriculture and Forestry  |
| <b>MCDEM</b>                   | Ministry of Civil Defence and Emergency Management                              |
| <b>MFAT</b>                    | Ministry of Foreign Affairs and Trade   |
| <b>MoH</b>                     | Ministry of Health  |
| <b>MoT</b>                     | Ministry of Transport   |
| <b>MSA</b>                     | Maritime Safety Authority   |
| <b>NAC</b>                     | National Assessments Committee  |
| <b>NMCC</b>                    | National Maritime Co-ordination Centre  |
| <b>NZDF</b>                    | New Zealand Defence Force   |
| <b>NZSIS</b>                   | New Zealand Security Intelligence Service                                       |
| <b>ODESC</b>                   | Officials Committee for Domestic and External Security<br>Co-ordination         |
| <b>STG</b>                     | Special Tactics Group of the Police   |
| <b>WCO</b>                     | World Customs Organisation  |



# Summary

## Background to Our Audit

The events of 11 September 2001 led to an increased focus on domestic security around the world. A mindset change took place whereby responsibility for domestic security no longer lay solely with the traditional security agencies, but began to be shared across a wide range of government agencies. The Bali bombings on 12 October 2002 reinforced the need for an increased focus on domestic security, especially for countries such as Australia and New Zealand.

New Zealand has responded to these events in several ways. A number of government agencies have received a total of almost \$30 million in additional funding over the years 2001-02 to 2003-04<sup>1</sup> for initiatives such as:

- extra security at airports;
- increased provision of intelligence capability for both the Security Intelligence Service and the Police; and
- the establishment of a bio-chemical incident response capability.

For the three years 2003-04 to 2005-06, ODESC has endorsed budget bids for \$73 million of operational expenditure and \$25 million of capital expenditure. These bids have been further refined and included in each department's budget bids. In addition, Cabinet has agreed that the Immigration Service will receive \$5.4 million in 2003-04 and \$4.8 million for each subsequent year to strengthen its immigration intelligence capacity.

Legislation has been passed to give effect to United Nations Security Council Resolution 1373<sup>2</sup> and to obligations under a number of international anti-terrorist conventions. The Government sent troops in support of operations in Afghanistan.

These changes are being driven by international requirements, and by the recognition that the country's domestic security arrangements needed to be enhanced to reflect the new security environment.

---

1 Operating funding of \$26.916 million and capital funding of \$2.894 million. Details are given in Appendix 4 on pages 91-92.

2 Resolution 1373 is reproduced in Appendix 1 on pages 84-87.



### Purpose of Our Audit

We set out to provide assurance to Parliament and the public that threats to the country's domestic security are being adequately managed. To do this, we examined the arrangements in place to identify and respond to domestic security threats. In particular, we looked at whether:

- there was an adequate *framework* to guide domestic security efforts;
- the collection and dissemination of relevant *intelligence* was *well co-ordinated* and the intelligence collected was *sufficient* to address the risks, goals, and objectives identified;
- the *preparedness and capability* of the various agencies to respond to threats to domestic security was being monitored; and
- there were effective arrangements for monitoring and evaluating the *allocation of resources* used to achieve domestic security goals.

### Overall Findings

New Zealand has taken, and is continuing to take, steps to ensure that it is meeting current “international best practice” in relation to domestic security. New Zealand faces similar problems to many other countries, but this country is relatively small, and the allocation of responsibilities across different parts of government is relatively simple. These are both important advantages in co-ordinating whole-of-government responses on domestic security matters.

We found examples of good practice across all areas, and progress in some areas has been substantial. The DESC structure (described on pages 31-33) provides a good framework to facilitate multi-agency interaction, and has recently been re-structured to reflect the new security environment.

Both formal and informal mechanisms exist to share and co-ordinate domestic security information and intelligence. The capability to collect and analyse information was enhanced after September 2001. The Aviation Security Service (AvSec) and the Counter Terrorist Group of the New Zealand Defence Force (NZDF) stood out in terms of preparedness monitoring. A number of agencies carry out or take part in exercises or simulations to test their capabilities and procedures.



A number of issues still need to be addressed that arise mainly from the number of contributing agencies whose primary responsibilities do not have a domestic security focus. These issues are summarised in the following paragraphs.

### *A Whole-of-government Domestic Security Strategy*

---

See Part Three on pages 35-48.

There is no single document or collection of documents that sets out:

- key issues in relation to domestic security – including comprehensive assessments of national threats, risks and vulnerabilities;
- priority ranking of the issues;
- which issues will be addressed and how – including explicit goals and objectives to guide overall efforts; and
- the responsibilities of the individual agencies – who is responsible for what and where each agency sits within the whole.

Notwithstanding the adoption this year of a framework for a whole-of-government approach to the allocation of additional resources, a whole-of-government strategy along these lines would provide a focus for the efforts of the many agencies (both public and private) involved in domestic security. Such a strategy would:

- enhance the current annual basis for resource allocation by providing a framework for setting long-term funding priorities;
- provide a framework for other relevant strategies – such as the Biosecurity Strategy – to support overall domestic security efforts; and
- be a basis for providing assurance to Parliament and the public that these considerable efforts are being directed to the areas of greatest need.

Work is in progress to provide a national framework that government departments and other agencies can use to guide and co-ordinate their operational and tactical plans and procedures.



### *Further Enhancements of Domestic Intelligence Co-ordination*

---

See Part Four on pages 49-62.

At present, domestic intelligence collection is undertaken on the basis of an individual agency's needs and mandate, and most co-operation between agencies is not formalised. We believe that there would be benefit in exploring formal ways to ensure that domestic security intelligence collection is co-ordinated across agencies. Such exploratory work would need to consider the implications of formalised processes – including legislative, operational and technical factors – in identifying potential solutions.

There is also no cross-agency information/intelligence system. Such a system would enable individual agencies to share information required for preparing risk and threat profiles, and would potentially provide a reliable whole-of-government picture of any likely threats.

Domestic intelligence co-ordination could consequently be strengthened in two ways:

- By having a more formal process for identifying domestic intelligence requirements that includes inter-agency consultation.
- By establishing a computer-based cross-agency information/intelligence system. The establishment of the New Zealand Intelligence Community Network will assist in this regard.

### **Establishing Wider Agency Capability to Analyse Intelligence**

The majority of agencies (the NZSIS, the Police, and the NZDF) analyse and use intelligence as part of their day-to-day operations. For other agencies, there are a number of obstacles to fully participating in the intelligence field. However, the other agencies need to make good use of information and intelligence in order to make the right decisions on targeting and deploying their resources.

There is scope for the agencies with a well-developed capability in intelligence analysis to provide more support to those agencies that need to build up their capability in order to play their full part in domestic security arrangements.



## **Undertaking a Stock-take of Total Capability**

The large number of agencies involved in domestic security have a wide range of capabilities between them. To date, there has been no systematic stock-take of all these capabilities to help clarify what exists and where, and to reveal any gaps or overlaps. A stock-take of capabilities has taken place in certain areas, but a comprehensive stock-take is required to enable the Government to identify weaknesses and decide what remedial actions need to be put in hand.

## ***Whole-of-government Reporting of Preparedness***

---

See Part Five on pages 63-81.

The Government requires assurance on the level of preparedness of domestic security arrangements. Currently, assurance is provided to varying degrees through each agency's Purchase Agreement.

Some of the reporting clearly notes contributions to domestic security, while other activities are reported as normal agency business. The reporting is required to support individual agency accountability, but does not provide a whole-of-government picture of preparedness.

In view of the primary importance of domestic security, we believe the current reporting should be supplemented by whole-of-government reporting that provides the Government with assurance on the level of preparedness for key domestic security capabilities.

## ***Increased Effort on the Recovery Phase***

---

While the traditional domestic security response elements (for example, the NZDF's Counter Terrorist Group) are well-practised and planned in response aspects, the requirements of the recovery phase of a security incident have not received as much attention. These requirements include having plans for recovery, and understanding the capabilities that are required and available for recovery.

DPMC, along with domestic security agencies, has recognised this gap and is looking at ways of increasing the depth of plans for recovery.







## Part One

# Introduction



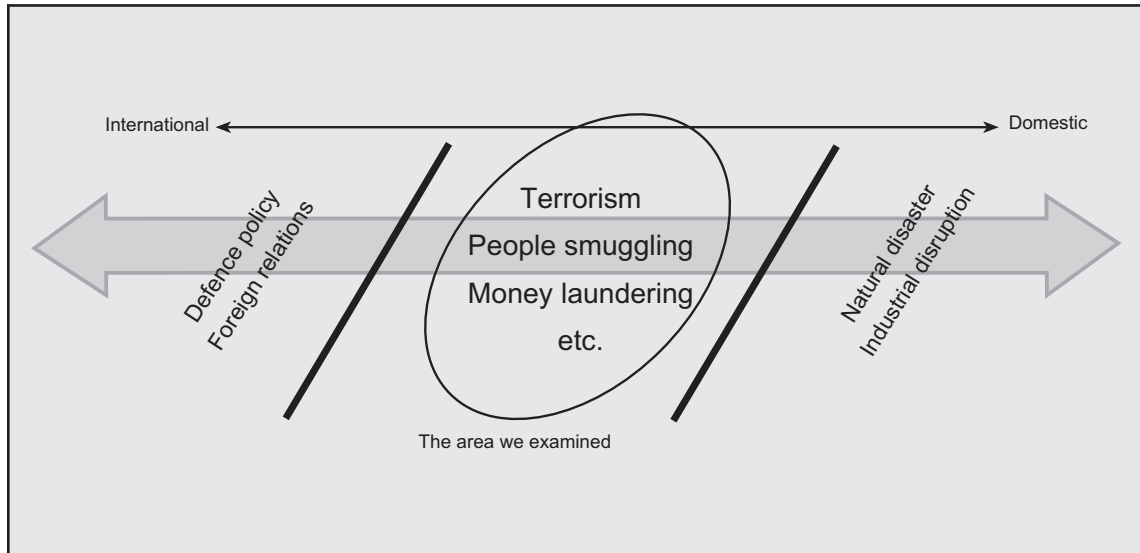


## What Is Domestic Security?

- 1.1 We have defined 'domestic security' as "preventing or defending against threats that are unconventional in approach (i.e. not by traditional military means) and are directed towards the interior of a state rather than its external forces." This definition is consistent with that adopted in the United States of America (USA) and elsewhere, and is commonly known as 'homeland security'.
- 1.2 Threats to domestic security include threats from terrorism (including agri-terrorism and bio-terrorism), a cyber attack on major information or business systems, and attacks against critical physical infrastructure (such as the public water supply). Threats to domestic security are all crimes or the result of criminal actions.
- 1.3 Domestic security can also be affected by other major international events, which, while not necessarily criminal, are likely to threaten the country's economic and social well-being. Such events might include an outbreak of foot and mouth disease, the introduction of pests and diseases that will affect primary industry, or an outbreak of an infectious disease – the Severe Acute Respiratory Syndrome (SARS) virus was a recent example.
- 1.4 Our definition of domestic security in paragraph 1.1 excludes the majority of defence and foreign policy actions. We did not examine the impact that maintaining a specific defence or foreign policy has upon domestic security. However, we did examine those elements of the NZDF and MFAT that have a domestic security focus. For example, the NZDF's Counter Terrorist Group (part of the Special Air Service) plays a contingency role in domestic security arrangements in support of the Police, once authorised.
- 1.5 Our audit did not look at civil emergencies and disasters, such as flooding, earthquakes, or industrial action. However, as the mechanisms used to respond to these events can be used for domestic security incidents, we did examine certain aspects of the agencies with civil emergency roles.
- 1.6 The scope of our examination is illustrated in Figure 1 on the next page.



*Figure 1*  
*The Security Spectrum*



## Why Domestic Security?

- 1.7 Since the attacks on 11 September 2001, the world has become more aware of the risks to domestic security – especially the risk of terrorist attacks designed to cause mass casualties. The bombings in Bali in October 2002 further confirmed that the security environment had changed, and that countries needed to adapt to meet new security challenges.
- 1.8 New Zealand is not immune to these changes. It is important – for the country's own protection and well-being, and to meet international obligations – that New Zealand adapts to meet the new security environment in the most effective way possible. Unless security measures keep pace with those being adopted elsewhere, New Zealand risks attracting terrorist attention, and could unwittingly provide a 'safe haven' for terrorists and terrorist activities.



1.9 In this audit, we set out to provide assurance to Parliament and the public that threats to domestic security are being adequately managed. Our unique mandate as auditor of the public sector enabled us to examine the wide range of arrangements in place to identify and respond to domestic security threats.<sup>3</sup> In particular, we looked at whether:

- There was an adequate *framework* to guide domestic security efforts;
- the collection and dissemination of relevant *intelligence* was *well co-ordinated* and the intelligence collected was *sufficient* to address the risks, goals, and objectives identified;
- the *preparedness and capability* of the various agencies to respond to threats to domestic security was being monitored; and
- there were effective arrangements for monitoring and evaluating the *allocation of resources* used to achieve domestic security goals.

## What Did We Do?

1.10 Our approach to the audit was to:

- first identify best-practice principles for managing threats to domestic security; and
- then compare what was actually happening against those principles.

### *How Did We Identify Best-practice Principles?*

1.11 We talked to a variety of New Zealand experts about national security issues to gain an appreciation of the issues affecting domestic security and the current environment. We also made a preliminary visit to the entities that we identified as having a key role in domestic security to establish what their roles were and what they considered the key issues to be.

