



Australian Government

# Protecting Australia Against Terrorism 2006



AUSTRALIA'S NATIONAL COUNTER-TERRORISM POLICY AND ARRANGEMENTS



**Australian Government**

## **Protecting Australia Against Terrorism 2006**



AUSTRALIA'S NATIONAL COUNTER-TERRORISM POLICY AND ARRANGEMENTS

© Commonwealth of Australia 2006

ISBN 0-9752387-9-5

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the *Copyright Act 1968*, all other rights are reserved.

Requests and inquiries concerning reproduction and rights should be addressed to Commonwealth Copyright Administration, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>.

Published by: The Department of the Prime Minister and Cabinet,  
National Circuit, Barton ACT 2600

**Internet website**

[www.pmc.gov.au](http://www.pmc.gov.au)

Edited by: Words@Work Editorial Services Pty Ltd

Designed and typeset by: ZOO, Canberra

Printed by: NCP, Canberra

# Contents

---

<b>Prime Minister's foreword</b>	<b>i</b>
<b>Executive summary</b>	<b>1</b>
<b>Part I: Australia's national strategy</b>	<b>7</b>
The terrorist threat	8
The nature of the terrorist threat	8
The significance of the terrorist threat to Australia	11
Australia's counter-terrorism strategy	12
Australia's counter-terrorism arrangements	13
Domestic counter-terrorism arrangements	13
International counter-terrorism arrangements	19
Engaging the Australian public	24
Engaging the private sector	29
<b>Part II: Australia's counter-terrorism capability</b>	<b>31</b>
Prevention and preparedness	32
Counter-terrorism legislation	32
Intelligence	37
Law enforcement	42
Critical infrastructure protection	45
Border security	48
Transport security	53
Identity security	59
e-security	60
Chemical, biological, radiological and nuclear security	62
Security-related science and technology research	65
Response and recovery	67
First response arrangements	68
Defence support	69
Public health	71
Recovery arrangements	73
The prepared and resilient community	75
Australia's future capability	77
<b>Acronyms</b>	<b>78</b>
<b>Index</b>	<b>79</b>



## Prime Minister's foreword

---



Five years have passed since the attacks on the World Trade Centre and the Pentagon on 11 September 2001. They introduced a new and confronting dimension to the international security environment. Today, terrorism remains a serious threat to Australia and our international partners and allies.

Terrorism requires us to maintain a clear strategic focus, underpinned by robust and sustainable capabilities. The Australian Government's response to terrorism has been decisive and wide-ranging. A total of \$8.3 billion in additional funding has been committed since 2001 to ensure that those agencies tasked with countering the terrorist threat have the resources they need to achieve their objective.

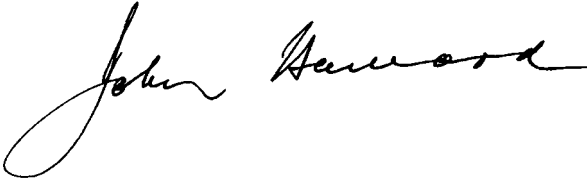
We are continually strengthening our counter-terrorism capabilities. Australia's enduring counter-terrorism aim is to protect Australians and Australian interests. The Australian Government seeks to achieve this aim by working with state, territory and local governments, the private sector and the community to build an effective, nation-wide counter-terrorism capability, and by contributing to regional and wider international efforts to counter terrorism.

Effective domestic action is essential in fighting terrorism, but terrorism knows no boundaries and no single country or government can combat the threat by acting alone. Australia's counter-terrorism strategy is therefore based on the close alignment of our domestic and international policies. Australia is pursuing a targeted bilateral, regional and global approach to enhance our national security.

Australia's counter-terrorism strategy provides the overall structure for the Australian Government's efforts to protect all Australians from terrorism. The government is aware that global efforts to counter terrorism have on occasion created pressures for Muslims, the overwhelming majority of whom do not subscribe to the radical ideology and actions promoted by the likes of Al Qaida and Jemaah Islamiyah. The government is committed to ensuring that its counter-terrorism policies, programmes and operations reflect the input and concerns of all Australians, including the Australian Muslim communities, and are not used by any individual or group as a pretext for targeting Australian Muslims or Islam itself. At the same time, it is the responsibility of every member of the Australian community to work with law enforcement and security agencies to prevent terrorism and to challenge those who threaten the peace and security of Australia.

This publication—*Protecting Australia Against Terrorism 2006*—updates and builds on the 2004 edition of *Protecting Australia Against Terrorism* to explain the Australian Government's counter-terrorism strategy, and outlines the key elements of Australia's domestic and international counter-terrorism policy and arrangements.

Despite our strong counter-terrorism capabilities, Australia cannot be complacent. The terrorist threat to Australia is very real and will be with us for some time. There can be no guarantees that we will always be able to prevent an act of terrorism. The Australian Government will continue to take resolute action, domestically and internationally, to advance our national interests, to counter the threat of terrorism and prevent those who seek to endanger the lives of Australian citizens.

A handwritten signature in black ink, reading "John Howard". The signature is fluid and cursive, with the first name "John" and the last name "Howard" clearly distinguishable.

John Howard  
*Prime Minister of Australia*

## Executive summary

---

The first responsibility of the Australian Government is to protect Australia, its people and interests. Five years on from the attacks of 11 September 2001 on the United States, terrorism remains a serious threat to Australia.

This publication updates the 2004 edition of *Protecting Australia Against Terrorism* and describes the Australian Government's counter-terrorism strategy. It:

- explains the steps the Australian Government has taken to protect Australians and Australian interests against the threat of terrorism
- outlines the government's partnership with state, territory and local governments as well as the private sector in developing the nation-wide counter-terrorism capability.

*Protecting Australia Against Terrorism 2006* comprises two parts. Part I describes Australia's national counter-terrorism strategy. It can be read by itself to gain a broad understanding of the strategy or in conjunction with Part II, which provides greater functional details about Australia's national counter-terrorism capabilities.

### PART I: AUSTRALIA'S NATIONAL STRATEGY

#### The terrorist threat

Terrorism remains a serious threat to Australia. In particular, the threat from Al Qaida, those who share its beliefs or are inspired by its ideology and example, and regional networks such as Jemaah Islamiyah, continues to evolve, adapting to the emergence of new technologies, opportunities and the counter-terrorism policies and operations of governments. Australia's counter-terrorism strategy will continue to evolve to address this threat.

#### Australia's counter-terrorism strategy

Australia's enduring national counter-terrorism aim is to protect Australians and Australian interests. The Australian Government seeks to achieve this by:

- working with state, territory and local governments, businesses and the community to build an effective nation-wide counter-terrorism capability
- contributing to regional and wider international counter-terrorism efforts.

The pursuit of these objectives is guided by four principles: constitutionality, proportionality, comprehensiveness and sustainability.

During the past five years, Australia has critically reviewed its national security arrangements and introduced a range of important measures and reforms. The Australian Government has committed \$8.3 billion in additional funds over the ten years from 2001 to support these reforms.

#### Australia's domestic and international counter-terrorism arrangements

The domestic and international aspects of Australia's counter-terrorism arrangements together form the government's strategic response to terrorism.



The Commonwealth, state and territory governments have established organisational arrangements and lines of reporting to effectively prevent, prepare for, respond to and recover from emergencies. Primary responsibility for the protection of life, property and the environment rests with the states and territories. They are typically the first responders in emergencies, including terrorist incidents, in their jurisdictions. The Commonwealth provides support to states and territories in times of emergency, as requested and appropriate to the nature of the threat. Emergency Management Australia is the lead Commonwealth agency involved in consequence management.

The National Counter-Terrorism Committee (NCTC) is a high-level committee of Commonwealth, state and territory officials, established by the Council of Australian Governments (COAG) to coordinate and advance the national counter-terrorism arrangements. The NCTC maintains the National Counter-Terrorism Plan, which outlines responsibilities, authorities and mechanisms to prevent acts of terrorism and manage their consequences within Australia.

Due to the global nature of the terrorist threat, Australia is constantly engaged beyond its borders in order to pursue common counter-terrorism goals with our partners and allies. Australia's Ambassador for Counter-Terrorism, based in the Department of Foreign Affairs and Trade, is responsible for the development and implementation of Australia's international counter-terrorism agenda.

Australia's international counter-terrorism arrangements aim to increase regional understanding of the nature of the terrorist threat; identify terrorists and deny them the operating conditions or environment to plan and execute terrorist attacks; disrupt terrorist networks; and strengthen the counter-terrorism capabilities of our international partners and allies.

Australia has cooperative relationships with authorities around the world, including in the United States of America, the United Kingdom, New Zealand, Canada, Japan, the European Union, and Middle Eastern and South-East Asian states. The Australian Government has also signed memoranda of understanding (MOUs) on counter-terrorism with several countries. The MOUs support practical, operational-level cooperation in every area of counter-terrorism capability.

### **Engaging the Australian public**

Australia's counter-terrorism strategy provides the overall structure for the Australian Government's efforts to protect all Australians, irrespective of creed, culture or religion, from terrorism. The government is committed to ensuring that its counter-terrorism policies, programmes and operations reflect the input and concerns of all Australians.

Well informed and engaged citizens are pivotal to Australia's counter-terrorism efforts. The National Security Public Information Campaign encourages the Australian public to remain vigilant and report anything suspicious to the National Security Hotline.

### **Engaging the private sector**

Australian businesses are key partners in Australia's national counter-terrorism strategy. The private sector owns and operates a great deal of the nation's critical infrastructure, including communications, transport and energy systems, banking and finance, national

food supply and utilities. The Australian Government actively engages the private sector in the development of long-term approaches that both protect Australia's economic interests and leverage business expertise and capabilities to help in countering terrorism.

## **PART II: AUSTRALIA'S COUNTER-TERRORISM CAPABILITIES**

The Australian Government employs a comprehensive approach to emergency management as the basis of its counter-terrorism arrangements. The four aspects of the comprehensive approach are prevention, preparedness, response and recovery.

### **Prevention and preparedness**

Prevention and preparedness cover the range of measures undertaken before a terrorist incident or attack. These measures include mitigation, deterrence and disruption of terrorist threats, and denial of the operating environment and conditions necessary for the preparation and execution of an attack.

#### ***Counter-terrorism legislation***

An effective counter-terrorism legal framework is fundamental to Australia's ability to address the terrorist threat. Since the 11 September 2001 terrorist attacks, the government has introduced a suite of new counter-terrorism legislation, including new terrorism offences and new powers for intelligence and law enforcement agencies. In 2005, the Commonwealth Parliament passed the *Anti-Terrorism Act (No. 2) 2005*. This amended the *Criminal Code Act 2005* to enable Australia to better deter and prevent potential acts of terrorism, and to more effectively prosecute where terrorist acts occur.

#### ***Intelligence***

Australia relies on intelligence to support its counter-terrorism strategy. The Australian Government is committed to ensuring that Australia's intelligence agencies have the expertise and resources to collect and analyse the information needed to combat terrorism. Since 2001, the government has committed more than \$2.5 billion in additional funding to bolster its intelligence gathering and assessment capability across the Australian intelligence community. As a result, the intelligence community today has a significantly enhanced capacity to collect and analyse information related to national security.

#### ***Law enforcement***

The Australian Government has significantly strengthened its law enforcement capabilities to undertake investigations into national crime and terrorist activity. The government's principal law enforcement agency, the Australian Federal Police (AFP), has expanded its practical cooperation with state and territory police and with overseas counterparts. Investigative capabilities and relations between federal, state and territory police have been strengthened through Joint Counter-Terrorism Teams.

#### ***Critical infrastructure protection***

The Australian Government works to coordinate a nationally consistent approach to critical infrastructure protection. The National Guidelines for Protecting Critical Infrastructure from Terrorism provide such an approach to help critical infrastructure

owners and operators protect their assets from terrorist attacks. The government has also established the Trusted Information Sharing Network for Critical Infrastructure Protection. The Network brings industry together through a range of sector-based groups to address key security issues. The Critical Infrastructure Protection Modelling and Analysis Programme is another important initiative that will analyse the dependencies and relationships between industry sectors. The Programme will help business and government develop better targeted security strategies and policies.

### ***Border security***

Australia's layered system of border control is regarded as world-class. The Australian Government has invested \$1.1 billion since 2001 to increase the robustness and efficiency of our border security regime. The government has strengthened Australia's national borders through major initiatives that include: a tighter legal framework and increased enforcement powers for the AFP, the Australian Customs Service and other Commonwealth agencies; enhanced immigration visa processing, information storage systems and airline liaison officer and overseas compliance networks; increased capacity to detect fraudulent documentation and the development and use of biometrics to detect identity fraud; bolstered security in the screening of air freight and sea-borne cargo; additional surveillance of seas to the north and northwest of Australia; and stronger cooperation with countries in our region.

### ***Transport security***

The Australian Government has introduced comprehensive new measures to counter potential threats to the security of Australia's domestic and international transport networks. Australian aviation and maritime security arrangements are being strengthened further. In response to the Wheeler Review of Airport Security and Policing in 2005, the government allocated significant additional resources to enhance its capability to identify, inspect and respond to high-risk export air cargo. The government also established AusCheck in the Attorney-General's Department to coordinate background checks on people who work in the secure areas of air and sea ports, namely, those who are required to have an Aviation Security Identification Card or Maritime Security Identification Card.

The Commonwealth, state and territory governments have agreed to a national, risk-based approach to enhancing the use of closed-circuit television (CCTV) for counter-terrorism purposes, including the development of a voluntary National Code of Practice for CCTV systems for the mass passenger transport sector.

### ***Identity security***

Identity security is central to Australia's national security, law enforcement and economic interests. The Australian Government announced the development of a National Identity Security Strategy (NISS) in 2005 to combat the misuse of stolen or assumed identities in the provision of government services. NISS aims to strengthen identity security through rigorous enrolment and authentication processes, while ensuring personal privacy. The identity of Australians will be further protected with the rollout of the national Document Verification Service.

### ***e-security***

Australia's capacity to participate in the global economy increasingly depends on information communications technologies. Our growing dependence on the information economy increases our vulnerability to acts of cyber-terrorism and other e-security threats. The government is committed to building a robust e-security policy framework to maintain a secure online environment that promotes trust and confidence in the information economy.

### ***Chemical, biological, radiological and nuclear (CBRN) security***

A national CBRN security strategy is being developed by the NCTC, to enhance the protection of Australians and Australian interests from CBRN terrorism threats, with the main focus being on domestic capabilities. The Australian Government is working with regional and international partners to ensure that CBRN materials do not fall into the hands of terrorist groups.

### ***Security-related science and technology research***

Australian Government agencies are increasingly harnessing science, engineering and technology capabilities to provide solutions to a wide range of national security threats. Australia's research community is developing a range of new technologies to address some key security challenges, including detection of explosives; protection of people and equipment in the event of an incident; forensic analysis; and critical infrastructure protection.

The Australian Government promotes collaboration on research on terrorism through the National Security Science and Technology Unit in the Department of the Prime Minister and Cabinet. The Unit supports a range of research projects with other agencies through its Research Support for Counter-Terrorism programme.

## **Response and recovery**

Response and recovery refer to the range of measures undertaken to address the consequences of a terrorist incident. Measures include first response; defence support; public health; recovery; and the prepared and resilient community.

### ***First response arrangements***

State and territory government agencies—particularly the police and emergency services—are responsible for the operational response to, and investigation of, terrorist incidents occurring in their jurisdictions. Commonwealth agencies provide support to the states and territories, as requested and appropriate to the nature of the incident. Emergency Management Australia is the lead Commonwealth agency involved in consequence management. It works closely with other Commonwealth agencies and state and territory police forces, fire and ambulance services, emergency services and public health authorities to ensure that appropriate consequence management arrangements are in place and supported.

### ***Defence support***

Defence delivers a range of capabilities to form part of a comprehensive, nation-wide approach to counter-terrorism. The cardinal principle governing Defence assistance in an emergency is to maintain and support the primacy of the civil authority in a domestic

security incident. Defence is enhancing command and control mechanisms to coordinate its domestic security functions.

### ***Public health***

State and territory governments are primarily responsible for delivering health services. State disaster planning assets like the National Trauma Centre at the Royal Darwin Hospital are critical to the national public health response capacity.

The Office of Health Protection, in the Department of Health and Ageing, provides national health infrastructure to support Australia's ability to respond to significant health threats, including terrorism. In the event of a health disaster the Australian Health Protection Committee will provide high-level, cross-jurisdictional collaboration in public health protection management planning, preparedness, response and recovery.

### ***Recovery arrangements***

The primary role for coordinating and planning recovery arrangements is based on the emergency management arrangements of state and territory governments and a series of less formal linkages between agencies and organisations with a role in recovery. The Australian Government effort is coordinated through the Australian Government Disaster Recovery Committee. The current arrangements are designed to respond quickly to the impacts of a disaster or crisis and long-term community recovery issues. These arrangements have proved effective; they are internationally recognised and draw on the experience of government and non-government organisations over many years.

### ***The prepared and resilient community***

Australia's emergency management approach is designed to ensure that the efforts of all relevant government agencies at all levels, organisations and affected communities can be coordinated effectively in the development of safer and more resilient communities. Local government and community organisations, with their understanding of local needs and capabilities, provide the basis for organising effective and immediately available community self-help. Commonwealth, state and territory governments are also working towards building the resilience of communities through a range of measures, such as better linkages between levels of government, and specific capabilities, such as a national emergency call centre.

### ***Australia's future capability***

Terrorism requires us to maintain a clear strategic focus, underpinned by robust and sustainable capabilities. The Australian Government has systematically reviewed the critical components of Australia's strategy to counter terrorism. A great deal has been done at all levels of government and by the private sector, the research community and the members of the Australian public to give effect to these priorities.

Australia cannot be complacent. As we prepare for the possibility of terrorist attacks today, we also continue to develop a strong and flexible national counter-terrorism framework into the future.

## Part I: Australia's national strategy



## THE TERRORIST THREAT

### The nature of the terrorist threat

Terrorism is not a new or static phenomenon. Over the past century, the world has seen a succession of terrorist acts and campaigns in support of various ideological or political causes. Methods of attack have evolved and terrorist actors—both state and non-state—have come and gone. This evolution will continue.

Five years on from the attacks of 11 September 2001 on the United States, terrorism remains a serious threat to Australia and Australia's interests overseas. In particular, the threat remains from Al Qaida and those who share its beliefs or are inspired by its ideology and example.

The terrorist threat is globally dispersed, constantly changing and evolving. Those involved are actively working to avoid detection. Typically, terrorist cells are small, difficult to penetrate and increasingly adept at concealing their activities and intentions from the authorities.

While the attacks of 11 September 2001 were the largest and most lethal to date, they are also part of a longer trend of successive terrorist attacks. Since 2001, major attacks have occurred in Mumbai, Karachi, Mombasa, Riyadh, Casablanca, Jakarta, Istanbul, Madrid, London and Amman. The Bali bombings of 2002 and 2005 together killed 222 people, including 92 Australians, and injured scores of others. Terrorists have also carried out many significant attacks in Iraq since 2003.

The persistence of terrorists and their capacity for strategic and innovative thinking was highlighted in the alleged plot to blow up multiple US-bound airplanes, which was disrupted by UK authorities in August 2006. Had the plot been successful, the human and economic costs would have been significant.

#### **Madrid 2004**

The attacks in Madrid in March 2004, using remote-control bombs on crowded commuter trains timed to detonate during the city's rush hour, killed 191 people and injured more than 2000. The bombers, young men legally residing in Spain, were inspired by Al Qaida's ideology, but appeared to operate without any direct participation or guidance from Al Qaida.