---

3 In particular, section 16(1)(a) of the Public Audit Act 2001, which says that –  
*The Auditor-General may at any time examine:  
 The extent to which a public entity is carrying out its activities effectively and efficiently;*  
 Section 16(2) says such an examination *may relate to 1 or more public entities.*



## INTRODUCTION

- 1.12 We then established a set of expectations so that we could assess how New Zealand was responding to the issues identified. These expectations related to:
- the overall security framework;
  - the co-ordination of intelligence flows;
  - assessing how well entities are prepared to prevent a domestic security incident from happening on a day-to-day basis;
  - the entities' ability to respond should an incident occur; and
  - how well entities are able to recover from an incident.
- 1.13 Having established our expectations, we visited our USA counterpart (the General Accounting Office) and reviewed the work that it had carried out on this subject over the last six years.<sup>4</sup> We also visited and reviewed the work undertaken by the Australian National Audit Office. In both cases, we tested with them the soundness of our expectations to ensure that they represented what would be considered best practice.
- 1.14 We also talked with a variety of academics, and attended a conference on Australian Homeland Security in Canberra. We visited think-tanks and academics in Washington D.C., and, while in Canberra, we talked to a number of academics who specialise in the field of security. The main purpose of these visits was to test our expectations as well as gauge how other countries were reacting to the new and emerging security threats – including the public policy implications.
- 1.15 While in Washington and Canberra, we talked to several government agencies involved in domestic security to establish how they perform their threat assessments and establish and measure their capability levels.

### *What Field Work Did We Do?*

- 1.16 We obtained and reviewed relevant Cabinet papers to establish the Government's overall response and the advice that it was given in relation to the changing security environment.

---

<sup>4</sup> The reports of the General Accounting Office can be accessed at [www.gao.gov](http://www.gao.gov). There are special sections devoted to homeland security and counter-terrorism.





- 1.17 We reviewed relevant legislation – in particular, the legislation that has recently been enacted or is expected soon to be enacted – to ensure that New Zealand incorporates new international requirements into its domestic law. A list of the legislation is given in Appendix 3 on page 90.
- 1.18 We interviewed staff from 18 New Zealand agencies.<sup>5</sup> In the majority of cases, we conducted several interviews with various staff members from throughout the agency. We reviewed relevant documents – including strategies, policy and procedure manuals, and monitoring reports.
- 1.19 We observed Customs officers, Immigration Service officers and aviation security staff going about their day-to-day duties, and we talked with them about:
- the current environment and emerging issues;
  - training and assessment programmes; and
  - how they co-ordinate their activities with other agencies and professional bodies.
- 1.20 We also observed the procedures in the mail collection area at the Auckland International Mail Centre, and observed drug and explosive detector dogs at work.
- 1.21 We visited the Parliament Buildings Executive Wing (“the Beehive”) basement where the new National Crisis Management Centre is being established.

### *Audit Personnel Security*

- 1.22 Our staff obtained the necessary security clearances, and were given briefings, to ensure that they were able to cover all of the New Zealand agencies in sufficient depth and were able to read all relevant documentation.

---

5 These agencies were: The Department of the Prime Minister and Cabinet, the Security Intelligence Service, the Government Communications Security Bureau, the Customs Service, the Police, the Immigration Service, the New Zealand Defence Force, the Ministry of Agriculture and Forestry, the Ministry of Fisheries, the Ministry of Foreign Affairs and Trade, the Civil Aviation Authority, the Aviation Security Service, the Maritime Safety Authority, the Ministry of Health, the Ministry of Civil Defence and Emergency Management, the Ministry of Transport, the National Maritime Co-ordination Centre, and the Treasury.





## Part Two

# The Context for Domestic Security





- 2.1 In this part we explain the context for domestic security in terms of:
- the complex policy dimensions of domestic security as they relate to risk and mitigation of risk;
  - the agreements that are driving the international response;
  - how New Zealand has responded; and
  - the allocation of responsibility for domestic security.

### Policy Dimensions of Domestic Security

- 2.2 Much can be done to reduce the risk of terrorism – such as intercepting information to warn of potential incidents, or implementing strong border security – but the risk cannot be totally eradicated. Therefore, the Government needs to establish the level of risk that it is prepared to accept and the precautions required to maintain the risk at or below this acceptable level.
- 2.3 It is not easy to assess what the accepted level of risk should be, and what level of investment in precautions is the most effective. Difficulties include:
- the infrequency of domestic security incidents;
  - a lack of any models or norms to help assess the most effective level of investment in domestic security;
  - the ‘globalisation of the border’<sup>6</sup>, so that it is no longer enough just to focus on people and goods at the point of entry into the country; and
  - the variety of participants in domestic security.

---

6 See paragraphs 2.13-2.15 on pages 26-27.



## THE CONTEXT FOR DOMESTIC SECURITY

### *Infrequency of Domestic Security Incidents*

---

- 2.4 Many public policy decisions (for example – for reducing: the road toll, the rates of burglary, and the incidence of diabetes) can be subjected to detailed analysis over time, so that the effects of different policy initiatives can be assessed with some certainty. In these examples, it is also often possible to demonstrate a clear link between the policy initiative and its outcome.
- 2.5 This is not the case for domestic security. Because domestic security incidents occur infrequently, it is difficult to test the effect of domestic security policies, systems, and procedures. The fact that no domestic security incident occurs may be the result of good systems and procedures – but it could equally be because no threat has arisen.
- 2.6 The infrequency of domestic security incidents can also make it difficult to maintain public support. This is especially the case when initiatives to deter threats are likely to impinge on business interests or the freedoms people enjoy. For example, increasing border security generally results in longer delays for people crossing the border, and higher costs for imported goods. The greater the length of time between security incidents, the greater the likelihood of reduced public consciousness of the threat, and the more likely people will be to perceive precautions as excessive.

### *Lack of Models for Defining Levels of Investment in Domestic Security*

---

- 2.7 There are few generally accepted approaches to designing, or analysing the efficiency or effectiveness of domestic security initiatives.
- 2.8 A policy framework that is utilised in many countries in some form or another deals with domestic security incidents in three phases – prevention, response, and recovery (see Figure 2 on the opposite page). This framework helps to define where capabilities are required – for example, a certain amount of intelligence resource is required to support an adequate preventive capability.





*Figure 2*  
*Three-phase Policy Framework for Domestic Security*

|                   |  |
|-------------------|--|
| <b>Prevention</b> | <p>Taking the measures necessary to prevent terrorism and other forms of politically motivated violence, which include:</p> <ul style="list-style-type: none"> <li>• collecting, analysing and disseminating intelligence about terrorist intentions and capabilities;</li> <li>• having effective border security that prevents known or suspected terrorists from entering the country;</li> <li>• other security that successfully deters individuals and groups from carrying out any attack;</li> <li>• reducing the vulnerability of potential victims and targets; and</li> <li>• identifying and protecting critical infrastructure and key assets.</li> </ul> |
| <b>Response</b>   | <p>Having adequate systems and arrangements that come into effect, especially where a joint response is required, when an incident or threat occurs. The aim is to resolve the incident or reduce the possible impact. Those responding include police officers, fire fighters, emergency medical providers, and emergency management specialists. The ability to respond also means having appropriate technical advice and capabilities to prevent cascading effects, especially with infrastructure.</p>  |
| <b>Recovery</b>   | <p>Having sound financial, legal, and social systems in place to be able to recover from a domestic security incident. Recovery may include:</p> <ul style="list-style-type: none"> <li>• rehabilitation, including medical care for people affected;</li> <li>• rebuilding destroyed property;</li> <li>• rebuilding or replacing critical infrastructure to minimise the potential adverse effects on people's lives and the economy;</li> <li>• re-establishing our reputation (e.g. after bio-terrorist attack);</li> <li>• assisting victims and their families; and</li> <li>• rapidly restoring normal economic and social functioning.</li> </ul>              |



## THE CONTEXT FOR DOMESTIC SECURITY

- 2.9 However, it is difficult to know when enough resources have been applied to the prevention, response, and recovery phases, or whether the correct trade-offs between the phases have been made.
- 2.10 A variation of the three-phase policy framework that has worked well in other areas of risk management, and DPMC has adapted for wider security applications, is known as the “4-Rs” – Reduction, Readiness, Response, and Recovery. This provides for a slightly different balance of emphasis, with more attention to pre-emptive control and mitigation, and fits closely with the approach advocated by AS/NZS 4360:1999 *Risk Management* – the risk management standard developed jointly by Australia and New Zealand.
- 2.11 There are few international standards to help define required levels of preparedness. Individual governments must therefore define their own levels. To the extent that it would be very expensive and impractical to be fully prepared at all times, the affordability and feasibility of preparedness also predicates a level of acceptable risk.
- 2.12 The level of acceptable risk is a matter of judgement, and may change over time as people become accustomed to living with the threat of terrorism (or with the measures to counter the threat). In practice, judgements have to be made in the light of the complex tensions around what is publicly acceptable in terms of risk and the measures to reduce risk, perceptions about the relative importance of different forms of risk, and what is required to meet international obligations.

### ‘Globalisation of the Border’

- 2.13 Traditionally, domestic security has focused on monitoring goods and people at the point of entry, to prevent dangerous or illegal goods and undesirable immigrants and visitors entering the country. Efforts are now increasingly being directed at preventing undesirable visitors from departing for New Zealand.
- 2.14 Internationally (at the instigation of the USA), steps are being taken to ensure that goods are safe and legitimate at the time they are packed and shipped from the country of origin. These developments are extending and ‘globalising’ the traditional concept of the border.



- 2.15 Domestic security can be affected by events occurring outside the country – such as through trans-national organised crime operating in the Pacific, or nationals of one country being attacked in another country (as in Bali).

### *Involving a Variety of Participants*

- 2.16 Central government agencies have a prime role in domestic security, but local government, quasi-government agencies, and the private sector have increasingly important roles as well.
- 2.17 Much of the critical infrastructure (such as information and computer systems<sup>7</sup> within the banking system, water and power supplies, and telecommunications equipment) is controlled or owned by local government, private sector entities, or a mix of government and private sector entities. These entities serve a wide range of communities and stakeholders who have a variety of priorities and expectations – among which security and contingency planning may not be prominent.
- 2.18 Many security initiatives will place responsibilities on private sector as well as public sector organisations. Private sector participation in domestic security initiatives needs to be identified to ensure that best practice – in terms of security and recovery – is fully applied across all sectors. In this report we concentrate on how well central government agencies are managing risks to domestic security.

### What Is Driving the International Response?

- 2.19 After 11 September 2001, there was strong international support for comprehensive, collective action against terrorism. On 28 September 2001, the United Nations Security Council unanimously adopted Resolution 1373<sup>8</sup>, which binds all member states and provides a framework for the international response to the terrorist attacks.

7 The Centre for Critical Infrastructure Protection (a business unit within GCSB) was established in August 2001 to provide advice and support to protect the country's critical infrastructure from cyber threats.

8 Reproduced in full in Appendix 1 on pages 84-87.



## THE CONTEXT FOR DOMESTIC SECURITY

- 2.20 In summary, Resolution 1373 calls on all states to take action to:
- prevent and suppress the financing of terrorist acts;
  - prevent their country from being used to support terrorism;
  - improve co-ordination and information flows between countries; and
  - set up effective border controls to prevent the movement of terrorists and terrorist groups.
- 2.21 The Security Council also noted with concern the close connection between international terrorism and trans-national organised crime, illicit drugs, money-laundering, illegal arms-trafficking, and the illegal movement of nuclear, chemical, biological and other potentially deadly materials.
- 2.22 Obligations arising from New Zealand agency membership of international organisations – the WCO, the IMO, and the ICAO – include:
- identifying and examining high-risk containers and assuring in-transit integrity, implementing standards for electronic customs reporting, and promoting high standards of supply chain security in the private sector;
  - promoting ship and port security plans by July 2004, and the installation of automatic identification systems on certain ships by December 2004;
  - introducing new baggage screening procedures and equipment in all APEC major airports by 2005, reinforcing flight deck doors by April 2003, and supporting ICAO mandatory aviation security audits; and
  - implementing a common global standard on advance passenger information, adopting a biometrics standard, reforming immigration service procedures, and promoting adoption of air cargo security guidelines drawn up by the ICAO.



## New Zealand's Response

- 2.23 Resolution 1373 calls upon all countries to join and fully implement the relevant international conventions and protocols (in all, ten conventions and two protocols). New Zealand has been party to a number of these international conventions, with implementing legislation, for some years.
- 2.24 Following adoption of Resolution 1373, the Government acted quickly to:
- strengthen existing counter-terrorism legislation and obtain new legislation to implement obligations under the resolution and other conventions; and
  - require government agencies to review their procedures in relation to security, and strengthen them as required.
- 2.25 The legislative changes, both complete and intended (see Appendix 3 on page 90), have been wide-ranging and have addressed a number of identified deficiencies.
- 2.26 Government responses have included additional funding of almost \$30 million for the three years to June 2004 for initiatives such as extra security at airports, increased provision of intelligence capability, and the establishment of a bio-chemical incident response capability. A detailed list of those responses is provided in Appendix 4 on pages 91-92. The Government sent troops in support of operations in Afghanistan in 2002.
- 2.27 For the three years 2003-04 to 2005-06, ODESC has endorsed budget bids for \$73 million of operational expenditure and \$25 million of capital expenditure. These bids have been further refined and included in each department's budget bids. In addition, Cabinet has agreed that the Immigration Service will receive \$5.4 million in 2003-04 and \$4.8 million for each subsequent year to strengthen its immigration intelligence capacity.
- 2.28 Steps are also being taken to address port security, supply chain security, baggage screening, and advance passenger processing. These initiatives are discussed in Part Five on pages 63-81.
- 2.29 One important rationale for the changes is the need to ensure that New Zealand's security response does not get out of step with the responses of other countries. As some countries tighten their domestic security measures, the focus of terrorism could move to less-protected locations that provide an easier option for terrorists as a base for their activities, or as the target for an actual attack.