#### **London 2005**

On 7 July 2005, three suicide bombers detonated bombs on the London Underground, and a fourth detonated a device on the upper deck of a London bus in Tavistock Square. One Australian was among the 52 people killed. The bombings were the first successful Islamist terrorist attacks in the United Kingdom.

On 21 July 2005, a separate and apparently unconnected group tried unsuccessfully to conduct similar suicide attacks. Security agencies had come across two members of the 7 July group on the peripheries of other investigations, but none of the suicide bombers had been identified as potential terrorist threats. The extent to which the attacks were externally planned, directed or controlled remains unclear.

## ***Al Qaida***

Islamist terrorism has never depended on a single group or any formal organisation. There are linkages between the diverse array of terrorists and terrorist groups in the world but they do not form any single definable network. Decentralisation and adaptability are key characteristics of modern Islamist terrorism.

However, Al Qaida has been at the vanguard of global Islamist terrorism in both an operational and ideological capacity. At its narrowest, Al Qaida refers to the core group of terrorists who swore an oath of allegiance to Osama bin Laden, the founder and leader of Al Qaida. It has planned and undertaken attacks itself and funded, facilitated and directed attacks by others.

Al Qaida has also run a sophisticated global propaganda campaign and become an inspiration to Islamist terrorists operating outside its direct control. In 1998 Osama bin Laden issued the 'Declaration of the World Islamic Front for Jihad against the Jews and the Crusaders', signed by Al Qaida and four other terrorist groups. The declaration articulated that 'The ruling to kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the Al-Aqsa Mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim.' This advocacy of violent 'jihad' is viewed as a perversion of Islam by the overwhelming majority of Muslim people.

International counter-terrorism efforts have weakened Al Qaida. However, Al Qaida retains the capacity and intent to carry out major attacks. Its ideology has succeeded in persuading individuals to engage in terrorist acts, and in encouraging Muslim groups engaged in local insurgencies with nationalistic or ethnic dimensions to view their struggle in global, strategic terms. Many attacks have been mounted with limited, if any, financial or operational support or guidance from Al Qaida.

## ***The regional and international terrorist threat***

Countries in South-East Asia have made considerable progress in countering local terrorist groups, including by arresting or eliminating key leaders. The threat of further attacks, however, remains high.

Terrorists associated with Jemaah Islamiyah (JI)—the regional group responsible for the 2002 and 2005 Bali Bombings, as well as the 2004 bombing of the Australian Embassy in Jakarta—remain a great threat to Australians and Australian interests in our region. Under pressure from counter-terrorism operations, JI appears to have become more decentralised in its structure and operational planning. However, it remains resilient and dangerous. It retains links with Al Qaida, but is not dependent on it for either funding or operational support. JI also has links with other terrorist groups in South-East Asia, such as the Abu Sayyaf Group in the Philippines.

Terrorists have also shown themselves capable of effectively exploiting weak and failing states and conflict zones. In Afghanistan, which is a key international front in the global effort to counter terrorism, the removal of the Taliban regime was part of the broader objective of ensuring that the country does not again become a sanctuary for terrorism and a base for its export. The establishment of a democratically elected government in



Kabul was a significant step in meeting this objective, but the process of building stable governance continues for much of the country.

Iraq has become a key operating ground for groups affiliated with Al Qaida (most notably the group called Al Qaida in Iraq) and those inspired by its ideology and example. A major challenge is to counter terrorists who want Iraq to become the base for an expansion of the political and ideological influence of extremists in the Middle East and more broadly.

### **Bali 2005**

On 1 October 2005, three suicide bombers detonated explosive devices in Bali cafés, killing 20 people, including four Australians. Noordin Top, a key JI operative, claimed responsibility for the attacks.

Like the attacks in Bali in 2002, which killed 202 people, including 88 Australians, the 2005 Bali attacks were highly coordinated. Although a number of JI terrorists have been arrested in South-East Asia, JI and other groups continue to pose a serious threat in the region. Raids on JI safe houses following the Bali attacks pointed to preparations by JI to conduct more terrorist attacks.

### ***The ongoing terrorist threat***

The terrorist threat will likely be with us for some time to come. Al Qaida is still an active threat. Groups and individuals inspired by Al Qaida's ideology and example have been identified in many countries around the world, including Australia. Some of these groups and individuals have demonstrated a willingness to use violence in pursuit of their goals.

While most terrorist attacks are conducted using conventional explosives, including in suicide bombings, the attacks of 11 September 2001 demonstrated how creative and ruthless the attack planning of ideologically motivated terrorists can be. In this sense, the potential for terrorist use of chemical, biological, radiological or nuclear (CBRN) weapons generates particular concern. We know that terrorists are interested in CBRN weapons, but obtaining, producing, handling and disseminating such weapons is difficult.

State-sponsored terrorism, common throughout the 20th century, also remains a concern. Some states have, in pursuit of their strategic interests, supported terrorist groups. State sponsorship of terrorist groups can range from limited support, such as 'turning a blind eye' to a terrorist presence in a state's territory, to full support, including the provision of training facilities, weapons, logistics and even political support. Several state sponsors continue to harbour terrorist groups and we cannot exclude the possibility of future alliances between non-state and state-sponsored terrorists. Tactical and opportunistic cooperation between terrorists and other types of criminals will also continue to pose a security challenge.

## **The significance of the terrorist threat to Australia**

Even before 11 September 2001, targets in Australia—specifically Israeli interests and Jewish sites—were being considered by Al Qaida. Since 2001, public statements by Al Qaida’s leaders and other terrorists have singled out Australia for criticism and encouraged attacks against us. Fundamentally, Australia is identified by these terrorists as part of the West—and as such deemed a political, religious, military and cultural enemy. There have also been references to Australia’s alliance with the United States, our regional and global counter-terrorism efforts and our military commitments in East Timor, Afghanistan and Iraq.

While not capable of endangering the existence of the Australian state or greatly limiting its freedom of action, the terrorist threat to Australians and Australian interests is serious because terrorists are:

- in many cases expressly targeting Australians and Australian interests
- prepared to cause mass civilian casualties
- capable of attacks that could have long-lasting security, social and economic impacts for Australia.

History shows that the nature of the terrorist threat will continue to evolve over time, adapting to the emergence of new technologies, strategic opportunities and the counter-terrorism policies and operations of governments. We can expect to see continuing changes in terrorists’ area of operation, choice of targets, types of weapons, alliances, scale and timing of attacks and attack-related propaganda. We may also see the emergence of new terrorist actors with different goals and ideologies. Australia’s counter-terrorism strategy will continue to evolve to address this threat.

## AUSTRALIA'S COUNTER-TERRORISM STRATEGY

The critical challenge for government in responding to the terrorist threat is to ensure that our approach to national security is effective, while affirming and reinforcing the free and democratic nature of our society.

In the aftermath of the attacks of 11 September 2001, the Bali bombings of 2002 and 2005, and the London bombings of 2005, Australia critically reviewed its national security arrangements, ushering in a stream of important measures and reforms affecting the culture, structures and capabilities of our national counter-terrorism arrangements. The Australian Government has supported these reforms with a significant injection of additional financial resources—\$8.3 billion over ten years from 2001—for all agencies responsible for the delivery of the counter-terrorism agenda.

Australia's enduring national counter-terrorism aim is to protect Australians and Australian interests. The Australian Government seeks to achieve this by:

- working with state, territory and local governments, businesses and the community to build an effective nation-wide counter-terrorism capability
- contributing to regional and wider international counter-terrorism efforts.

The way in which the government pursues these objectives is guided by four principles:

- **Constitutionality:** Counter-terrorism policies and operations are bound by the Australian Constitution and Australian law.
- **Proportionality:** Australia's response is calibrated to the magnitude and nature of the threat.
- **Comprehensiveness:** Counter-terrorism policies address the prevention–preparedness–response–recovery aspects of emergency management and employ all necessary instruments and assets of national power.
- **Sustainability:** The counter-terrorism policy agenda has a long-term focus, consistent with the nature of the threat, and the agenda is underpinned by arrangements that are able to adapt to changes in the nature of the terrorist threat.



Department of the Prime Minister and Cabinet (AUSPIC)

## AUSTRALIA'S COUNTER-TERRORISM ARRANGEMENTS

Australia's counter-terrorism arrangements continue to evolve to address the terrorist threat in support of our national counter-terrorism aim and principles. The domestic and international aspects of these arrangements together form the government's strategic response to terrorism. The arrangements are based on a comprehensive approach to emergency management that recognises the need to prevent and prepare for and, if necessary, respond to and recover from terrorist attacks and their consequences. The four aspects of the comprehensive approach are:

- **Prevention:** to hinder, deter, mitigate and disrupt terrorist activity, while maintaining readiness to deal with a terrorist incident
- **Preparedness:** to protect our people, assets, infrastructure and institutions from terrorist activity and planning; and to establish, train for and exercise arrangements to respond to, and recover from a terrorist incident
- **Response:** to respond rapidly and decisively to a terrorist incident, should one occur, and manage its immediate consequences
- **Recovery:** to return national and community life to normal as quickly as possible after a terrorist incident, through the restoration of social, economic, physical and environmental wellbeing.

### Domestic counter-terrorism arrangements

#### *National security and Australian federalism*

Australia's counter-terrorism arrangements reflect the fact that Australia operates under a federal system that divides constitutional powers and responsibilities between two levels of government—the Commonwealth and the states and territories. A third level of government, local government, draws its constitutional powers and responsibilities from state and territory governments. Australia's domestic counter-terrorism arrangements support the following objectives:

- to increase national awareness of the terrorist threat
- to identify terrorists and deny them the operating conditions or environment to plan and execute terrorist attacks
- to strengthen Australia's counter-terrorism prevention, preparedness, response and recovery capabilities.

The Commonwealth, state and territory governments have established organisational arrangements and lines of reporting to effectively prevent, prepare for and, if necessary, respond to and recover from emergencies. Primary responsibility for the protection of life, property and the environment rests with the states and territories. They are typically the first responders in emergencies, including terrorist incidents, in their jurisdictions. Criminal law and procedure are also largely, but not entirely, constitutional responsibilities of the states and territories.

The Commonwealth, for its part, is uniquely placed to promote inter-jurisdictional consistency and coordination of counter-terrorism arrangements and to address counter-terrorism policy issues of national scope and importance. The Commonwealth

is committed to supporting states and territories in developing their capacity for dealing with emergencies, and provides physical and financial assistance to requesting states and territories in times of emergency. Given that the Commonwealth has exclusive constitutional responsibility for national defence, call-out of the military on Australian sovereign territory is an example of a measure that the Commonwealth can take, in appropriate circumstances, to assist states and territories. Defence call-out arrangements are governed by legislation and clear understandings between levels of government.

In addition to the military, the Commonwealth also has a number of key capabilities that support Australia's domestic counter-terrorism arrangements. These include capabilities in intelligence, law enforcement, border security, emergency management and foreign affairs.

Local governments also have specific responsibilities in emergencies, including terrorism, often directly legislated by state and territory governments. These responsibilities include contributing to a range of measures to manage risks to their communities, and in coordinating community resources and capabilities.

The National Counter-Terrorism Plan (NCTP), which outlines Australia's national counter-terrorism arrangements in some detail, recognises the joint responsibility of all levels of government in the maintenance of a national approach to counter-terrorism. This plan is regularly updated to reflect changes in national security structures, policies and processes, consistent with the evolving threat.

### ***Counter-terrorism coordination between Australian governments***

Two key overarching intergovernmental bodies provide an effective link between the Commonwealth, states and territories in respect of counter-terrorism. These are:

- the Council of Australian Governments (COAG)
- the National Counter-Terrorism Committee (NCTC).

COAG is Australia's principal intergovernmental policy forum. It is chaired by the Prime Minister, and includes the premiers and chief ministers of all states and territories, as well as the President of the Australian Local Government Association (ALGA). The role of COAG is to initiate, develop and monitor the implementation of policy initiatives that are of national significance—including security-related ones—and which require cooperative action by Australian governments.

On 27 September 2005, the Prime Minister chaired a special meeting of COAG at which a long-term national counter-terrorism agenda was agreed in response to the emerging threat environment, typified by the terrorist attacks in London in July 2005.

The NCTC is a high-level committee of officials established by an Inter-Governmental Agreement on national counter-terrorism arrangements in October 2002, to coordinate and advance the national counter-terrorism arrangements. It meets up to four times a year, and can also meet at short notice to consider urgent matters of national security, as it did following both the London and Bali attacks in 2005.

The NCTC is co-chaired by a Deputy Secretary of the Department of the Prime Minister and Cabinet and a senior state or territory official from the jurisdiction hosting the NCTC

meeting. Membership consists of senior officials from key Commonwealth departments and agencies, the premiers' and chief ministers' departments of the states and territories, as well as representatives of state and territory police. The New Zealand Department of the Prime Minister and Cabinet and the New Zealand Police also attend NCTC meetings as observers.

The NCTC is the central vehicle for counter-terrorism policy development and effective nation-wide operational coordination of initiatives and information in respect of counter-terrorism. The NCTC maintains the National Counter-Terrorism Plan (NCTP), which outlines responsibilities, authorities and mechanisms to prevent or manage acts of terrorism and their consequences within Australia. The NCTC reports annually to COAG.

### **COAG Special Meeting on Counter-Terrorism 27 September 2005<sup>1</sup>**

Following the 2005 London bombings a special meeting of COAG was called to consider Australia's national counter-terrorism arrangements. COAG agreed to:

- a National Emergency Protocol to ensure effective coordination and communication among jurisdictions in the event of an emergency of significant magnitude
- a national, risk-based approach to enhancing the use of closed-circuit television (CCTV) for counter-terrorism purposes, including the development of a National Code of Practice for CCTV systems for the mass passenger transport sector
- strengthened counter-terrorism laws at both the Commonwealth and state and territory levels, subject to appropriate safeguard against abuse
- implementation of the findings of the 2005 Wheeler Report on Aviation Security and Policing at Australian Airports, particularly in respect of the establishment of a single police command structure at Australian airports
- a national identity security strategy to enhance identification and verification processes and develop other measures to combat identity crime
- national standards for the private security industry, including review of security industry training, competence, accreditation, registration and licensing to identify variations in approaches and any response required
- refocused counter-terrorism exercises, including regular drill-style exercises in all major Australian cities, focusing on transport infrastructure and other places of mass gatherings, to provide greater exercising and training of Australia's ability to manage mass-casualty incidents
- a national strategy for promoting public understanding of the national counter-terrorism arrangements
- development of a national chemical, biological, radiological and nuclear (CBRN) security strategy
- a National Action Plan to build on the Principles agreed at the Prime Minister's meeting with Australian Islamic Community Leaders on 23 August 2005, which unanimously rejected terrorism in all its forms.

<sup>1</sup> Communiqué of meeting available at <http://www.coag.gov.au/meetings/270905/index.htm>

### ***Counter-terrorism coordination arrangements within the Australian Government***

The Australian Government's security arrangements are designed to advise and support the National Security Committee of Cabinet (NSC), the peak political decision-making body in the Australian Government on security-related policy, strategy and resources. Meetings are chaired by the Prime Minister. Other members include the Deputy Prime Minister, Treasurer, Minister for Defence, Minister for Foreign Affairs and the Attorney-General. Other ministers participate in the NSC when specific issues relevant to their portfolios are addressed.

Other key Australian Government committees include:

- the Secretaries' Committee on National Security, a senior officials' committee, chaired by the Secretary of the Department of the Prime Minister and Cabinet, which supports the NSC
- the Australian Government Counter-Terrorism Policy Committee, the key Commonwealth interdepartmental counter-terrorism strategic policy coordination and information-sharing forum in the Australian Government
- the Australian Government Counter-Terrorism Committee (AGCTC), an officials' committee responsible for the coordination of the Australian Government's role in operational aspects of the national counter-terrorism arrangements.

### ***Functional counter-terrorism coordination committees between Australian governments***

A number of intergovernmental committees coordinate with and, in a number of cases, report to the NCTC on aspects of their work that relate to counter-terrorism. These groups have representation from the Commonwealth, state and territory governments. They include:

- Australian Health Protection Committee, which facilitates inter-jurisdictional cooperation on, and response to, health disasters arising from either a natural or terrorist event
- National Committee for Critical Infrastructure Protection, which coordinates critical infrastructure protection policy development across all levels of government
- Australian Emergency Management Committee, the peak national consultative emergency management forum for Australian governments
- Transport Security Working Group, the key intergovernmental forum to advance transport security work with a view to improving security in Australia's transport system.

### ***A consistent and coordinated approach to national emergencies***

At its special meeting on counter-terrorism in September 2005, COAG noted the importance of a consistent and coordinated response by governments at the onset of any national emergency, and agreed to develop a protocol to ensure effective coordination and communication in the event of an emergency agreed to be of national significance.

The National Emergency Protocol describes the communication arrangements between the Prime Minister, premiers, chief ministers and the President of the ALGA during a

national emergency. The Protocol ensures that in the event of an emergency agreed to be of national significance:

- Australia's Commonwealth, state, territory and local government leaders can be contacted and are able to confer at all times
- leaders agree to coordinate key messages to the public.

The Protocol is an 'all hazards' overarching document that provides for the coordination of communications both between the leaders and with the public during an imminent or actual emergency of national significance, including terrorism.

### ***The national crisis arrangements and inter-governmental decision-making***

In the event of a terrorist incident, the Protective Security Coordination Centre (PSCC) within the Attorney-General's Department convenes a meeting of the AGCTC. The AGCTC includes representatives from a range of relevant Australian Government agencies, including the Department of the Prime Minister and Cabinet, the Attorney-General's Department, the Department of Defence, the Australian Security Intelligence Organisation, the Australian Federal Police, the Department of Foreign Affairs and Trade, the Department of Transport and Regional Services, the Department of Health and Ageing, Emergency Management Australia and others, depending on the nature of the incident. Similarly, strategic policy and operational response focused meetings engaging all relevant agencies are convened by affected states or territories under their own arrangements.

Should there be a terrorist incident on Australian sovereign territory, the Australian Government will consider, in consultation and agreement with states and territories, whether a National Terrorist Situation should be declared. Factors affecting such a declaration include:

- the scale and nature of the incident
- whether the incident is of a multi-jurisdictional character
- the impact of a threat involving civil aviation, maritime operations or critical infrastructure
- the possible involvement of foreign or international interests.

If a National Terrorist Situation is declared, overall responsibility for policy and broad strategy in relation to that situation transfers to the Australian Government, in close consultation with the affected states or territories. The National Terrorist Situation will apply to all jurisdictions.

### ***Information management and coordination***

Getting the right information to the right people at the right time is critical to achieving Australia's counter-terrorism goals. Information management and coordination is therefore a key driver of national counter-terrorism arrangements. The Australian Government has invested significant resources to set a standard of seamless, near real-time information-sharing and coordination across Commonwealth agencies and between jurisdictions. This has resulted in significant technological enhancements, procedural innovations and changes in interdepartmental culture.



The PSCC manages the Australian Government's protective security responsibilities and performs a coordination role in marshalling government resources to prevent or respond to threats to national security. It maintains close working relationships with all Commonwealth agencies, premiers' and chief ministers' departments, state and territory police services, and security agencies.

#### **Protective Security Coordination Centre Watch Office**

The PSCC Watch Office is the Australian Government's 24-hour-a-day, seven-days-a-week protective security and national security coordination centre. It supports the government's protective security arrangements, and coordinates information flows between the Commonwealth, state and territory governments on national security issues.

Under the NCTP, the PSCC Watch Office performs a critical coordination role in the national crisis management arrangements, which operate in the event a terrorist incident. The Watch Office also works closely with the National Security Hotline to ensure that time-critical information reported by the public is disseminated promptly to relevant agencies for immediate assessment and appropriate action. The Watch Office issues daily briefs and a weekly bulletin to a wide range of stakeholders.