## THE CONTEXT FOR DOMESTIC SECURITY

- 2.30 Security issues are also relevant to New Zealand's interaction with Pacific Island nations. The international community is looking to regional partners like Australia and New Zealand to work with Pacific Island nations to help them upgrade their systems to meet international requirements. As a result, government agencies – the Police, the NZDF, Customs, the Immigration Service, MFAT, the NZSIS, the Ministry of Fisheries, and the CAA – increasingly have to take this wider environment into account.
- 2.31 On 31 March 2003, Cabinet noted that, as part of the 2003 Budget process, a Pacific Security Fund of \$2 million was being established in Vote Foreign Affairs and Trade to meet the costs of advisory, training, and technical support for Pacific Island nations to meet security threats (and risks to New Zealand interests).
- 2.32 MFAT was directed to lead and co-ordinate the preparation of a whole-of-government strategy to guide the allocation of Pacific Security Fund resources. An inter-agency working group was established and recommended that a Pacific Security Co-ordinating Committee be established.<sup>9</sup>
- 2.33 In August 2003, Cabinet approved the establishment of the Committee (to be based in MFAT) to:
- assess and prioritise security risks in the Pacific;
  - develop (for ODESC approval) an annual package of security initiatives to assist Pacific Island nations resourced through the Pacific Security Fund; and
  - evaluate and report on implementation of Pacific Security Fund initiatives by New Zealand agencies.
- 2.34 An Ambassador for Counter-Terrorism was also appointed in August this year. The Ambassador's responsibilities will include:
- co-ordinating counter-terrorism policy and activities within MFAT to ensure that New Zealand is complying with all its legal and reporting obligations (such as Resolution 1373);
  - liaising with other government agencies to ensure that MFAT understands their priorities and activities in relation to counter-terrorism;

---

<sup>9</sup> Committee membership will include DPMC, Ministry of Fisheries, MAF, MFAT, NZ Agency for International Development, the Immigration Service, the Police, NZDF, Customs, NZSIS, the Treasury, MoT (AvSec, MSA, and CAA), with provision to co-opt as appropriate.



- participating in the development and implementation of whole-of-government counter-terrorism policies; and
- assisting South Pacific nations to develop and manage their own security from a counter-terrorism perspective.

### Who Is Responsible for Domestic Security?

- 2.35 The Domestic and External Security Coordination (DESC) structure is used for co-ordinating the efforts of security-related agencies.
- 2.36 Figure 3 on page 32 illustrates the key groups and organisations involved in domestic security. Responsibility for domestic security is at three levels:
- the Cabinet Committee on Domestic and External Security Co-ordination (DES);
  - the Officials Committee for Domestic and External Security Co-ordination (ODESC); and
  - the individual agencies involved in domestic security.
- 2.37 DES<sup>10</sup> is the central decision-making body of executive government for issues involving intelligence, security, and crisis management. The Prime Minister chairs the committee, and its members comprise those Ministers with portfolio responsibilities for key agencies involved in domestic security. Other Ministers can be co-opted onto DES depending on the needs of any specific crisis.
- 2.38 Under DES sits the ODESC, which facilitates a whole-of-government approach to national crises and circumstances affecting security. ODESC is a chief executive level forum in which agencies come together to establish whole-of-government approaches to domestic security. ODESC comprises a generic committee having flexible membership that deals primarily with response and recovery issues for specific events or issues. ODESC has two standing committees – ODESC(P) for ongoing policy, planning and preparedness, and ODESC(I) for intelligence matters.

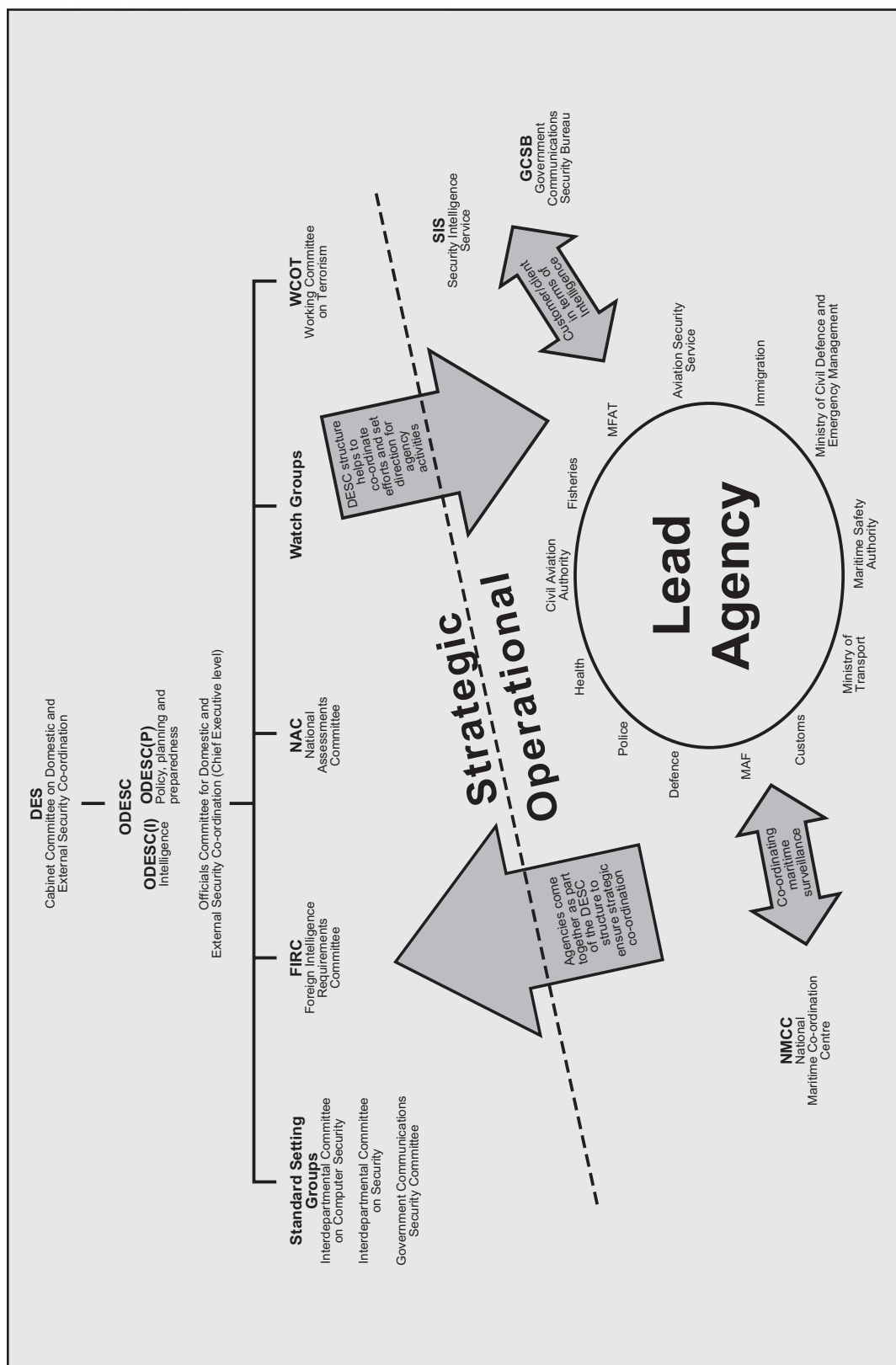
---

10 This Committee replaced two former committees – the Ad Hoc Cabinet Committee on Intelligence and Security and the Ad Hoc Cabinet Committee on Domestic and External Security Coordination. Its Terms of Reference incorporate the Terms of Reference of both former committees.



# THE CONTEXT FOR DOMESTIC SECURITY

Figure 3  
Who's Who in Domestic Security



- 2.39 A number of committees and working groups support the DESC structure. Standing working committees include the Foreign Intelligence Requirements Committee, the Interdepartmental Committee on Security, and the Working Committee on Terrorism. Ad hoc working groups (known as Watch Groups) are formed to concentrate on specific crises or issues as they arise (for example, the Iraq war, or the deployment between 1999 and 2002 of peace-keeping forces to East Timor).
- 2.40 The DESC structure does not override the statutory powers and responsibilities of Ministers and departments. Responsibility for actions and policies remains with the chief executive of an agency and the relevant Minister. The aim of the DESC structure is to ensure that agencies work together in order to achieve better outcomes, not to provide an additional accountability or control mechanism.
- 2.41 Security and intelligence is a primary focus for some agencies – such as the NZSIS and GCSB. Where such intelligence indicates criminal activity (as terrorism and terrorist acts are “crime”) the Police become involved arising from their aims to reduce the incidence and effects of crime, detect and apprehend offenders, maintain law and order, and enhance public safety. However, this responsibility is only part of the wider duties that the Police undertake.
- 2.42 For a large number of agencies, domestic security is increasingly becoming an important aspect of their wider responsibilities. For example, the agencies that control who and what is crossing the border bear some responsibility for identifying potential threats to domestic security. Often, these agencies must balance domestic security concerns with the need to ensure the economic benefits of the free flow of people and goods.

### *The Current Structure Is an Advantage*

- 2.43 New Zealand is a lot less complex in terms of policy development and co-ordination than other countries because it has a unitary system of government and national Police and Fire Services. The simplicity of structure is a major benefit in implementing domestic security policies, or in responding to events.



## THE CONTEXT FOR DOMESTIC SECURITY

- 2.44 For example, all civil aviation activities in New Zealand fall under a single jurisdiction, which is legislated for by the Civil Aviation Act 1990. Civil aviation activities in most other countries are divided among a range of federal, state, county, and private jurisdictions. Sydney, for example, has a range of different organisations providing aviation security services at its international airport.



## Part Three

# Developing a Co-ordinated Response





- 3.1 With the range of both public sector and private sector agencies whose primary function is domestic security, and others for which domestic security is a responsibility but not a primary priority, effective co-ordination of effort is required to make best use of resources. Therefore, we expected that there would be a strategic domestic security framework to guide the work of the many agencies involved.
- 3.2 Key elements of a strategic framework would include:
- a common understanding of what domestic security is;
  - clear goals and objectives (identified through the use of risk, threat, and vulnerability assessments) for the medium-to-long term;
  - clearly stated roles and responsibilities of various agencies and groups;
  - content and quality aspects in line with international best practice; and
  - periodic review to ensure that the framework continues to reflect the enduring risk environment.

### Key Findings

- 3.3 The DESC structure provides an effective mechanism for establishing a whole-of-government response to domestic security matters.
- 3.4 The structure has historically been used in strategic responses to particular risk situations and for particular activities – for example, in developing the *National Counter Terrorist Manual* and in establishing the National Maritime Co-ordination Centre. However, DESC has not been used to plan strategically across the full range of risk areas.
- 3.5 The DESC structure and terms of reference have been amended to establish responsibility to monitor emerging threats, risks, and vulnerabilities to both domestic and external security, and to secure measures to manage potential problems or their consequences. Once fully in place, these changes should give DESC a wider focus and support longer-term planning.



## DEVELOPING A CO-ORDINATED RESPONSE

- 3.6 A whole-of-government strategy for domestic security needs to be prepared to ensure that the efforts of the various agencies are being combined to achieve maximum effect. There is currently no such strategy, but DPMC is drawing up a national framework (or strategy) for domestic security. To be effective, this strategy will need to include a comprehensive description and assessment of the risks and threats facing New Zealand, and allocate to specific agencies the responsibility for countering these threats.
- 3.7 A framework was drawn up for a whole-of-government approach to the allocation of additional resources to domestic security, and was further refined for the 2003-04 budget bids. Through this framework, the purpose and rationale for new funds are well understood. However, funding priorities are currently reviewed and set on an annual basis. There would be benefits in taking a multi-year approach, that would assess the resources required to bring agencies up to an acceptable level of preparedness across all areas, and prioritising them over the next three-to-five years.

### Effectiveness of the DESC Structure for Domestic Security

- 3.8 The DESC structure is, overall, an effective mechanism for establishing a whole-of-government approach to domestic security.
- 3.9 Historically, DESC has been used to respond to events once they occur, or where there is a high likelihood that they will occur. When ODESC was set up in 1987, it quite deliberately established a broad definition of security – covering natural disasters, as well as more traditional security threat situations requiring intelligence, military and/or police resources, and diplomacy. Since then, ODESC has been expanded to provide an effective whole-of-government approach to a range of issues – from the deployment of troops overseas, through counter-terrorism, to managing the SARS risk.
- 3.10 The following changes have been made to ensure that DESC better reflects today's security environment:
- The Cabinet Committee on Domestic and External Security Co-ordination (DES) co-ordinates and manages the national response to all circumstances affecting domestic security (such as a natural disaster, biosecurity problem, health emergency, or terrorist/military threat) within New Zealand or involving New Zealand's interests overseas.



- The DESC structure has been adopted for the management of all major national crises and circumstances affecting domestic security.
  - The ODESC(I) standing committee has been widened to include the Police, in recognition of the key role they play in providing information about security.
  - A new ODESC(P) committee covers policy, planning, and preparedness.
  - The Domestic and External Security Secretariat (based in DPMC) has been expanded in order to provide increased support to the DESC structure.
  - ODESC has been made more flexible to address specific crises and emergencies – for example, the ODESC that was formed to respond to the outbreak of SARS.
- 3.11 Participants in DESC whom we spoke to felt that the structure helped them to achieve both their own and the Government's goals. Critical comments were about refining the structure rather than challenging it fundamentally or challenging the need for it.
- 3.12 The changes outlined in paragraph 3.10 are important. However, we identified two further key opportunities to strengthen DESC that would involve:
- taking a consistent 'over-the-horizon' approach to threats; and
  - the provision of regular whole-of-government advice.
- 3.13 We also consider that the DESC structure could be used more effectively to assess and monitor the overall preparedness of the various agencies involved in domestic security. We discuss this further in Part Five on pages 63-81.

### *An 'Over-the-horizon' Approach*

- 3.14 The majority of the activities that DESC covers are focused on the short-to-medium term. This focus has been reinforced by the fact that, historically, DESC only comes together to facilitate a whole-of-government response to an incident (for example, a specific terrorism threat), or an immediately foreseeable incident (for example, the arrival of a boat carrying refugees or, more recently, the SARS outbreak).