#### ***National counter-terrorism exercise programme***

Australia's counter-terrorism arrangements are well practised and tested. Exercises involving simulated and hypothetical terrorist incidents, such as counter-terrorism exercise Mercury 05, are regularly conducted to verify and validate the response capabilities of key agencies to a range of threat scenarios. These exercises also test the effectiveness of coordination arrangements between the Commonwealth, states and territories.

Consistent with the agreement reached at the special COAG meeting of September 2005, the Australian Government allocated \$9.3 million over four years from 2006–07 to enable elements of the national counter-terrorism exercise programme to be refocused. This funding was in addition to the government's commitment of \$4 million over four years from 2004–05 and the provision of \$15.6 million over four years in the 2003–04 Budget.

To reflect lessons learned from previous terrorist attacks, including the attacks in Madrid in 2004 and London in 2005, the refocused elements of the exercise programme will include regular drill-style counter-terrorism exercises in all major Australian cities, concentrating on transport infrastructure and other places of mass gatherings, to provide greater exercising and training of Australia's ability to manage mass-casualty incidents. The programme will also involve, where appropriate, a broad range of government agencies, local government and the private sector.

### **Counter-terrorism exercise Mercury 05**

A major multi-jurisdictional counter-terrorism exercise, Mercury 05, was conducted in October 2005 to test national security arrangements for the Melbourne 2006 Commonwealth Games. Mercury 05 was the largest counter-terrorism exercise to be conducted within Australia to date, involving large-scale deployment activities and more than 4000 participants from Victoria, South Australia, Western Australia, New South Wales, the Australian Capital Territory and the Australian Government.

Mercury 05 was successful in testing the national counter-terrorism arrangements in terms of decision-making, coordination and interoperability across all levels of government, as well as security, law enforcement, intelligence, emergency management departments and agencies and private industry. The exercise also featured the involvement of the executive level of government, with issues considered by the Prime Minister, other members of the National Security Committee of Cabinet and premiers and chief ministers from participating states and territories.

### ***Special public events***

Hosting and attending major public events is an important part of the Australian way of life. Such events involve extensive security planning and coordination, including against possible terrorist attacks.

The work of our security agencies also extends to overseas events where large numbers of Australians are involved. While security measures put in place for such events are ultimately a matter for the host government, a range of Australian Government agencies have worked closely with their international counterparts to implement appropriate security arrangements for events such as Anzac Day at Gallipoli, the Bali Commemoration Services and the Interfaith Dialogue.

### **International counter-terrorism arrangements**

The government recognises that measures to build social cohesion and community harmony, and to empower those who may feel disaffected or marginalised, are an important part of the broader strategy to combat terrorism in Australia. Due to the global nature of the terrorist threat, Australia is constantly engaged beyond its borders in order to pursue common counter-terrorism goals with its partners and allies. Like the domestic arrangements, Australia's international counter-terrorism arrangements are whole-of-government in nature, involve numerous Australian Government agencies, and deploy a range of government instruments simultaneously—political, diplomatic, intelligence, law enforcement, immigration, finance, transport, development assistance and defence. Australia's international counter-terrorism arrangements support the following objectives:

- increase regional understanding of the nature of the terrorist threat
- identify terrorists and deny them the operating conditions or environment to plan and execute terrorist attacks
- disrupt terrorist networks
- strengthen the counter-terrorism prevention, preparedness, response and recovery capabilities of our international partners.

### *Practical cooperation in the region*

Australia is situated in a complex geopolitical environment. The archipelagic nature of a number of the region's countries, porous borders, religious sensitivities, differing perceptions of the terrorist threat and variable counter-terrorism capabilities across the region are major challenges to countering terrorism, as terrorists may seek to exploit these variations and differences.

In May 2006, the government announced its third successive cross-portfolio regional counter-terrorism package, totalling \$92.6 million over four years. A key element of that package involves working with regional partners to counter terrorist propaganda and challenge the violent ideology that has radicalised groups and individuals in the region.

Australia has developed particularly close and mutually beneficial counter-terrorism partnerships with Indonesia and the Philippines, including through counter-terrorism capacity-building activities. Indonesia is a critical partner in tackling the terrorist threat in our region. The region's most potent terrorist group, Jemaah Islamiyah, which has links across South-East Asia, has historical roots in Indonesia. As a result, our security cooperation with Indonesia is deep and multidimensional, involving many Australian and Indonesian Government agencies. It has yielded many successes.

Australia and the Philippines are also working together to advance our common counter-terrorism objectives, particularly through the mutual sharing of expertise and experience. The Southern Philippines has been a focal point for terrorist activity in South-East Asia and the potential development of cooperative relationships between international and local terrorist and insurgency groups—notably the Abu Sayyaf Group and the Moro Islamic Liberation Front. Australia will continue to engage the Philippines on a whole-of-government basis, seeking to counter these groups.

Australia's national security could also be directly affected by criminal exploitation of small states in the South Pacific. Many Pacific island countries are characterised by periodic instability, porous borders and variable counter-terrorism capabilities. They are vulnerable to the transnational trafficking of drugs, arms and people. Money laundering is also a large risk, although this is now being managed through a wholly new level of technical assistance delivered by Australia's Anti-Money Laundering Assistance Team working collaboratively with the new Pacific Anti-Money Laundering Programme funded by the United States Government. The vulnerabilities of the Pacific region and the potential nexus of such vulnerabilities with terrorism make Pacific island countries important allies in Australia's counter-terrorism efforts. On both a bilateral basis and through regional groupings like the Pacific Islands Forum, Australia continues to work with Pacific island countries to improve governance structures and capabilities in order to manage the security challenges.

Australian Federal Police



### **Regional counter-terrorism capacity-building assistance**

The Australian Government places great importance on helping countries in our region to develop robust counter-terrorist capabilities in areas such as legislation, law enforcement, border control, transport security, intelligence, finance regulation, emergency management and defence.

Since 2004, the Australian Government has provided more than \$354 million in regional counter-terrorism capacity-building assistance. For example, the government is contributing funds to the Jakarta Centre for Law Enforcement Cooperation, building on the close cooperation between Australian and Indonesian law enforcement agencies in the wake of the Bali bombings. This international education and training institution, opened in July 2004, is greatly increasing the ability of regional law enforcement agencies to respond to the complex challenges posed by terrorism in our region.

The 2006–07 Budget committed an additional \$92.6 million over four years to help boost the capacity of regional countries to combat the terrorist threat. The new measures will build on existing regional cooperation in law enforcement, intelligence, transport security and border control funded by cross-portfolio regional counter-terrorism packages from the 2004–05 and 2005–06 Budgets. They will also expand regional cooperation to keep weapons of mass destruction out of the hands of terrorists; make it more difficult for terrorists to travel to train and operate; build regional capability for responding to terrorist attacks; and promote tolerance and counteract terrorist propaganda.

The government has also established the Counter-Terrorism Intelligence Training Programme within ASIO. The programme coordinates Australian intelligence training and enhances cooperation in the region.

### ***Wider international cooperation***

Australia's enduring alliance with the United States is a key pillar of Australian security in general and our international counter-terrorism arrangements in particular. Afghanistan and Iraq are two theatres where our mutual security interests are being defended. The United States brings vast resources and commitment to countering the terrorist threat. Australia shares this commitment and also brings resources and excellence in specific strategic and operational capabilities, particularly in our region of the world.

We have cooperative relationships with authorities around the world, including in the United Kingdom, New Zealand, Canada, Japan, the European Union, and Middle Eastern and South-East Asian states. Australia is also working alongside security alliances such as the North Atlantic Treaty Organisation (NATO).

In 2002, Australia, the United States and Japan established the Trilateral Strategic Dialogue, which aims to promote peace and stability in the Asia-Pacific region. In 2005, the Dialogue launched a process of trilateral multi-agency counter-terrorism consultations with the aim of improving strategic coordination of counter-terrorism activities in South-East Asia.

To date, the Australian Government has signed memoranda of understanding (MOUs) on counter-terrorism with the following countries: Malaysia, Thailand, the Philippines, Fiji, Cambodia, Papua New Guinea, Indonesia, India, East Timor, Brunei, Pakistan and Afghanistan. This network of bilateral MOUs supports practical, operational-level cooperation in every area of counter-terrorism capability, including legislative capacity, law enforcement, terrorist financing and money laundering, border control, transport security, emergency response and defence cooperation.

### ***Multilateral efforts***

Australia participates in multilateral fora directed at combating global terrorism, including the United Nations, the Asia-Pacific Economic Cooperation Counter-Terrorism Task Force, the Association of South-East Asian Nations Regional Forum and the Pacific Islands Forum. The Australia Group, chaired by Australia since 1985, also plays an important role in international efforts to prevent countries of concern or terrorists from acquiring chemical and biological weapons.

### ***Coordination of international counter-terrorism policy agenda***

Australia has a dedicated Ambassador for Counter-Terrorism, responsible for the development and implementation of Australia's international counter-terrorism agenda. The Ambassador, who is based in the Department of Foreign Affairs and Trade, has a key role in ensuring a coherent and effective approach to Australia's counter-terrorism cooperation with both regional and global partners. This entails identifying needs and opportunities for practical action to counter the terrorist threat, and maximising Australia's capacity to respond internationally to this threat. As chair of the Australian Government's International Counter-Terrorism Coordination Group, the Ambassador works closely with a range of Australian Government agencies to contribute to international counter-terrorism efforts.

### ***Pivotal Australian Defence Force Missions***

The Australian Defence Force (ADF) is an important asset for the protection of Australians and Australian interests against the terrorist threat within Australia, in our region and globally. The ADF has been particularly active in protecting Australia's strategic interests in our region, and in Afghanistan and Iraq.