## DEVELOPING A CO-ORDINATED RESPONSE

- 3.15 DESC has not been used to plan strategically across the full range of risk areas. For example, it has not attempted to assess what the domestic environment might be like in several years' time, and what, therefore, needs to be done to address shortfalls in our capability to deal with longer-term emerging risks. Some elements of DESC – such as the External Assessments Bureau and the National Assessments Committee – give it an 'over-the-horizon' capability for off-shore events only. Even then, the short-to-medium-term focus means that these capabilities are not used to their full effectiveness to create an 'over-the-horizon' culture throughout DESC.
- 3.16 In our view, a potentially effective way to move the emphasis towards the longer-term would be to give DESC the task of drawing up a domestic security strategy. The strategy work would require DESC to analyse risks, vulnerabilities, and gaps. Once it has drawn up the strategy, DESC should periodically review progress against the strategy, and whether the environment has changed in ways that require the strategy to be updated. The strategy would also facilitate long-term planning and funding of additional capability, based on priorities assessed across the whole of government.

### *Whole-of-government Advice and Reporting*

- 3.17 Whole-of-government advice and reporting on domestic security should not alter the accountability of individual agencies. However, such information and advice is required to provide the Government with a complete picture of domestic security arrangements that would otherwise be difficult to piece together from individual agency reports.
- 3.18 ODESC has begun to provide to the Government (through DES) quarterly security reports that cover issues such as updates on potential threat levels, and progress on security projects and activities. We believe that this reporting should be extended to include information on:
- preparedness of domestic security apparatus – including results of actual responses, exercises, or simulations;
  - changes in vulnerability or risk assessments; and
  - evaluations of the effectiveness of resources.



### A Domestic Security Strategy

- 3.19 There is currently no whole-of-government strategy to guide the efforts of the many agencies involved in domestic security. There is no document or set of documents that sets out:
- the goals and objectives for domestic security;
  - the various roles and responsibilities of the agencies involved in domestic security – including who is responsible for what and where they sit within the whole;
  - key capabilities required of each agency; and
  - identified shortfalls in capability and how and when these will be addressed.

### *Why Have a Domestic Security Strategy?*

---

- 3.20 Domestic security is complex because it involves:
- a range of government and private sector capabilities;
  - a co-ordinated and focused effort from many organisations that may not otherwise need to work together, and for some of which domestic security is not their first priority; and
  - efforts both within New Zealand and abroad.
- 3.21 An overall strategy is needed to:
- co-ordinate efforts to ensure that there are no significant gaps or overlaps in roles and functions;
  - raise awareness of the public and private sector entities that do not have security as a primary priority, and help them to better understand their contribution to domestic security;
  - guide and establish an acceptable level of risk in relation to domestic security – referred to as “risk tolerance”;
  - guide the allocation of financial resources by providing a framework for balancing the benefits and costs of an appropriate level of domestic security effort; and
  - assist in establishing where effort would best be targeted.



## DEVELOPING A CO-ORDINATED RESPONSE

### *Do Other Countries Have a Domestic Security Strategy?*

- 3.22 Australia has a *National Anti-Terrorist Plan* that deals with the three elements described in Figure 2 on page 25 – prevention, response, and recovery. Although not intended to be a national strategy, the Plan includes a section that recognises the need to establish a strategic framework – both in terms of establishing and maintaining international links, and a legal framework within which counter-terrorism can be effectively managed.
- 3.23 The USA released the *National Strategy for Homeland Security* in July 2002. The Strategy establishes three objectives – to prevent terrorist attacks within the USA; reduce vulnerability to terrorism; and minimise the damage and recover from attacks that do occur. It aligns homeland security functions into six critical mission areas<sup>11</sup> that focus on these three objectives. The Strategy also describes four foundations – law, science and technology, information sharing and systems, and international cooperation – that cut across all the mission areas, levels of government, and sectors of society. It establishes the additional resources and capability that needed to be addressed in the 2003 fiscal budget<sup>12</sup> and the 2004 fiscal budget<sup>13</sup>.

### *Current Position in New Zealand*

- 3.24 New Zealand currently has a *National Counter Terrorist Manual* (the *Manual*) that ODESC adopted in 1996. The *Manual* details the policies and procedures that have been developed to co-ordinate the responses of the Government and departments, should a terrorist incident occur. However, the *Manual* was not intended to provide a domestic security strategy and, consequently, does not contain the essential components outlined in paragraph 3.19 on page 41.

11 These six areas are: intelligence and warning, border and transportation security, domestic counter-terrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response.

12 Four priority areas were identified: support first responders; defend against bio-terrorism; secure US borders; and use 21<sup>st</sup>-century technology to secure the homeland.

13 Eight priority areas were identified: enhance the analytic capabilities of the FBI; build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed Department of Homeland Security; create “smart borders”; improve the security of international shipping containers; recapitalise the US Coast Guard; prevent terrorist use of nuclear weapons through better sensors and procedures; develop broad-spectrum vaccines, antimicrobials, and antidotes; and integrate information sharing across the federal government.

- 3.25 The *Manual* is currently predicated on the traditional threats (siege/ hostage, acts of terrorism) and delivery mechanisms (a combined Police/ NZDF response). It reinforces the role of the Police in relation to terrorism as a crime. Responsibility for counter-terrorist operations in New Zealand resides with the Police, with support from other government agencies. The *Manual* recognises that terrorist incidents require political intervention that is facilitated through the DESC structure.
- 3.26 The *Manual* does not take into account more contemporary terrorist threats. In particular, it does not address:
- the prevention and reducing vulnerability aspects of the New Zealand agencies;
  - the levels of effort required during the emergency response and recovery phases of events;
  - the overall framework and the roles that the various agencies play; and
  - areas requiring improvement and where resources – both monetary and human effort – need to be directed.
- 3.27 DPMC has recognised that the *Manual* is narrowly focused and outdated, and has plans to update it. Key departments have also acknowledged that the *Manual* needs to be strengthened in respect of emergency response and recovery.
- 3.28 Work is in progress to provide a national framework, which government departments and other agencies can use to guide and co-ordinate their operational and tactical plans and procedures for counter-terrorism. The framework is intended to provide strategies for prevention, readiness, response, and recovery that:
- meet New Zealand's national interests;
  - minimise the risk of acts of terrorism;
  - quickly restore normality after such an event; and
  - minimise adverse outcomes.



## DEVELOPING A CO-ORDINATED RESPONSE

- 3.29 Key elements of the counter-terrorism framework are to ensure that New Zealand:
- has access to all relevant information (including secret intelligence) relating to terrorist threats;
  - participates effectively in international collective efforts to counter terrorism;
  - has effective security measures in place to protect the population from the risk of a terrorist attack;
  - has the capacity to respond to a terrorist emergency, and maintains an appropriate state of readiness; and
  - has a legislative framework that enables action to be taken against terrorism.

### Supporting Strategies

- 3.30 A number of agencies have prepared strategies that would potentially underpin a national domestic security strategy.
- 3.31 Not surprisingly, given their central role, the Police are preparing a *Police National Security Strategy* that looks likely to provide a good “second-tier” strategy. The draft strategy is aligned with the *Police Strategic Plan to 2006*, and is based on six strategic components – detection, preparation, prevention, protection, response, and recovery – and each component has objectives, a description and success factors.
- 3.32 The strategy goes much wider than traditional policing activity, and includes supporting or working in conjunction with partner agencies, the private sector and the general public. It also includes contingency plans in relation to critical infrastructure, the protection of public health and safety, essential government services, and emergency relief.
- 3.33 The strategy also recognises the connection between New Zealand’s domestic security and criminal links around the world, particularly those that operate in the Asia-Pacific region. It considers the links between trans-national crime – including international manufacture and supply of drugs, people smuggling, and money laundering – and the use of the funds from such crime to support terrorism.





- 3.34 Other potential supporting strategies are:
- the biosecurity strategy;
  - a draft civil defence emergency management strategy; and
  - the National Aviation Security Programme (which is a whole-of-industry strategy).
- 3.35 *Tiakina Aotearoa Protection New Zealand – The Biosecurity Strategy for New Zealand* was released in August 2003. The strategy has a focus on pre-border, border, and post-border activities designed to keep out new pests. The strategy addresses the Crown's role in maintaining and monitoring the framework for pest management – under which agencies, industry, and individuals take collective action against pests. The strategy does not focus on the framework for managing the intentional introduction of new organisms; nor does it discuss bio-terrorism (since it is simply another avenue for transmission of unwanted pests and species).
- 3.36 The need for a border strategy was identified in past reviews of border control. The latest review<sup>14</sup> was undertaken in 1999 and looked at options for improving the effectiveness and efficiency of the border control machinery. The review also looked at border risk management, and noted that:
- the current border management system is limited in its ability to facilitate efficient risk management;
  - each policy agency with an interest at the border prepares its own strategy for managing risks; and
  - as a result, risk management strategies can potentially be in conflict.
- 3.37 Following this review, the Government asked Customs and MAF to jointly lead the preparation of a whole-of-government border vision and strategy. Cabinet has recently withdrawn the requirement for the strategy on the basis that co-ordination between the agencies will be achieved through the Statement of Intent process.
- 3.38 MCDEM is establishing a National Civil Defence and Emergency Management strategy structure. A draft strategy – *Resilient New Zealand* – has been released for discussion purposes. The strategy is focused on reducing vulnerability by increasing awareness, reducing the risks, managing emergencies, and recovering from disasters.

<sup>14</sup> *Border Management – A review of New Zealand's Border Management System*: discussion document, July 1999, ISBN 0-477-01879-3.

## DEVELOPING A CO-ORDINATED RESPONSE

- 3.39 Each of these strategies is being prepared from a particular focus. But only the Police strategy – given the security responsibilities of the Police – is driven specifically from a focus on domestic security. In our view, a national domestic security strategy would provide direction – particularly to agencies for which domestic security is not a primary objective – to enable agencies to define their desired contribution to maintaining and improving domestic security.

### Assessing and Obtaining Resources for Domestic Security

- 3.40 It is important that the resource requirements for domestic security are adequately assessed, and the effectiveness of the use of resources is evaluated. This should include:
- a consistent and transparent basis – linked through to the goals and objectives – for the allocation of domestic security resources; and
  - a clear framework for monitoring and evaluating the effectiveness of the use of these resources.

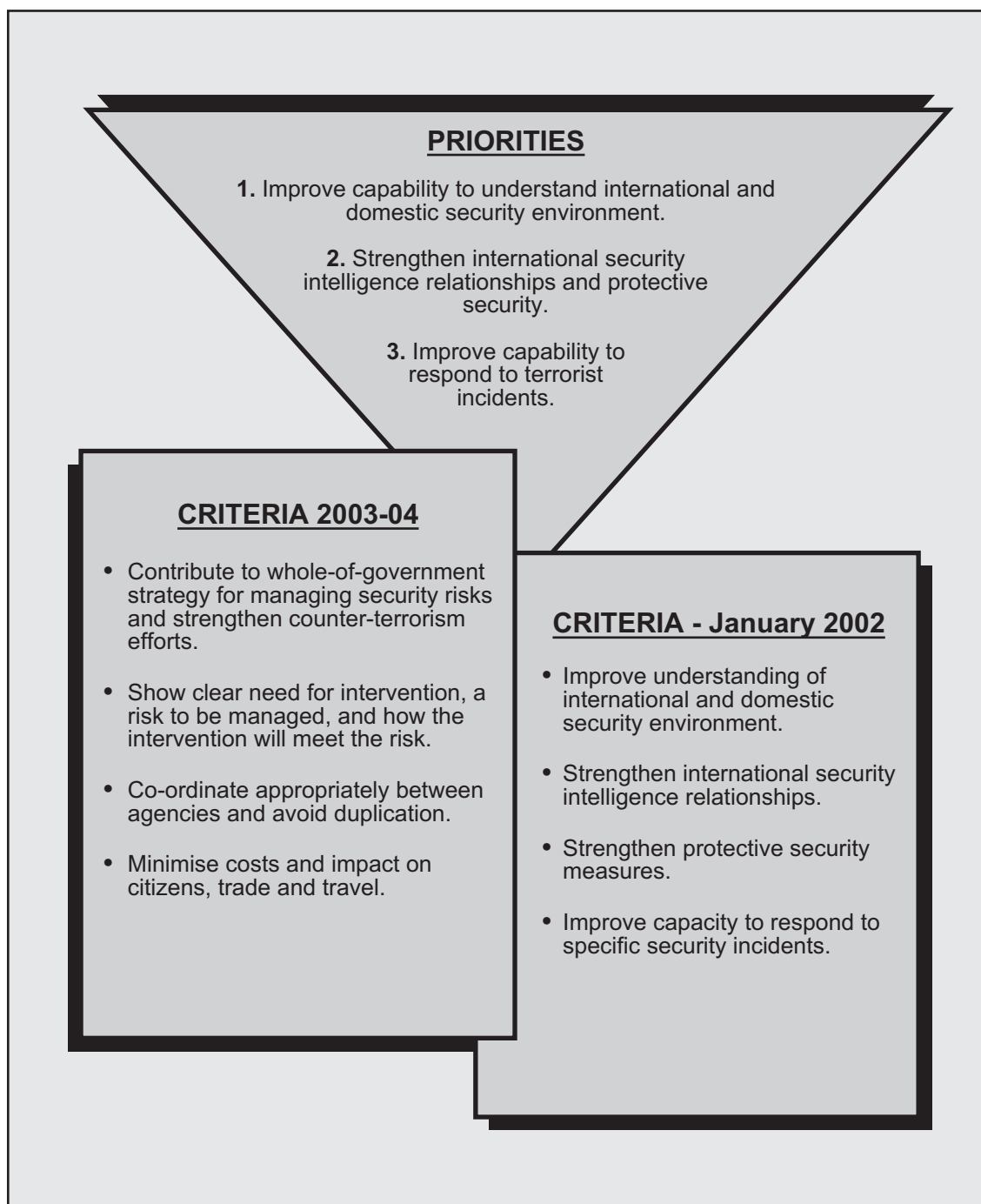
### *Setting the Funding Framework*

- 3.41 Following the September 11 attacks, the Government asked agencies to assess what they needed in order to respond to the changed environment. Their assessments focused on the immediate threats and risks, and whether the actions being taken were sufficient to comply with the Security Council Resolution 1373 (see paragraph 2.19 on page 27 and Appendix 1 on pages 84-87). The Government received proposals totalling \$51.9 million in ongoing operating costs, and \$6.6 million in capital costs to be spent over three years to June 2004.
- 3.42 ODESC endorsed a framework for evaluating the proposals and their funding implications that provided a method for categorising proposals on the basis of their contribution to managing security risks – see Figure 4 on the opposite page showing the criteria for January 2002. ODESC also set three priorities to be applied across the funding proposals, as shown in Figure 4.