### **Afghanistan**

In September 2005, a Special Forces Task Group of about 190 personnel was deployed for 12 months to support the reconstruction and stabilisation of Afghanistan by providing combat patrols in remote regions, and reconnaissance and surveillance operations with coalition partners. In addition, in August 2006 the government deployed a Reconstruction Task Force consisting of approximately 400 ADF personnel as part of a Netherlands-led Provincial Reconstruction Team. The ADF contribution will be a mixed security and reconstruction task force to work on reconstruction and community-based projects to assist Afghanistan to achieve a stable and secure future.

### **Iraq**

The security and stability of the Middle East are fundamental to global security, and are inextricably linked to Australia's strategic interests. Allowing terrorists, insurgents and former regime elements to gain the upper hand in Iraq would be a major setback for Iraq and the Middle East. Australia's commitment to Iraq includes a Task Group to southern Iraq to provide support to the new Iraqi army.

### ***Countering radicalisation***

Much has been done in recent years to disrupt transnational terrorist networks, prevent terrorist attacks, apprehend those involved and bring them to justice. This work will remain at the forefront of Australia's counter-terrorism efforts in the coming years as we tackle the complex and evolving terrorist challenge.

However, over the medium to long term, Australia and its allies and partners will increasingly need to counter the spread of the ideology that underpins violent extremism, and promote tolerance and pluralism. In May 2006, the Australian Government announced the third successive cross-portfolio regional counter-terrorism package totalling \$92.6 million over four years. A key element of that package is working with regional partners to counter terrorist propaganda and challenge and contest violent ideology that has radicalised groups and individuals.

## ENGAGING THE AUSTRALIAN PUBLIC

Well informed and engaged citizens are pivotal to Australia's counter-terrorism efforts. The government is committed to keeping the public informed on key counter-terrorism issues and to ensuring that public information is used effectively to counter terrorism. Over time, public engagement provides a critical basis for sustained public confidence in our national counter-terrorism arrangements.

### ***National Security Public Information Guidelines***

The Commonwealth, state and territory governments have a coordinated information-sharing and public communications network. This network is governed by the National Security Public Information Guidelines, which seek to ensure that all government agencies with national security responsibilities work to:

- improve the public's understanding of Australia's national security organisations and systems
- generate public confidence in Australia's ability to respond to any terrorist threat or activity
- create public trust that the government will release all information possible, subject to specific operational and security considerations.

### ***National Security Public Information Campaign***

The National Security Public Information Campaign encourages the Australian public to remain vigilant and report possible signs of terrorist activity to the National Security Hotline.

The first phase of the campaign, Let's Look Out for Australia, was launched in December 2002. It used television, radio and press advertising to give the public information on what the Australian Government was doing to protect Australia against terrorism. The campaign also involved the distribution of the *Let's look out for Australia* booklet to 7.8 million Australian households.

The second phase of the campaign, Every Piece of Information Helps, was launched in September 2004 to remind Australians to remain vigilant and continue calling the National Security Hotline. The campaign used television, press, transit and outdoor advertising. Campaign advertising recommenced following the terrorist attacks in London in July 2005, and continued through to March 2006.

### ***National counter-terrorism alert levels***

The national counter-terrorism alert level guides national preparedness and planning and dictates levels of precaution and vigilance to minimise the risk of a terrorist incident occurring. It is also the basis of public discussion on the risk of the terrorist threat to Australia. The four national counter-terrorism levels of alert are:

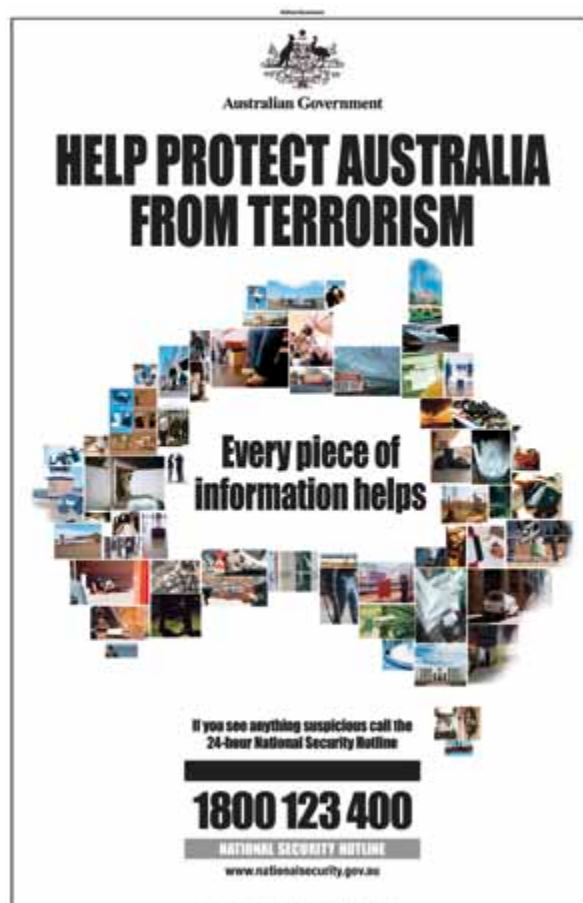
- low—a terrorist attack is not expected
- medium—a terrorist attack could occur
- high—a terrorist attack is likely
- extreme—a terrorist attack is imminent or has occurred.



### **National Security Hotline**

The National Security Hotline commenced operations on 27 December 2002, providing a new and innovative capability for the public to pass information potentially relevant to countering terrorism. It is now an indispensable part of Australia's counter-terrorism arrangements.

The Hotline operates 24 hours a day, seven days a week, allowing members of the public to report any suspicious or unusual activity or behaviour. Information provided to the Hotline is passed on to relevant police and security agencies. The Hotline has received more than 80 000 calls, letters and emails from alert members of the public.



Anything suspicious can be reported to the Hotline on 1800 123 400 or by email to [hotline@nationalsecurity.gov.au](mailto:hotline@nationalsecurity.gov.au). All information received remains confidential and callers can remain anonymous. Strong checks and vetting processes are in place to ensure that the Hotline is not misused for denunciation of, or attacks on, individuals.

At the time of writing (November 2006), the national counter-terrorism alert level is at medium, where it has been since 12 September 2001. Should any information come to light that caused the government, acting on expert advice, to change the alert level, the public would be advised without delay. Information about the alert level is available at [www.nationalsecurity.gov.au](http://www.nationalsecurity.gov.au). The government is able to advise an increased security concern without raising the national alert level.

### ***Overseas travel advisories***

The Australian Government monitors security conditions overseas to provide up-to-date advice to the Australian public about credible threats against Australians and their interests globally. The government's travel advice is key to protecting Australians abroad. It enables Australian travellers to make well informed judgements about the safety and security conditions of their travel destinations.



When the government receives intelligence information about terrorist and related security information that could endanger Australians overseas, it assesses and translates that information into appropriate travel advice. Rigorous processes are in place to ensure consistency between intelligence assessments and travel advice. There is close liaison and consultation between the Department of Foreign Affairs and Trade and the Australian Security Intelligence Organisation (ASIO) on new overseas threat information. The government also maintains a general advice service for Australian travellers that addresses global terrorist risks at destinations not covered by specific travel advice. Based on this information, an Australian traveller can take appropriate measures to minimise risks, ranging from simple personal safety precautions to deferring or cancelling travel plans.

All Australians overseas are encouraged to subscribe to destination-specific travel advice at [www.smartraveller.gov.au](http://www.smartraveller.gov.au) and register their presence abroad with the Department of Foreign Affairs and Trade. Registration is available online at [www.orao.dfat.gov.au](http://www.orao.dfat.gov.au). The online registration process also provides the government with critical information for contingency planning and allows the government to contact Australians overseas in the event of an emergency.

### ***Engaging Australia's Muslim communities***

Australia's counter-terrorism strategy provides the overall structure for the Australian Government's efforts to protect all Australians from terrorism, irrespective of creed, culture or religion.

The government recognises that measures to build social cohesion and community harmony, and to empower those who may feel disaffected or marginalised, are an important part of the broader strategy to combat terrorism in Australia. Global efforts to counter terrorism have, on occasion, created pressures for Muslims, the overwhelming majority of whom do not subscribe to the radical ideology and actions promoted by the likes of Al Qaida and affiliated or sympathetic groups and individuals. The government is committed to ensuring that its counter-terrorism policies, programmes and operations reflect the input and concerns of the Australian community, and are not used by any individual or group as a pretext for targeting Australian Muslims or Islam itself.

### ***Prime Minister's meeting with leaders of Australia's Muslim Communities***

Following the terrorist attacks in London in 2005, the Prime Minister met with leaders of Australia's Muslim communities on 23 August 2005. The meeting issued a 'Statement of Principles' that commits all Australians to work together to protect Australia from extremism and promote tolerance, harmony and understanding. It was also agreed that the Commonwealth would seek the cooperation of the state and territory governments in working towards a national strategy to reinforce social cohesion and combat extremism.

***Prime Minister's meeting with leaders of Australian Muslim communities:  
Statement of Principles***

The Prime Minister met with leaders of Australia's Muslim communities on 23 August 2005. They agreed on the following Statement of Principles.

An overriding loyalty to Australia and a commitment to its traditions, values and institutions are the common bonds that unite us all. In confronting the challenges of terrorism, we agree that:

1. All Australians are subject to the laws of this country and in turn are entitled to equal protection under those laws.
2. All Australians should respect and participate in the democratic institutions and practices of this country.
3. All Australians unconditionally reject and denounce all forms of violence or terrorism and acts or language which promote hatred, violence or terrorism. Such behaviour has no role in advancing the political or religious objectives of any group and is contrary to the values embraced by all Australians.
4. Violence and acts of terrorism committed in the name of Islam are a perversion of the Muslim faith.
5. Acts of terrorism are repugnant to all Australians irrespective of their race or religion, and all Australians must work together to ensure that everything is done to prevent the scourge of terrorism from coming to Australia.
6. Members of the Muslim faith, and in particular its leaders, have a responsibility to challenge and counteract those who seek to encourage the use of violence and terrorism in the name of Islam. The Government must support and encourage Islamic leaders to challenge and eradicate extremism.
7. We commit ourselves to work together with all Australians to produce positive outcomes which protect Australia against violence, terrorism and intolerance and promote our common goals of harmony and understanding.