*Figure 4*  
*Funding Framework for Domestic Security*



## DEVELOPING A CO-ORDINATED RESPONSE

- 3.43 On the basis of this framework, \$26.9 million operating and \$2.9 million capital funding was approved by the Ad Hoc Committee on Intelligence and Security on 22 January 2002 and was confirmed by Cabinet on 29 January 2002.

### *Refining the Funding Framework*

---

- 3.44 The framework was further refined during 2002. In January 2003, ODESC members decided that the framework was at risk of becoming too detailed to be useful as an evaluation tool, so they agreed to recast it. In late-2002/early-2003, DPMC and the Treasury evaluated domestic security bids and made recommendations to ODESC using a framework that included the refined evaluation criteria for 2003-04, as shown in Figure 4.
- 3.45 In our opinion, the framework would be strengthened if it was linked to an overall strategy and used to define resourcing needs for the medium-to-long term. The current annual focus is unlikely to be able to adequately match future needs to the demands that have been assessed through risk, threat, or vulnerability analyses. More emphasis on medium-to-long-term planning would also support fuller consideration of those capabilities that need to be established before they can be fully effective – for example, intelligence.



## Part Four

# Determining Intelligence Needs and Co-ordinating Information Flows





## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

- 4.1 Intelligence, as far as domestic security is concerned, is information that has been obtained by secret methods or that has been analysed for security purposes. Intelligence is a key element of security. Intelligence is different from most other forms of information in that it needs to be protected and used carefully.
- 4.2 Using the framework illustrated in Figure 2 on page 25, information and intelligence are needed for:
- **Prevention** – in order to know that an event might occur, so that action can be taken to either prevent or mitigate the effects of the event. At this stage, the intelligence is likely to be “sensitive” – it may come from sources that need to be protected. The intelligence may also be relatively obscure, be put together from a variety of sources, and require considerable analysis to put a recognisable picture together.
  - **Response** – The intelligence needs of the various agencies differ widely. For example, the Police want intelligence to assist in establishing who are the perpetrators of any offence, whereas primary responders require situational information to assist their response, e.g. what health facilities are available and their capacity to treat victims.
  - **Recovery** – information is required for contingency planning, roles and responsibilities in relation to recovery. Intelligence is seldom required in recovery.
- 4.3 Ensuring that the right intelligence is obtained and that it is passed on to the right people in a timely manner are key features of the intelligence process. Equally important is analysis of the information from which operational judgements can be made. Inadequate analysis negates any efforts to increase the quality and quantity of information gathered.
- 4.4 In this part of the report, we examine how intelligence needs are met, how the collection and flows of intelligence are co-ordinated, and the specific intelligence requirements for prevention and response.
- 4.5 We also examine the capability among agencies to assess preparedness and undertake effective analysis. We took account of performance measures for, and reviews of, analytical products and the processes for producing them.



## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

### Key Findings

- 4.6 The inter-agency Foreign Intelligence Requirements Committee process (see Figure 3 on page 32 and paragraphs 4.21-4.22 on page 55) establishes clear requirements for the collection agencies to collect foreign intelligence. But a similar process does not exist for the collection of domestic intelligence.
- 4.7 The creation of a more formalised process for sharing information and intelligence would enable individual agencies to share the substantial amounts of intelligence and other forms of information collected as part of their day-to-day business. ODESC recently supported the establishment of the New Zealand Intelligence Community Network (NZIC Net), which will provide a secure communications network to the Wellington intelligence community and key customer departments and agencies. NZIC Net will include secure e-mail services and the capability to distribute secret intelligence reports and classified assessment papers.
- 4.8 Formal and informal mechanisms combine to facilitate the flow of information between agencies and within agencies. These mechanisms are often supported by a co-operative attitude between individuals of different agencies, though inter-agency trust can – and should – take time to develop. Overall, these mechanisms are effective, particularly in relation to responses to incidents.
- 4.9 The maturity of agencies' intelligence functions varied. Some had had extensive experience in intelligence analysis and collection, while others were in the process of extending the breadth of their intelligence coverage. One agency was in the early stages of establishing an effective intelligence capability. We observed differences in agencies' use of intelligence and information – some used intelligence better to support their operations than others.
- 4.10 There are few examples of performance measures or 'lessons learned' reviews for analytical products. There are also few international models of how best to devise and implement new products. Given the very limited existing research and experience, this is clearly an area where agencies could benefit from working closely together and pooling knowledge and resources.



### The Fundamentals of Intelligence Co-ordination

- 4.11 Trust is fundamental to sharing intelligence. If one organisation does not trust another to treat the information it is given with due sensitivity, the level of intelligence sharing between the two is likely to be low. The need for trust based on previous experience and relationships makes it difficult for new participants to enter the intelligence community.
- 4.12 This obstacle has important benefits in placing the onus on new participants to strengthen their systems and processes for handling classified material and information, and helps to maintain the integrity of the system. For example, until two years ago, Customs played a minor role in the intelligence community, and it was not until it improved its own internal security and established a sound intelligence capability that it was able to participate fully in intelligence matters. It is important that existing participants do all they can to bring 'new entrants' up to the required standard.
- 4.13 The system for classifying information is also fundamental. The *Security in the Government Sector*<sup>15</sup> publication provides a classification framework to help ensure a consistent standard across government agencies. Getting information to the people who can take action often requires 'declassification' of some type, a process that needs to consider the source of the information and the attendant risks. Declassification may be required in both passing information between agencies (for example, from the Police to private sector organisations) and within agencies from senior staff with the appropriate clearance to front-line staff (such as Customs staff at airports). All agencies should ensure that they understand these processes.

### Agencies' Use of Intelligence

- 4.14 The value that an agency places on intelligence is generally related to the extent to which it is used to assist, direct, or drive agency operations. Intelligence is also used to inform policymaking. Agencies' use of intelligence to drive operations varies substantially. Some agencies, such as the Police and Customs, have integrated intelligence fully as part of their operations. They use intelligence routinely to identify trends and target their resources.

---

15 See [www.security.govt.nz/sigs](http://www.security.govt.nz/sigs).



## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

- 4.15 Some other agencies do not place as much emphasis on gathering information for intelligence purposes. For example, the Immigration Service has a limited intelligence capability. Its business units may produce valuable information and intelligence, but there are few opportunities to match this with external information, or to establish a Service-wide picture of risks and threats.
- 4.16 The Immigration Service is in the process of improving its intelligence capability, and is planning for an enhanced capability to be operating within a year. Cabinet agreed to allocate \$5.4 million for 2003-04 and \$4.8 million for each subsequent year. The enhanced capability should:
- strengthen links with other security agencies at both the operational and strategic level;
  - help to target resources through the use of risk and threat analyses; and
  - help to comprehensively identify where vulnerabilities currently exist in the system.

### Meeting General Intelligence Needs

- 4.17 We examined the measures that are in place to establish what information and intelligence is needed to warn that a security incident is likely to occur. We also looked at the use made of information and intelligence within and between agencies to identify potential events, and to assist them more widely in undertaking their domestic security functions.
- 4.18 Foreign intelligence is that which is collected to meet the Government's foreign intelligence requirement. Domestic intelligence is that which is collected to meet the relevant agencies' security intelligence requirements. Different procedures apply to these two types of intelligence.

### *Foreign Information and Intelligence*

- 4.19 Both the NZSIS and the GCSB collect foreign intelligence. The NZSIS focus is predominantly domestic intelligence, and the GCSB is focused solely on foreign intelligence.





## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

- 4.20 The GCSB is responsible for collecting and reporting foreign signals intelligence from a variety of foreign communications. It processes, decrypts or decodes and/or translates the information the signals contain before passing the information on as a report to the appropriate government department. It does not assess the information it collects.
- 4.21 The Foreign Intelligence Requirements Committee (FIRC) is responsible for bringing together a range of agencies with the aim of providing to the GCSB and the NZSIS a comprehensive list of New Zealand's foreign intelligence needs. This list is then used to determine and prioritise the foreign intelligence that will be collected, with the aim of effective use of available intelligence resources.
- 4.22 Sub-groups of FIRC (known as CIRGs – Current Intelligence Requirement Groups) have recently been established to give the process for defining information and intelligence requirements enough flexibility to handle immediate needs as they arise. DPMC has also been working with the agencies involved to rationalise the list of requirements to make the collection tasks more manageable, while still providing flexibility to collectors to be alert for intelligence relating to items that are not explicitly on the list.
- 4.23 The strengths of the FIRC process include:
- clear definition of agency needs for foreign intelligence collection;
  - provision of clear guidance for collection agencies to follow; and
  - flexibility to respond to urgent requirements.
- 4.24 In our view, the FIRC process could be further strengthened by undertaking a 'gap analysis' of what the collector agencies have been asked for compared with what they are able to provide. While individual consumer agencies will already be aware of the information they have asked for that has not been provided, a systematic, system-wide gap analysis is more likely to reveal the main areas where collection capability cannot meet the stated requirements. The analysis would also provide assurance on the capabilities available to meet information and intelligence needs.
- 4.25 In addition to the FIRC process, individual agencies receive intelligence and information from overseas counterparts and through membership of international organisations. For example, the Police have access to Interpol, and Customs receives information on the latest methods for smuggling from its international counterparts.



## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

### *Domestic Intelligence*

- 4.26 Unlike foreign intelligence collection, domestic intelligence collection is not based on any consumer/collector system or multi-agency requirement definition. Individual agencies collect large quantities of information and intelligence for their own purposes. For example:
- Customs and the Immigration Service have access to detailed information on both goods and people entering and leaving New Zealand;
  - the Police collect information and produce intelligence in relation to national and trans-national criminal activities (especially the newly established Strategic Intelligence Unit); and
  - the Ministry of Fisheries receives information and intelligence on the movement of fishing vessels around the coastline, the catches, and the potential illegal export of fish.
- 4.27 The NZSIS has responsibilities under its Act<sup>16</sup> to obtain, correlate and evaluate intelligence relating to security. Much of the intelligence collected is secret.<sup>17</sup> The Director of the NZSIS has the legislative authority<sup>18</sup> to decide what intelligence will be collected and to whom it will be communicated.
- 4.28 The NZSIS considers its requirements and resources twice a year. The first exercise formally establishes the Objectives and Requirements Plan for the coming year, and the second (mid-term) exercise reviews the Plan decisions.
- 4.29 The NZSIS consults a range of other agencies in the areas of its operations in which it shares responsibilities – such as counter-terrorism – or in which it collects intelligence in support of the requirements of other agencies – as in illegal immigration. While the consultation appears sound, the setting of the final Objectives and Requirements Plan is entirely internal to the NZSIS.
- 4.30 We believe that more interaction with other relevant agencies would be likely to lead to plans that better reflect wider intelligence requirements. Greater interaction could include invitations to other domestic security agencies to submit their needs for input into the objective-setting process.

16 The New Zealand Security Intelligence Service Act 1969.

17 “Secret” in that the holders of the information would prefer that lawful authorities were not aware of the content of that information.

18 Section 4 of the New Zealand Security Intelligence Service Act 1969.



- 4.31 These additions would not alter NZSIS control over the process. The final decisions on what information is to be collected would remain with the Director, consistent with his independence in these matters.
- 4.32 Further, we consider that there would be benefit in formalising domestic security intelligence collection along the lines of the FIRC process. A more formal process should be in conjunction with, and support, individual agencies continuing to pursue their own information and intelligence needs. It should ensure that any duplication is reduced, and that opportunities for co-operation are taken.

### Co-ordinating the Flow of Intelligence

- 4.33 The GCSB and the NZSIS have formal and informal processes for disseminating the intelligence they provide. The GCSB has liaison officers sited within key customer agencies for this purpose, and the NZSIS has daily or as required delivery arrangements with its customer agencies. Both agencies have a programme of visits.
- 4.34 The NZSIS also has a formal system for assessing how agencies rank the value of foreign intelligence it provides.
- 4.35 There are few formal processes to co-ordinate information collection and flows more widely across the various agencies. We noted the following examples:
- In particular circumstances, DPMC will form Watch Groups to monitor developments (e.g. the potential for sea-borne unauthorised migrants). These are multi-agency, and continue until the need diminishes to the point where inter-agency processes resume (see paragraphs 4.40-4.41 on page 59).
  - The Police Strategic Intelligence Unit produces reports on subjects of relevance from a domestic security perspective and disseminates them to partner agencies as appropriate.
  - Customs and the CAA have established a system to process the information that they receive, which other agencies have access to and are able to use.
  - The arrangements for co-ordinating the collection of maritime intelligence (see Figure 5 on the next page) facilitates close co-operation between agencies to achieve whole-of-government goals, a common understanding of the maritime environment, and effective use of Government resources.

## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

*Figure 5*  
*Co-ordination of Maritime Intelligence*

The National Maritime Co-ordination Centre (NMCC) was established in 2002 and is governed by the Chief Executives from NZDF, Fisheries, Customs, the Police and the MSA. The centre is co-located with the NZDF Joint Force Headquarters in Trentham and is staffed from the NZDF and the civilian agencies. The NMCC is responsible for co-ordinating maritime surveillance to:

- maximise the effectiveness of New Zealand's maritime surveillance assets;
- ensure the best possible use of available information; and
- enable a whole-of-government approach to maritime security, using a common risk management framework.

Its two main functions are therefore co-ordinating:

- agency maritime patrol and response activities; and
- the provision of a maritime intelligence picture compiled from multiple sources to participating agencies.

The NMCC does not have any direct operational responsibilities; these remain with the individual agencies.

A Risk Management Framework has been established which provides a clear methodology to assess security risks and enable competing patrol tasks to be prioritised on a multi-agency basis.