We together have agreed that:

- Our discussions today represented an important exchange of ideas between the Australian Government and the Islamic community that should continue.
- The Australian Government will seek the cooperation of the governments of the states and territories in working toward a national strategy to address intolerance and the promotion of violence.
- Those present will continue to take a lead in working with their communities and with other Islamic organisations to promote harmony, mutual understanding and Australian values within their communities and to challenge violence and extremism.
- The Australian Government will ensure that its programmes and policies enhance mutual understanding between the Islamic community and the broader Australian community, and promote the Australian values of harmony, justice and democracy.

In September 2005, the Muslim Community Reference Group was established for a one-year term to advise the government on Muslim community issues. The government is currently considering future models for dialogue with the Muslim community. Community input has been a key aspect of the development of the National Action Plan.

### ***National Action Plan***

At its special meeting on counter-terrorism in September 2005, the Council of Australian Governments (COAG) requested that the Ministerial Council on Immigration and Multicultural Affairs develop a National Action Plan for Commonwealth, state and territory governments, built upon the 'Statement of Principles' agreed at the Prime Minister's meeting with leaders of Australia's Muslim communities and at meetings between state and territory faith leaders.

The National Action Plan is a whole-of-government initiative being coordinated by the Department of Immigration and Multicultural Affairs (DIMA). It builds on existing cultural diversity policies and programmes at all levels of government, incorporates research findings from Australian and overseas studies, and is informed by community input.

On 16 July 2006, the government announced a \$35 million package including a range of initiatives to implement the National Action Plan. These initiatives focus on:

- programmes, including pilots, involving:
  - a new values-based education initiative
  - employment coordinators
  - employment workshops for young job seekers
  - a sporting programme to increase the participation of children in local sporting clubs
  - a mentoring programme to increase participation of young people in work, education, training and community life.

In the first instance, the pilots will be conducted in Lakemba and Macquarie Fields in New South Wales.

- the creation of a centre of research and educational excellence in Islamic studies within a major Australian university, to play a leadership role in exploring the place of Islam in modern society
- Interfaith dialogue projects
- a volunteer-staffed counselling and support helpline for the Muslim communities based on a successful UK project
- specialist training, educational materials and forums to bring law enforcement agencies and Muslim communities together to resolve issues
- crisis management training to help empower the Muslim communities to plan for and respond to issues, incidents and crises.

## ENGAGING THE PRIVATE SECTOR

Australian businesses are both key partners in Australia's national counter-terrorism strategy and potential targets of terrorism. The principal means by which terrorists may target or adversely affect Australian business are:

- a direct attack, possibly because of the profile, symbolism or economic status of the business or industry in question
- indirect impacts caused by a terrorist attack that affects critical infrastructure or related business concerns, such as producers, suppliers or customers, or that affects consumer confidence in the economy.

Recent terrorist attacks have demonstrated the continued terrorist threat to critical infrastructure, in particular, transport infrastructure. The targeting of public transport systems in Madrid, London and Mumbai was consistent with the aim of terrorists to cause mass casualties.

In some parts of Australia, a great deal of critical infrastructure is privately owned or operated on a commercial basis. Critical infrastructure extends across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, the food supply and communications. It also includes key government services, including emergency services and supply chains that operate through a complex network of producers, processors, manufacturers, distributors and retailers—for example, the food supply chain.

The Australian Government therefore actively engages the private sector in the development of long-term approaches that both protect Australia's economic interests and leverage business expertise and capabilities to help counter the terrorist threat.

### *Role of the Australian Government*

The Australian Government does not dictate to businesses what security measures they should take, except in a few specific sectors. Most business security decisions are best made by individual businesses, taking into account their own circumstances and levels of risk.

The government has a key role in providing businesses with the information, knowledge and tools they need to understand the security environment, and to make informed decisions that meet their specific security needs and objectives. To this end, the government is consulting with businesses through several mechanisms. These reinforce the importance of security considerations in business planning, and provide businesses with the latest security information and advice. For example:

- The Business Government Advisory Group on National Security brings together senior ministers of the Australian Government and the Chief Executive Officers of Australia's major corporations to discuss security issues. The advisory group offers the business community the opportunity to provide input into the strategic direction of Australian Government policies in relation to national security.

- To enhance critical infrastructure protection, the government is working closely with the owners and operators of critical infrastructure through initiatives such as the Trusted Information Sharing Network for Critical Infrastructure Protection. The Australian Security Intelligence Organisation (ASIO) produces threat assessments for specific events, facilities, sectors and critical infrastructure, in consultation with government departments and agencies and the private sector. These assessments fall into two broad categories: those that assist preparedness and planning; and those that deal with a specific threat or a heightened assessment of threat.
- ASIO established a Business Liaison Unit in late 2005 to provide an interface between business and the Australian intelligence community. The Unit provides advice on possible threats to specific industry sectors and other national security issues.
- The National Security website provides advice and information on security issues for business at [www.nationalsecurity.gov.au](http://www.nationalsecurity.gov.au).

The government has established a genuine partnership with the private sector in the interest of countering terrorism. The combined knowledge, expertise and resources of Australia's governments and the private sector provide Australia with a robust capability to counter terrorism.

## Part II: Australia's counter-terrorism capability



## PREVENTION AND PREPAREDNESS

The Australian Government employs a comprehensive approach to emergency management as the basis of its counter-terrorism arrangements. The four aspects of the comprehensive approach are prevention, preparedness, response and recovery.

Prevention and preparedness refer to the range of measures undertaken before a terrorist incident or attack. These measures include mitigation, deterrence and disruption of terrorist threats and strategic and tactical denial—that is, denying terrorists the operating environment and conditions necessary for the preparation and execution of an attack. In the event of a terrorist incident or successful terrorist attack against Australian interests, activities undertaken in the prevention and preparedness phases will bolster the national capability to respond and recover.

Prevention and preparedness cover the following areas of counter-terrorism activity:

- counter-terrorism legislation
- intelligence
- law enforcement
- critical infrastructure protection
- border security
- transport security
- identity security
- e-security
- chemical, biological, radiological and nuclear security
- security-related science and technology research.

### Counter-terrorism legislation

An effective counter-terrorism legal framework is fundamental to Australia's ability to address the terrorist threat. This framework is not static. It is adapted as the terrorist threat evolves to ensure that it remains effective.

The Australian Constitution does not give the Commonwealth explicit power to make laws in respect of terrorism. The Commonwealth and states and territories must work cooperatively to maintain a national legal regime. The establishment of comprehensive terrorism offences at the Commonwealth level was made possible by a reference of legislative powers to the Commonwealth by the states and territories.

Following the 11 September 2001 terrorist attacks on the United States, the Australian Government, for the first time in Australian history, introduced comprehensive counter-terrorism legislation to address the emerging security environment. The suite of counter-terrorism legislation passed in 2002 defined terrorism and introduced new terrorism offences targeting anyone who engages in, trains for, prepares, plans, finances or otherwise supports terrorist activities. This and subsequent legislation created terrorism and terrorist organisations offences, terrorist bombing offences, offences

against Australians overseas, questioning and detention powers for the Australian Security Intelligence Organisation (ASIO), border protection, maritime security and aviation security.

### **Australia's legal definition of terrorism\***

The Criminal Code defines a terrorist act as an action or threat of action that causes serious physical harm or death to a person, or endangers a person's life or involves serious risk to public health or safety, serious damage to property or serious interference with essential electronic systems.

In addition, the action or threat of action must be intended to advance a political, ideological or religious cause and to coerce or influence by intimidation an Australian or foreign government or intimidate any section of the public of any country.

\*For the full definition, please see Section 100.1 of the *Commonwealth Criminal Code Act 1995*.

In the aftermath of the terrorist attacks in London in July 2005, the Council of Australian Governments (COAG) held a special meeting on counter-terrorism in September 2005. COAG agreed that there was a clear case for further strengthening Australia's counter-terrorism laws, subject to strong safeguards, to better protect Australians and Australian interests.

Premiers and chief ministers also agreed to enact legislation to give effect to measures that the Commonwealth could not otherwise enact because of constitutional constraints, including preventative detention for up to 14 days, and stop, question and search powers in areas such as transport hubs and places of mass gatherings.

In 2005, the Commonwealth Parliament passed the *Anti-Terrorism Act (No. 2) 2005*.<sup>2</sup> This amended the *Criminal Code Act 1995* to enable Australia to better deter and prevent potential acts of terrorism, and to more effectively prosecute where these occur. New measures include:

- control orders for up to 12 months and preventative detention for up to 48 hours to restrict the movement of those who pose a terrorist risk to the community
- new offences that apply where a person intentionally urges another person to use force or violence to overthrow, interfere with or threaten the peace, order and good government of the Commonwealth, or assist an enemy at war with the Commonwealth
- a new regime for stop, question, search and seize powers at airports and other Commonwealth places.

<sup>2</sup> The *Anti-Terrorism Act (No. 1) 2005* introduced an interpretative amendment to Commonwealth terrorism offences to ensure that the policy of the existing offences is implemented in the way it was originally intended. The amendment clarified that, when proving that someone is intending to commit a terrorist act, it is not necessary for the prosecution to identify intention to commit a *specific* act of terrorism.



### **Commonwealth control orders**

The Australian Federal Police (AFP) may, with the consent of the Commonwealth Attorney-General, apply to a court for control orders for up to 12 months for individuals who pose a terrorist risk to the community. Control orders are similar to apprehended violence orders, but allow stricter conditions to be imposed on an individual. A court may approve a control order application if it is satisfied that, on the balance of probabilities:

- the issuing of a control order would substantially assist in preventing a terrorist act, or
- an individual has provided training to, or received training from, a listed terrorist organisation, and
- each of the control mechanisms in the order is reasonably necessary, and reasonably appropriate and adapted for the purpose of protecting the public from a terrorist act.