- 4.36 Informal interactions range from telephone calls and informal meetings between individual security analysts to the establishment of semi-formal groups. A Combined Law Agencies Group (CLAG) was set up in 1999 to improve co-ordination between agencies at an operational level, and there are now a number of regional CLAGs that operate under a national-level CLAG. They have evolved over time to include networking and information sharing as well as allowing law agencies to co-operate on common issues. Membership of a regional CLAG varies depending on agency representation in the region.
- 4.37 Agency officials involved in the CLAGs valued the groups, especially the informality and the flexibility of their size and location (for example, a location such as Auckland Airport could have a CLAG). They have enabled networks to be developed that have been helpful when needing to make contacts or initiate more formal co-operation.

- 4.38 While the initial informality of the CLAGs had some disadvantages, they have evolved to be an officially mandated accepted element of the law enforcement environment in New Zealand.

### *Intelligence Co-ordination During Response*

---

- 4.39 We examined the processes and procedures to co-ordinate information and intelligence during security incidents or where incidents are highly likely to occur.

### **Responding to Potential Incidents**

- 4.40 ODESC and its Watch Groups provide an effective mechanism to co-ordinate information and intelligence flows in relation to potential events or actual events. Sometimes ODESC will meet when potential events requiring a combined agency response are identified (for example, the potential arrival of a boat carrying illegal immigrants). In such cases, irrespective of whether an immediate operational response is required, a Watch Group is often formed to keep the situation under review.
- 4.41 On other occasions, a Watch Group is formed to keep the situation under review even if it is not considered necessary to convene ODESC at that time. If circumstances worsen, ODESC would be convened. In all cases, reports are made to Ministers – for information or decisions. ODESC and Watch Groups both provide opportunities for agencies to exchange information and intelligence about potential and actual events.

### **During Response to a Specific Incident**

- 4.42 The co-ordination of information and intelligence at times of specific incidents is relatively well developed.
- 4.43 Co-ordination of information and intelligence in respect of a terrorist incident is achieved through the Joint Intelligence Group (JIG), comprising analysts from the Police and other agencies<sup>19</sup>. The JIG draws together and assesses all sources of intelligence to support the Police Operation Commander, and/or provide strategic intelligence to ODESC and Ministers (which together constitute the Terrorism Emergency Group) where a strategic response is required. The Police determine the JIG's size, structure and location, taking account of the nature of the terrorist incident.

---

<sup>19</sup> A Memorandum of Understanding is agreed between agencies employing intelligence analysts, to provide intelligence support to the JIG in the event of a terrorist incident.

## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

- 4.44 An ad hoc Intelligence Co-ordinator is generally also appointed to:
- liaise with the Police to co-ordinate specific requests from officials for further intelligence and information from the JIG to support policy formulation and decision-making;
  - co-ordinate the strategic assessments (forward-looking and longer-term) required to inform Government decision-making, using the widest possible range of intelligence from both open and secret sources; and
  - arrange for particular aspects to be analysed by a specific agency other than the JIG if the Watch Group considers it necessary.

### Responding to Other Incidents

- 4.45 Most incidents, whether major emergencies, disasters, or localised incidents, require a response from a number of different agencies. No single agency or department is able to handle a large-scale incident alone.
- 4.46 The Co-ordinated Incident Management System (CIMS) is designed to improve the management of the response phase to emergency incidents through better co-ordination between the major emergency services (Fire, Police, Ambulance, and Civil Defence). It also provides for co-ordination with the various other organisations that have a role in emergency response (local authorities, NZDF, MSA). CIMS is used in responding to natural hazards, incidents involving multiple casualties, environmental incidents, and public health and medical emergencies.
- 4.47 CIMS provides an effective way to facilitate information co-ordination when responding to an event. It was established to address a number of problems identified with emergency response including:
- non-standard terminology among responding agencies;
  - non-standard and non-integrated communications;
  - lack of consolidated action plans; and
  - lack of facilities designated as available for a response.





## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

- 4.48 To help co-ordinate the effective use of all available resources, CIMS is built around four major sections:
- **Incident Control** – is responsible for the overall direction of the response, and the management of an incident across agencies. An incident will have only one incident controller, but multiple lines of command depending on the number of agencies involved.
  - **Planning/Information** – includes gathering, evaluating and disseminating information about the incident and the status of resources. This section is also responsible for the creation of an Incident Action Plan.
  - **Operations** – is responsible for carrying out the response activities described in the Incident Action Plan and directing an agency's resources in combating the incident.
  - **Logistics** – is responsible for providing facilities, services and materials required to combat the incident.
- 4.49 CIMS can be expanded and contracted to manage the response to varying types and sizes of incidents – including single agency responses, multi-agency responses, major incidents requiring maximum organisation support, and multi-incident responses.

### Providing Effective Analysis of Information and Intelligence

- 4.50 Making good use of intelligence and information requires sound analysis – including consideration of alternative means of analysis; otherwise the effectiveness of collection efforts is undermined. We therefore looked for performance measures around, and reviews of, analytical products and the processes for producing them.
- 4.51 We did not find many examples of reviews of analytical products and processes. The intelligence section of Customs has good practices in this respect – for example, external review is a quality indicator. Some other agencies attempt to evaluate the quality of analytical products, but not in a formal manner. Most agencies rely on individual analysts' performance agreements to monitor the quality of analytical products.





## DETERMINING INTELLIGENCE NEEDS AND CO-ORDINATING INFORMATION FLOWS

4.52 New Zealand agencies are not alone in this respect. Our field work in Australia and the USA, and the available literature, illustrated that other countries also struggle with determining performance and quality measures for analytical products. Techniques exist, but have not been used systematically to create an analytical quality system. The techniques include:

- Using ‘A’ and ‘B’ teams for competitive analysis – this involves having two teams analyse information or a situation independently, and the two results are then compared. This technique is often used to challenge assumptions that analysts may be using when undertaking their work.
- Interdisciplinary review and debate – a form of external review but with a focus on the reviewers challenging the mindset that was used to design the analytical product.
- Matrix-form evaluation – where competing hypotheses are lined up against each other and actual analytical products compared.



## Part Five

# Assessing the Capability to Respond





- 5.1 It is important that agencies know what level of threat they are expected to prepare for, and the type of incidents they are expected to respond to – and that the Government knows and monitors agency capability from each of these perspectives. It is also important that any capability gaps are known and communicated.
- 5.2 We looked at capability from two perspectives:
- Capability to perform day-to-day functions – generally a pre-emptive and preventative capability that includes the functions of the border agencies, AvSec and the MSA.
  - Capability to respond to particular events – a capability that includes contingency planning and encompasses the ability to respond to and mitigate the consequences of particular situations and events.
- 5.3 We examined:
- the extent of expectations about capability;
  - monitoring the extent to which agencies were meeting those expectations;
  - the training for and testing of responses, and contingency planning for anticipated incidents; and
  - monitoring of capability across agencies and functions.

### Key Findings

- 5.4 The security environment and the need for New Zealand to keep pace with international expectations and obligations largely drive day-to-day capability expectations for preparedness to meet security threats. Agencies individually monitor these expectations and assess what additional resources they require to meet them.
- 5.5 There is no central monitoring of key capabilities and preparedness across agencies. Monitoring (to varying degrees) takes place through agency accountability reporting, but this is mainly from an individual business perspective. Similarly, there has been no overall ‘stock-take’ of all capabilities that contribute to domestic security. This increases the risk of duplication of effort or capabilities.



## ASSESSING THE CAPABILITY TO RESPOND

- 5.6 Agencies' testing of their own systems and capabilities is variable. AvSec and the NZDF have extensive capability testing, but the majority of agencies are currently still designing their procedures, and they still need to establish procedures to measure their effectiveness.
- 5.7 Multi-agency exercises and simulations conducted to test the whole-of-government response to particular events provide an effective method to test systems and build relationships. A continuous, co-ordinated programme for all agencies to test their own systems and capabilities would further enhance the effectiveness of these exercises. Depending on the nature of the particular exercise, they could also usefully be extended to include front-line providers.
- 5.8 Multi-agency and individual agency exercises both currently focus on the response phase, with little emphasis on recovery. Substantial work is currently being undertaken to incorporate recovery into future exercises.

### Setting Day-to-day Capability Expectations

- 5.9 In the light of Resolution 1373 (see paragraph 2.19 on page 27 and Appendix 1 on pages 84-87), the Government asked agencies to review their procedures and resources to assess whether they were sufficient to respond to the new terrorist and security risks. The agency reviews identified areas that needed to be strengthened – including:
- legislative changes to give effect to the new international requirements;
  - improved intelligence capability – especially for GCSB, the NZSIS, Customs, and the Police;
  - changes in certain procedures – such as screening of export consignments (including mail) and examination of containers; and
  - implementation of additional systems – such as an Advanced Passenger Processing System to obtain data on all passengers on participating airlines.
- 5.10 Since their initial review, agencies have continued to monitor the security environment and the additional resources they require in order to keep pace with:
- international expectations; and
  - obligations to trading partners.



### *International Expectations*

- 5.11 International expectations and the related security initiatives are being driven through agency membership of international organisations as well as a variety of forums, Conventions and Protocols (that often include standards and recommended practices), and memoranda of understanding between countries.
- 5.12 These international obligations are also reflected in New Zealand's membership of international organisations. For example, Customs participates in the WCO, which is currently undertaking to:
- standardise information for identifying high-risk cargo;
  - develop guidelines for electronic submission of customs data; and
  - in conjunction with the International Maritime Organisation (IMO)<sup>20</sup>, identify measures to support increased supply chain security and secure containers.
- 5.13 Requirements for baggage screening and advance passenger information also arise through New Zealand's membership of the International Civil Aviation Organisation (ICAO)<sup>21</sup>. Members must comply with standards and recommended practices in Annex 17 to the Convention on International Civil Aviation, and these have been incorporated into our National Aviation Security Programme (see Figure 6 on the next page). For example, passengers on all domestic flights seating more than 90 passengers are required to be screened prior to boarding, and additional screening procedures required by 1 January 2006 for hold baggage will have a large impact on the aviation sector.
- 5.14 A similar framework is being adopted for Maritime Safety. The IMO introduced new security measures, which will come into force on 1 July 2004, to prevent the introduction of unauthorised weapons or dangerous substances and devices to ships<sup>22</sup> or port facilities (see Figure 7 on page 69).

20 The United Nations agency responsible for international conventions relating to maritime safety and marine environment protection measures.

21 The Civil Aviation Authority is a member of the ICAO Aviation Security Panel.

22 As a minimum, this must include passenger ships on international voyages, international cargo ships of 500 gross tonnage or more, and mobile offshore drilling units.



## ASSESSING THE CAPABILITY TO RESPOND

*Figure 6*  
*New Zealand Aviation Security*

Annex 17 to the Convention on International Civil Aviation – *International Standards and Recommended Practices – Security – Safeguarding International Civil Aviation Against Acts of Unlawful Interference* contains standards and recommended practices to be followed by contracting states, including:

- organisational aspects such as the establishment and implementation of a national civil aviation security programme and designating an appropriate authority to be responsible for the programme, airport operations, aircraft operators and quality control;
- preventative security measures relating to aircraft, passengers and their cabin baggage, hold baggage, cargo, mail and other goods, special categories of passengers, access to the aircraft, and restricted areas of airports; and
- responding to acts of unlawful interference – including prevention, response and exchange of information and reporting.

The Convention and standards are given legal effect by the Civil Aviation Act 1990, Aviation Crimes Act 1972, Civil Aviation (Offences) Regulations 1997, and Civil Aviation Rules.

New Zealand has drawn up a *National Aviation Security Programme* that incorporates the standards and recommended practices. The *Security Manual for Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, an ICAO advisory document, was also used as guidance by the CAA in drawing up the *National Aviation Security Programme*.



*Figure 7*  
*New Zealand Maritime Security*

IMO guidance recommends screening and/or searching of people, their possessions, vehicles, ships' stores and cargo entering a port facility, where such activities have been identified as necessary through the risk assessment and port facility plan process. There is a growing expectation in the cruise ship industry that similar screening measures to those adopted in air travel will be implemented for cruise ships.

The principal requirement for governments is to regulate ship and port facility regimes by assessing risks at port facilities that service international traffic; approving and auditing ship and port facility security plans; and setting the security (threat) level at which ships and ports operate. The MSA is the regulatory authority responsible for administering and ensuring compliance with the new security measures.

The MSA has established a number of representative bodies:

- A National Port and Ship Security Committee – comprising representatives of the border control agencies including MoT, Police, Customs, MAF, Food Safety Authority, Immigration Service, as well as the security and intelligence agencies – has been established to ensure a whole-of-government approach. This Committee, among other things:
  - considers requirements for and outcomes of port facility security assessments;
  - considers MSA's recommendations on which ships and port facilities will be required to prepare security plans; and
  - determines procedures for moving from one security level to another.
- A National Port and Ship Consultative Committee – to enable effective consultation with the maritime community and includes representatives from port and shipping companies, port and shipping users, maritime employee organisations, shipping agents, stevedores and Cruise New Zealand.
- Local Security Committees – convened at each port to replicate the National Consultative Committee and have a key role in establishing security measures at each port facility.

Legislation has been introduced in the Maritime Security Bill to give effect to the new measures.





## ASSESSING THE CAPABILITY TO RESPOND

### *Obligations to Trading Partners*

- 5.15 Improving supply chain security (in particular, container security) is increasingly emerging as a requirement of international trade. The initiatives have so far been driven by the USA, and the requirements being imposed are analogous to New Zealand's established arrangements for biosecurity checks on passengers and goods entering the country.
- 5.16 Figure 8 on the opposite page describes two USA initiatives that have required changes in procedures for cargo bound for, or passing through New Zealand to, the USA, including cargo remaining on board.

### *Publication of Day-to-day Capability Expectations*

- 5.17 Capability expectations for day-to-day activities are set out in agencies' purchase agreements with their ministers. They are also articulated in their departmental Forecast Reports and Statements of Intent.
- 5.18 The capability expectations set out in these documents have been variable between agencies, and often non-specific. These shortcomings have been identified and agencies are beginning to address them.
- 5.19 We reviewed five departmental Forecast Reports or Statements of Intent for 2003-04.<sup>23</sup> Each included improving national security (or biosecurity in relation to MAF) as an outcome. Customs, in particular, noted a shift to *a strong active border security to provide assurance that goods, people and craft arriving in New Zealand do not pose a threat to this country; and security of the export supply chain to provide assurance to both New Zealand and our trading partners.*
- 5.20 The departmental documents also linked the outcome to specific actions or intermediate outcomes. However, except in relation to Customs, there was still a need to explain links to agencies' outputs.

---

23 Police, Customs, NZDF, MAF, and Department of Labour (Immigration Service).



*Figure 8*  
*Obligations of Exporters to the United States of America*

### **Container Security Initiative (CSI)**

This initiative (which has been endorsed by WCO) involves US Customs officers working with counterparts in foreign ports to identify high-risk containers and search them before they are shipped to US ports. It uses X-ray and gamma ray technology for rapid pre-screening, and promotes the use of more secure types of containers.

The initial goal is to work with 20 ports that jointly account for a large proportion of the containers that enter the USA. Speed and predictability for container movements will increase because pre-screened containers may be released immediately on arriving at the US seaport. High-risk containers that have not been screened will be delayed until US Customs screens them.

The procedures require exporters to:

- have cargo at the port of departure at least 24 hours prior to the vessel arriving at the port; and
- submit cargo declarations to US Customs at least 4 working days prior to the vessel arriving at the port of discharge.

### **Customs-Trade Partnership Against Terrorism**

This is a joint government-business initiative to strengthen overall supply chain and border security. It involves US importers – and ultimately carriers and other businesses – entering into voluntary agreements with US Customs to enhance the security of their global supply chains and those of business partners. In return, US Customs will agree to expedite the clearance of the members' cargo at US ports of entry. Trading partners of the importers involved in this initiative will have to make changes to enable the importers to fulfil their agreements.

## **Monitoring Against Day-to-day Capability Expectations**

- 5.21 Agencies are required to report against the objectives in their Statements of Service Performances in their Annual Reports. In addition, each border agency undertakes some preparedness monitoring from an individual business perspective. Some use the ISO framework for this purpose, and accreditation against ISO standards provides a useful and systematic framework.



## ASSESSING THE CAPABILITY TO RESPOND

- 5.22 With regard to new and recent expectations, most agencies are currently still developing or working through processes for addressing them. Agencies that are by the nature of their responsibilities more mature in respect of domestic security provide examples that others can follow. For example, AvSec has relatively well advanced arrangements with clear procedures and standards, obligations to a range of stakeholders, and audits by a number of organisations – including:
- the (USA) Federal Aviation Administration and other international authorities;
  - the (NZ) Civil Aviation Authority (of which AvSec is a separate function);
  - the BVQI (the Bureau Veritas Quality International)<sup>24</sup>;
  - the (NZ) Ministry of Transport; and
  - airlines (which rely on the work of AvSec).
- 5.23 Screening tests covering AvSec's operations include aircraft searches, metal detector and X-ray searches, and physical search procedures. The results are reported monthly to the agency's General Manager.
- 5.24 Few<sup>25</sup> agencies undertake systematic "stock-takes" of their day-to-day capabilities. In most cases, such stock-takes would be very large exercises, and some agencies have undertaken reviews of key parts of their processes – for example, in September 2002, MAF published a review of biosecurity surveillance programmes operated by itself and other government departments. The aim of the review was to establish a framework for prioritising surveillance programmes, and an economic model to help determine appropriate funding levels for surveillance.
- 5.25 In our November 2002 report *Ministry of Agriculture and Forestry: Management of Biosecurity Risks*, we recommended that MAF and the other departments involved in biosecurity matters consider the need for a wide-ranging review of biosecurity capability (including preparedness for one or more major incursions)<sup>26</sup>. Even a single review such as this would be a large undertaking. Such reviews therefore need to be part of a planned programme of capability reviews. And given the interdependence of many of the agencies, they

24 An international certification organisation.

25 The NZDF routinely reports on the day-to-day capabilities of its force elements through the Operational Preparedness Reporting System.

26 Report available on our web site [www.oag.govt.nz](http://www.oag.govt.nz); ISBN 0-477-02898-5; see paragraph 3.51 on page 43 and related paragraphs 3.35-3.39 on pages 39-40.



need to plan the reviews together, so that in due course the results of a range of reviews can be added to the total knowledge that is available to assess overall capability for domestic security.

- 5.26 Capability reviews along these lines will require sophisticated measurement techniques to be developed to test key security elements. For example, the US Transportation Security Authority uses ‘fake’ contraband items (including bombs and weapons) to test detection systems and procedures. In New Zealand, AvSec uses similar techniques, and MAF tests systems at ports of entry on a random basis by having people attempt to bring in restricted items.
- 5.27 These kinds of tests could usefully be routinely operated across all border security agencies. They are particularly helpful in assessing the level of ‘risk tolerance’ that needs to be accepted, what level of further resource investment is needed to keep risk below acceptable levels, and what systems and procedures need to be strengthened. For example, it would be possible to assess what percentage of weapons illegally coming into the country would be picked up by current procedures, and to do further work to estimate the extra cost of increasing the percentage of weapons that are identified.

### Planning and Monitoring the Capability to Respond to Events

#### *Whole-of-government Response Through DESC*

- 5.28 In March 2002, the Government adopted the DESC structure to facilitate a whole-of-government approach to national crises and circumstances affecting security. As described in paragraphs 2.37-2.38 on page 31, DESC has two main components that work closely together – one to develop high-level whole-of-government approaches and policy, and the other to concentrate on crises as they arise.
- 5.29 When a crisis or event occurs, one agency takes responsibility for leading the operational response – normally the agency with the statutory responsibility and/or specialised knowledge for managing the particular crisis – such as the Police in relation to a terrorist emergency, or MAF in relation to a foot and mouth disease outbreak. The lead agency establishes an operational group to help manage the crisis, which includes assistance from other relevant agencies.

## ASSESSING THE CAPABILITY TO RESPOND

### *Exercises and Simulations to Test Whole-of-government Response*

- 5.30 Exercises and simulations provide important information on the capability of participants, and feed back into planning of future responses.
- 5.31 For example, a half-day simulation based on a foot and mouth disease scenario showed the need for better definitions of structures and roles, and better support. It also illustrated the need for further work by the Reserve Bank and the Treasury into the likely macroeconomic impacts of an outbreak<sup>27</sup> – which would be important information for the recovery phase that we consider in paragraphs 5.55-5.56 on page 80.
- 5.32 The Police, under the guidance of ODESC, are responsible for planning multi-agency simulations of possible terrorist incidents known as Exercise Guardian and Exercise Lawman. These exercises are large and resource-intensive, and the Police attempt to base them on up-to-date knowledge of the most likely terrorism threats:
- Exercise Guardian is a ‘tabletop’ exercise that has no operational elements deployed, but usually tests the decision-making aspects of an event, and the information and intelligence flows that are essential to a successful outcome.
  - Exercise Lawman utilises the full range of required assets – from co-ordination resources through to ‘on-the-ground’ units. Both exercises involve the participation of Ministers as a key element.
- 5.33 These multi-agency exercises are central to the domestic security arrangements. However, they take up a large amount of resources and cannot be undertaken with the frequency that would be required to cover all the most likely scenarios. They also have to be planned carefully to achieve maximum coverage of important issues, while at the same time ensuring that single key agencies are not over-burdened with the repeated need to participate, and that agencies with a less central role are not involved so infrequently that they have to re-learn how they should interact with other agencies in each exercise. ODESC is currently reviewing the frequency of the exercises in response to concerns raised in post-exercise reports.

---

<sup>27</sup> See [www.rbnz.govt.nz/research/0130346.html](http://www.rbnz.govt.nz/research/0130346.html).



- 5.34 The exercises have been run as ‘warm starts’ – which effectively means that agencies had advance notice, and systems (such as IT and communications) were set up before the exercise started – and the set-up phase of the exercise was not practised or reviewed. The establishment of a permanently set up National Crisis Management Centre in the Beehive basement is aimed at removing this deficiency.
- 5.35 We found good examples of contingency planning, exercises, and simulations as part of some agencies’ own operations. They provided an effective method to test systems and build relationships to enhance preparedness. For example, MAF carries out an annual exotic disease simulation exercise to maintain competency for staff involved in responses. Until 2000, the simulations were based on a foot and mouth disease scenario. Since then, there have been simulations based on Nipah virus in pigs and Newcastle disease in poultry, and a simulation based on an Anthrax scenario was carried out in November 2002.
- 5.36 The MoH recently ran a large simulation on an influenza pandemic – see Figure 9 on page 76. The exercise identified the following capability needs:
- establishment and maintenance of well-developed communication paths between the MoH and providers (such as general practitioners and rest home operators);
  - databases identifying local providers, resources, and supplies;
  - a Resource Command Centre with appropriate equipment and supplies, and improved communications within the Command Centres; and
  - a review of lessons learned during the exercise.
- 5.37 Since this exercise the MoH has established a Command Centre (called the Emergency Response Management Centre), which can be set up within an hour or so. This centre was last activated for the SARS response group. The MoH also noted that better communication linkages now exist, and it has a debriefing procedure to review how it handled the response.





## ASSESSING THE CAPABILITY TO RESPOND

*Figure 9*  
*Simulation – The Virus has Landed 02*

An influenza pandemic occurs when a new type of influenza virus emerges and spreads to most countries around the world. Because the virus is new, no one has immunity and many people become seriously ill. The pandemic can cause widespread death and illness, as well as social and economic disruption.

The aims of the exercise were to practice and evaluate the New Zealand influenza pandemic plan, and the operational response through District Health Boards' major incident and emergency plans and public health response plans.

**The objectives** of the exercise for the MoH were to:

- mitigate, respond to, and recover from a national influenza pandemic;
- test the communication links with the District Health Boards and public health services;
- identify triggers for escalation within the plan;
- gather and analyse information from District Health Boards to provide an action plan; and
- identify the gaps and overlaps within the planning process.

**The scenario** was devised around the *WHO – Pandemic Alert Levels* and the *New Zealand Influenza Pandemic Plan* and had five stages. The objectives not tested were the recovery from the event and preparation for the second pandemic wave.

**The participants** were: the MoH – Emergency Response Centre, Public Health Services and Communicable Diseases Team; District Health Boards' public health services; and the National Pandemic Planning Committee.

- 5.38 District Health Boards are responsible for their own contingency planning and testing. Information on the capacity of District Health Boards to deal with crises and on the results of their testing is not maintained on a national basis. A similar issue was noted in relation to the MAF exercises, with the need to involve and know more about the capability of veterinary staff from private practice.





- 5.39 The MoH told us that work is currently being undertaken to address this issue. At the time of writing this report, ODESC was considering a proposal for regularly scheduled national level exercises across a number of government agencies and threats. The agencies currently being considered are at least the MoH, MAF, the Police, and MCDEM.
- 5.40 Currently, no programme brings together both multi-agency and individual exercises and simulations to ensure that adequate coverage and frequency across all agencies is achieved. Such a programme would also help agencies to identify opportunities for useful involvement in other agencies' exercises.

### *Learning from Actual Events*

---

- 5.41 We found a number of examples of post-operation reports and reviews undertaken after security incidents had occurred. These reviews focused on how agency performance could be improved, and illustrated a willingness among agencies to learn from real events and use them to ensure continuous improvement.
- 5.42 Two recent examples were post-operation reports from an incident where a suspected lethal chemical device was left on the steps of the Motueka Police Station, and the New Zealand consular response to the Bali bombings.
- 5.43 Each incident involved a range of agencies and identified key points for improvement in the future. In the Motueka case, there was no laboratory in the South Island with the ability to test the substance in the suspect device. It could not be transported by air to the North Island because the substance was unknown. The responders had to destroy the substance and forgo identifying it.
- 5.44 Consular staff took on the responsibility to identify bodies in the immediate aftermath of the Bali bombings. Post-operation reports noted that such tasks should have been carried out by specialists (the Police sent specialists within two days of the bombings), and suggested that cross-agency 'early response teams' be set up for use in such circumstances. These teams would be able to quickly assess specialist needs and arrange for them to be provided. In our opinion, such a team would have been a valuable asset in the Motueka incident as well.
- 5.45 The MoH used the recent international SARS outbreak to improve its contingency plan for a pandemic outbreak.

## ASSESSING THE CAPABILITY TO RESPOND

### *Securing Specialist Skills*

- 5.46 Most agencies have specialist skills that may be useful to the agency that is leading a response. For example, the Prime Minister (or if unavailable, the next most senior Minister) may authorise the NZDF to assist the Police to deal with some aspects of a terrorist emergency – such as:
- storming buildings and retrieving hostages;
  - locating and defusing bombs;
  - land, sea and air surveillance; and
  - personnel trained in defensive cordon or perimeter duties.
- 5.47 The Ministerial authorisation is based on information supplied by the Commissioner of Police (or Deputy Commissioner of Police) that the Police cannot deal with the emergency without the assistance of members of the Armed Forces exercising powers that are available to members of the Police.
- 5.48 Where NZDF assistance is sought, the Police remain in charge of the operation and a plan exists covering NZDF assistance to the Police in counter-terrorism operations, and the execution and command and control arrangements throughout.
- 5.49 The Chief of Defence Force, in support of the Police, may also authorise administrative support – such as transporting Police personnel; and logistic services, such as catering and medical support, that the NZDF is skilled in setting up in locations not specifically designed to accommodate them.
- 5.50 The NZDF played an important part in the post-September 11 review of resources and capability. The NZDF had an Improvised Explosive Device Disposal team, but the team had shortfalls in its capability to defuse chemical and biological bombs, and received funding to address the shortfalls. The NZDF was also able to point to a wider shortage of facilities to decontaminate emergency staff or civilians affected by a chemical or biological incident.
- 5.51 The New Zealand Fire Service has a relatively sophisticated decontamination facility for chemical spillages in the three main centres<sup>28</sup> and an anthrax decontamination protocol was drawn up. The NZDF and the New Zealand Fire Service are cooperating to ensure that the capability held between them both is optimised (i.e. duplication is minimised).



- 5.52 The CTG of the New Zealand Special Air Service reports its preparedness regularly as part of the NZDF's preparedness reporting system. This reporting covers issues such as the availability and serviceability of mission-critical equipment and the required level of manpower, and provides the Government with assurance that the CTG will be able to perform to the expectations set in its Purchase Agreement. For example, the agreement states that the Government expects the CTG to be available at very short notice, and able to cover certain contingencies. The reporting has clearly described areas of capability that are being improved, and has made it possible to monitor what shortfalls exist and what is being done to rectify them.
- 5.53 The Police STG, being an operational group continually being deployed against prioritised needs, reports preparedness in terms of total training hours. Since this provides only a very limited indicator, post-operation reports are in practice the key measurement tool for operational preparedness. We examined some post-operation reports and found them to be good examinations of events, including comments on the soundness of procedures and equipment used.
- 5.54 The STG has been looking into implementing reporting improvements and, given the range of capabilities of the STG and the importance of its role, there would be value in the STG considering the preparedness monitoring system used by the NZDF for the CTG. Such a monitoring system might include:
- expectations from the Government and within the Police of what the STG is to provide in terms of capability and response times;
  - checks on required manning levels;
  - statements on training completed compared with training planned; and
  - statements on response times to actual events.

---

28 The decontamination capability is more basic in smaller centres.



## ASSESSING THE CAPABILITY TO RESPOND

### *Capability to Recover From an Event*

- 5.55 The initial response to an event is of critical importance, but it is widely recognised that the recovery phase is of equal importance if further damage is to be avoided and communities or services are to be restored as quickly as possible. However, little work has been done on capability to recover from a domestic security event, and we identified gaps in a number of areas:
- whole-of-government and individual agency exercises tend to focus on the response phase to any scenario, with little time spent on the recovery phase;
  - recovery contingency planning for some critical infrastructure has not been undertaken<sup>29</sup>; and
  - no stock-takes of resources available for recovery from various events have been undertaken to check whether the necessary resources can be obtained when required.
- 5.56 Agencies have recognised these gaps and related work is in progress. For example, DPMC is looking at how to integrate the recovery phase into future exercises. MCDEM is looking to assessing recovery needs as part of its new National Strategy and Plan. What these agencies are doing would be enhanced by having an overall plan to ensure that the most critical areas are being covered, and to the depth required.

### **A Stock-take of Capabilities for Responding to Events**

- 5.57 As for day-to-day capabilities (see paragraph 5.24 on page 72), few agencies undertake systematic stock-takes of their capabilities to respond to events. A whole-of-government stock-take would help to identify any overlaps or gaps. It would be a large exercise, but information already exists that could be built upon.

---

<sup>29</sup> For critical infrastructure, key lifeline utilities are required to prepare recovery plans in accordance with their obligations under the Civil Defence Emergency Management Act 2002. Currently these are at varying stages of preparation – some are well advanced. Though prepared for civil defence emergencies, most of each plan should still be applicable to domestic security incidents.



- 5.58 Stock-takes already in progress include:
- the Police establishing an ‘agency capability matrix’ that covers 15 different types of chemical and biological threats – selected for review because it is an area where capabilities and responsibilities are spread among a number of agencies;
  - a similar stock-take by DPMC for critical infrastructure – to identify and prioritise critical infrastructure across the country, so that better-quality decisions can be made on matters of security; and
  - what the MoH is doing as part of its influenza pandemic exercise (see Figure 9 on page 76).
- 5.59 In our view, the DPMC exercise could usefully be extended to take account of contingency planning in the event that critical infrastructure is severely damaged or destroyed.





# Appendices





## Appendix 1

## United Nations Security Council Resolution 1373

Adopted by the Security Council at its 4385<sup>th</sup> meeting, on 28 September 2001

*The Security Council,*

*Reaffirming* its resolutions 1269 (1999) of 19 October 1999 and 1368 (2001) of 12 September 2001,

*Reaffirming also* its unequivocal condemnation of the terrorist attacks which took place in New York, Washington, D.C. and Pennsylvania on 11 September 2001, and expressing its determination to prevent all such acts,

*Reaffirming further* that such acts, like any act of international terrorism, constitute a threat to international peace and security,

*Reaffirming* the inherent right of individual or collective self-defence as recognised by the Charter of the United Nations as reiterated in resolution 1368 (2001),

*Reaffirming* the need to combat by all means, in accordance with the Charter of the United Nations, threats to international peace and security caused by terrorist acts,

*Deeply concerned* by the increase, in various regions of the world, of acts of terrorism motivated by intolerance or extremism,

*Calling* on States to work together urgently to prevent and suppress terrorist acts, including through increased cooperation and full implementation of the relevant international conventions relating to terrorism,

*Recognizing* the need for States to complement international cooperation by taking additional measures to prevent and suppress, in their territories through all lawful means, the financing and preparation of any acts of terrorism,



*Reaffirming* the principle established by the General Assembly in its declaration of October 1970 (resolution 2625 (XXV)), and reiterated by the Security Council in its resolution 1189 (1998) of 13 August 1998, namely that every State has the duty to refrain from organizing, instigating, assisting or participating in terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts,

*Acting under Chapter VII of the Charter of the United Nations,*

1. *Decides* that all States shall:
  - (a) Prevent and suppress the financing of terrorist acts;
  - (b) Criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;
  - (c) Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;
  - (d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons;
2. *Decides also* that all States shall:
  - (a) Refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists;
  - (b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;

- (c) Deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens;
  - (d) Prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens;
  - (e) Ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts;
  - (f) Afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings;
  - (g) Prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents;
3. *Calls* upon all States to:
- (a) Find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups;
  - (b) Exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts;
  - (c) Cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts;
  - (d) Become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;

- (e) Increase cooperation and fully implement the relevant international conventions and protocols relating to terrorism and Security Council resolutions 1269 (1999) and 1368 (2001);
  - (f) Take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for the purpose of ensuring that the asylum-seeker has not planned, facilitated or participated in the commission of terrorist acts;
  - (g) Ensure, in conformity with international law, that refugee status is not abused by the perpetrators, organizers or facilitators of terrorist acts, and that claims of political motivation are not recognized as grounds for refusing requests for the extradition of alleged terrorists;
4. *Notes* with concern the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials, and in this regard *emphasizes* the need to enhance coordination of efforts on national, subregional, regional and international levels in order to strengthen a global response to this serious challenge and threat to international security;
  5. *Declares* that acts, methods, and practices of terrorism are contrary to the purposes and principles of the United Nations and that knowingly financing, planning and inciting terrorist acts are also contrary to the purposes and principles of the United Nations;
  6. *Decides* to establish, in accordance with rule 28 of its provisional rules of procedure, a Committee of the Security Council, consisting of all the members of the Council, to monitor implementation of this resolution, with the assistance of appropriate expertise, and *calls upon* all States to report to the Committee, no later than 90 days from the date of adoption of this resolution and thereafter according to a timetable to be proposed by the Committee, on the steps they have taken to implement this resolution;
  7. *Directs* the Committee to delineate its tasks, submit a work programme within 30 days of the adoption of this resolution, and to consider the support it requires, in consultation with the Secretary-General;
  8. *Expresses* its determination to take all necessary steps in order to ensure the full implementation of this resolution, in accordance with its responsibilities under the Charter;
  9. *Decides* to remain seized of this matter.

### Appendix 2

# List of International Anti-terrorist Conventions

## Terrorism involving aircraft

Convention on Offences and Certain Other Acts Committed on Board Aircraft (1963)

Convention for the Suppression of Unlawful Seizure of Aircraft (1970)

Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971) and its Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (1988)

## Terrorism involving ships

Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (1988)

Convention for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf (1988)

## Terrorist acts against persons

Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, including Diplomatic Agents (1973)

Convention against the Taking of Hostages (1979)

Convention on the Safety of United Nations and Associated Personnel (1994)



## **Terrorism conventions relating to the use of particular materials**

Convention on the Physical Protection of Nuclear Material (1980) – New Zealand is not a party to this convention

Convention on the Marking of Plastic Explosives for the Purpose of Detection (1991) – New Zealand is not a party to this convention

Convention for the Suppression of Terrorist Bombings (1997)

## **Financing terrorism**

Convention for the Suppression of the Financing of Terrorism (1999)



## Appendix 3

# Legislative Activity Since September 2001

Terrorism Suppression Act 2002<sup>30</sup>

Crimes Amendment Act 2003

Counter-Terrorism Bill

Telecommunications (Interception Capability) Bill

Border Security Bill

Maritime Security Bill

---

<sup>30</sup> Makes provision to implement New Zealand's obligations under the International Convention for the Suppression of Terrorist Bombings, the International Convention for the Suppression of the Financing of Terrorism and the Security Council's anti-terrorism Resolution 1373 (see Appendix 1).





## Appendix 4

## Additional Funding for Domestic Security After September 11, 2001

Following the September 11 attacks, the Government agreed to increase domestic security capabilities across a number of agencies. These increases were backed up by commitments to meet United Nations resolutions – in part achieved by the Terrorism Suppression Act 2002.

### Summarised on a Capability Basis

Note: All increases are calculated from existing 2001-02 baselines.

| (\$ million)                | 2001-02      | 2002-03       | 2003-04       | Total         |
|-----------------------------|--------------|---------------|---------------|---------------|
| <b>OPERATING</b>            |              |               |               |               |
| Improving Understanding     | 1.376        | 6.550         | 7.121         | 15.047        |
| International Relationships | -            | 0.805         | 1.030         | 1.835         |
| Protective Security         | -            | 4.152         | 5.512         | 9.664         |
| Operational Response        | -            | 0.185         | 0.185         | 0.370         |
| <b>Total</b>                | <b>1.376</b> | <b>11.692</b> | <b>13.848</b> | <b>26.916</b> |
| <b>CAPITAL</b>              |              |               |               |               |
| Improving Understanding     | 0.600        | 0.300         | -             | 0.900         |
| Operational Response        | 0.150        | 1.844         | -             | 1.994         |
| <b>Total</b>                | <b>0.750</b> | <b>2.144</b>  | <b>-</b>      | <b>2.894</b>  |



## APPENDIX 4

### Summarised on a Departmental Basis

Note: All increases are calculated from existing 2001-02 baselines.

| (\$ million)                                   | 2001-02      | 2002-03       | 2003-04       | Total         |
|--|--------------|---------------|---------------|---------------|
| <b>OPERATING</b>                               |              |               |               |               |
| Intelligence agencies<br>(EAB, GCSB and NZSIS) | 1.376        | 4.888         | 5.459         | 11.723        |
| Immigration                                    | -            | 2.062         | 2.062         | 4.124         |
| Customs  | -            | 3.010         | 3.010         | 6.020         |
| Police   | -            | 0.985         | 2.570         | 3.555         |
| NZDF   | -            | 0.185         | 0.185         | 0.370         |
| Parliamentary Service                          | -            | 0.562         | 0.562         | 1.124         |
| <b>Total</b>                                   | <b>1.376</b> | <b>11.692</b> | <b>13.848</b> | <b>26.916</b> |
| <b>CAPITAL</b>                                 |              |               |               |               |
| Intelligence agencies                          | 0.600        | 0.300         | -             | 0.900         |
| DIA (MCDEM)                                    | 0.150        | -             | -             | 0.150         |
| NZDF   | -            | 1.844         | -             | 1.844         |
| <b>Total</b>                                   | <b>0.750</b> | <b>2.144</b>  | <b>-</b>      | <b>2.894</b>  |

Background to the Cabinet Minute noted that:

- the approach being adopted is to propose counter-terrorism measures based on conceivable security risks and identified vulnerabilities, with a particular focus on preventing New Zealand being used as a safe haven to plan and facilitate terrorist attacks in other countries;
- a number of other counter-terrorism measures are already under way to address the links between international terrorism and trans-national organised crime, aviation security concerns, and effective controls on identity papers and travel documents; and that
- the Police and NZDF have implemented a system of security alert levels, and officials (DPMC lead) will investigate the wider application of the system to other government departments and agencies.



## Recent Publications by the Auditor-General

Other publications issued by the Auditor-General in the past 12 months have been:

- Annual Report 2002-03 – B.28
- Co-ordination and Collaboration in the Criminal Justice Sector
- Local Government: Results of the 2001-02 Audits – B.29[03b]
- Inland Revenue Department: Performance of Taxpayer Audit
- Management of Hospital-acquired Infection
- Central Government: Results of the 2001-02 Audits – B.29[03a]
- Disposal of 17 Kelly Street by Institute of Environmental Science and Research Limited
- ACT Parliamentary Party Wellington Out-of-Parliament Offices
- Annual Plan 2003-04 – B.28AP(03)
- New Zealand Defence Force: Deployment to East Timor –  
*Performance of the Health Support Services*
- New Zealand Defence Force: Deployment to East Timor –  
*Performance of the Helicopter Detachment*
- Department of Conservation: Administration of the Conservation Services Programme
- Certain Matters Arising from Allegations of Impropriety at Transend Worldwide Limited
- Management of Biosecurity Risks: Case Studies
- Ministry of Agriculture and Forestry: Management of Biosecurity Risks
- *All about ...* The Controller and Auditor-General

### Web Site

All these reports are available in PDF form on our web site [www.oag.govt.nz](http://www.oag.govt.nz). They can also be obtained in hard copy on request – [reports@oag.govt.nz](mailto:reports@oag.govt.nz). A cost may apply for hard copies.

### Subscription for Notification of New Reports

We offer a subscription facility for people to be notified by e-mail when new Reports and Latest News are added to the web site. The link to this subscription service is on our Home Page and also in the Reports section of the web site.



# Managing Threats to Domestic Security

---

**Controller and Auditor-General**

*Tumuaki o te Mana Arotake*

**ISBN 0-478-18109-4**