A control order can prohibit or restrict the individual:

- being at specified areas or places or leaving Australia
- communicating or associating with other specified individuals
- accessing or using specified forms of telecommunication or other technology
- possessing or using specified articles or substances
- carrying out specified activities, including in respect of his or her work or occupation.

Orders can last for up to 12 months. The AFP or the individual who is the subject of the order may seek to revoke or vary the order.

### ***Safeguards***

Initially, an interim control order is made. The subject of the order may attend court and make representations on their behalf when the court decides to confirm, vary or revoke the order. The subject can apply for the order to be varied or revoked as soon as the subject is notified that an order is confirmed. Normal judicial review processes would apply to decisions to issue or revoke control orders. The subject and their lawyer are able to obtain a copy of the order containing the summary of the grounds for the order.

Control orders will not apply to people under the age of 16, and will apply in a modified way to people between the ages of 16 and 18.

Each year, the Attorney-General will report to Parliament on the operation of control orders.

The provisions will be reviewed by COAG after 5 years and will sunset after 10 years.

### **Commonwealth preventative detentions**

The Commonwealth preventative detention regime provides for detention for up to 48 hours in a terrorism situation. Complementary state and territory legislation allows for preventive detention of up to 14 days.

The AFP must have reasonable grounds to suspect that the subject:

- will engage in a terrorist act
- possesses a thing that is connected with the preparation for, or engagement of an individual in a terrorist act or
- has done an act in preparation for, or in planning for a terrorist act.

The AFP must also be satisfied that making the order for preventative detention will:

- substantially assist in preventing a terrorist attack, and that detaining the individual is reasonably necessary to do so, or
- preserve evidence, where a terrorist act has occurred, and that detaining the individual is reasonably necessary to do so.

A prohibited contact order can also be made to limit whom an individual can contact when they are in detention. A detained individual cannot be questioned except to confirm his or her identity or to enable safe detention. If the police intend to formally question a detained individual about an offence, they are required to release the individual from preventative detention, and then arrest that individual and use the detention for questioning powers under the *Crimes Act 1914*.

### ***Safeguards***

Any preventative detention order, as well as the treatment of the detained individual, is subject to judicial review. It can also be subject to investigation by the Commonwealth Ombudsman, and merits review by the Administrative Appeals Tribunal. Treatment of the detained individual is also legally required to be consistent with international human rights norms.

In considering an extension of the initial preventative detention order, the issuing authority must consider afresh the making of the order and any relevant information. State courts reviewing detention under a state regime may also review any detention under the Commonwealth regime.

Preventative detention will not apply to individuals under the age of 16, and will apply in a modified way to individuals between the ages of 16 and 18, as well as individuals incapable of managing their own affairs.

A detained individual will be given an opportunity to contact a lawyer, and is entitled to contact a family member or employer solely for the purpose of letting them know they are safe. If necessary, an interpreter may also be contacted.

Each year, the Attorney-General must report to Parliament on the operation of preventative detention orders.

### ***Stop, question and search powers***

The stop, question and search powers of the AFP have been extended for certain situations. The law previously authorised law enforcement officers to stop and search individuals airside when they deemed it necessary to safeguard against interference with aviation security. In addition, police had significant suspicion-based powers to stop and search individuals and their belongings without warrant, where certain legislated criteria were met. However, these powers did not extend beyond airports and diplomatic premises, effectively impeding the ability of law enforcement officers to safeguard against terrorism elsewhere.

To increase the AFP's ability to prevent and respond effectively to a terrorist attack, the new law extends AFP police and protective service powers to stop, question and search individuals within Commonwealth jurisdictional limitations, such as at Australian Government buildings in Canberra. These powers will be exercisable where:

- an AFP officer suspects on reasonable grounds that an individual might have just committed, might be committing, or might be about to commit a terrorism offence, or
- it is necessary for the prevention of, or in response to, terrorism and the Attorney-General declares a specified area or place (such as a transport hub or place of mass gatherings) a 'proscribed security zone'.

### ***ASIO questioning and detention powers***

In June 2006, the *ASIO Legislation Amendment Act 2006* (the Amendment Act) amended the Australian Security Intelligence Organisation's (ASIO) terrorism-related questioning and detention powers under the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). In June 2003 the ASIO Act was amended to empower ASIO to seek a warrant to question (for up to a total of 24 hours, or 48 hours if an interpreter is used), and in limited circumstances detain for up to 168 hours an individual who may have information that would substantially assist in the collection of intelligence in relation to a terrorism offence.

The Amendment Act followed a review by the then Parliamentary Joint Committee on ASIO, ASIS and DSD (which became the Parliamentary Joint Committee on Intelligence and Security) in November 2005 on the operation, effectiveness and implications of Part III, Division 3 of the ASIO Act, which contains ASIO's questioning and detention powers. The Amendment Act implemented many of the recommendations of the Committee to enhance the safeguards and clarify the operation of the regime. It also provided for the Committee to review the legislation and for the powers to sunset after 10 years (in 2016).

### ***Sedition laws***

Inciting an individual to commit a criminal offence is an offence in its own right under section 11.4 of the Criminal Code. The government has updated Australia's sedition offences to cover an individual who intentionally urges another individual to use force or violence to overthrow, interfere with or threaten the peace, order and good government of the Commonwealth, or assist an enemy at war with the Commonwealth.

There are good faith defences that cover communication that seeks to criticise government policy or publish reports or commentary on public interest matters. Such communication is consistent with legitimate activity in a democratic society.

### ***International efforts to strengthen counter-terrorism legislation***

The Australian Government established the Regional Legal Assistance Unit in the Attorney-General's Department in July 2005. The unit's main objective is to assist countries in South-East Asia to fulfil their international obligations by implementing in domestic law, international conventions and protocols on counter-terrorism. The unit also assists countries in the region in establishing and improving frameworks and capacity for international legal cooperation—for example, ensuring that legal and law enforcement officers in the region are able to assist in the investigation and prosecution of terrorists.

The government is also providing legal training to officials of Pacific island states through the Pacific Legal Knowledge Programme. The programme involves a series of capacity-building workshops across a number of areas, including international legal cooperation and legislative drafting.

### **Intelligence**

Australia relies on a strong intelligence effort to underpin the prevention, preparedness and response elements of our counter-terrorism strategy. While intelligence can never be guaranteed to provide knowledge or forewarning of terrorist intentions, it offers the best chance of preventing terrorist attacks before they can be carried out.

The goal of intelligence agencies is to identify those who are likely or intending to undertake terrorist attacks and monitor their capabilities, intentions and plans in order to allow preventative action. Intelligence can also enhance government decision-makers' strategic and situational awareness so they can make more informed decisions to protect Australians and Australian interests.

Australian intelligence agencies have been concerned with terrorism for many years. Since the 11 September 2001 attacks, terrorism has become a priority for all agencies, although conventional state-to-state threats also remain a key focus.

The 2004 Madrid and 2005 London bombings demonstrated the breadth of the task facing intelligence and law enforcement agencies in identifying and monitoring the many potential sources of threat. The threat is globally dispersed, constantly changing and evolving, and those involved are actively working to avoid detention. Typically terrorist cells are small, difficult to penetrate and increasingly adept at concealing their activities and intentions from the authorities.

Western countries have been investing significantly in their intelligence capabilities since the attacks of 11 September 2001. The Australian Government is committed to ensuring that Australia's intelligence agencies have the expertise, capacity and resources to combat terrorism. Since 2001, the government has committed over \$2.5 billion in additional funding to bolster its intelligence gathering and assessment capability across the Australian intelligence community (AIC). As a result, the AIC today has increased capacity to collect and analyse information related to national security. There is now much greater cooperation and information-sharing between AIC and other agencies, as well as with Australia's allies and partners in our region and globally.

The AIC consists of six key agencies:

- Office of National Assessments (ONA)
- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Defence Intelligence Organisation (DIO)
- Defence Signals Directorate (DSD)
- Defence Imagery and Geospatial Organisation (DIGO).



### ***Office of National Assessments***

ONA provides assessments on international political, strategic and economic developments to the Prime Minister, members of the National Security Committee of Cabinet and key senior policy makers in the government. ONA bases its assessments on information available to the Australian Government from all sources. ONA provides assessments on issues such as the evolving nature of terrorism and terrorist organisations, terrorist financing, terrorist interest in chemical, biological, radiological and nuclear weapons, and connections between terrorism and organised crime.

Since 2004, ONA has expanded and strengthened its coordination and evaluation role within the AIC. ONA has responsibility for coordinating and evaluating Australia's foreign intelligence activities and issues of common interest among Australia's foreign intelligence agencies. The Director-General of ONA is chair of the Foreign Intelligence Coordination Committee, established in August 2004 in response to the recommendations of the *Inquiry into the Australian Intelligence Agencies*, undertaken by Mr Philip Flood AO in 2004.

### **The Flood Inquiry into Australian Intelligence Agencies**

The 2004 Report on the Inquiry into Australian Intelligence Agencies by Mr Philip Flood AO was the result of the most significant review of the Australian intelligence community since the early 1990s. A key outcome of the Inquiry was recognition of the need for closer coordination of Australia's foreign intelligence agencies.

The Flood Inquiry arose out of increased scrutiny of the role of intelligence in the decision-making of the Australian Government. The government commissioned the inquiry in March 2004 in response to a recommendation of the Parliamentary Inquiry into Intelligence on Iraq's Weapons of Mass Destruction (WMD). The Flood Inquiry focused on the coordination, oversight, accountability, operations, independence and funding adequacy of the Australian foreign intelligence community.

A significant recommendation of the Inquiry was the formation of the Foreign Intelligence Coordination Committee, chaired by the Director-General of ONA. The Committee brings together the heads of the intelligence agencies, senior officials from the Department of the Prime Minister and Cabinet, DFAT, the Department of Defence and AFP. The Committee's primary role is to assist the Director-General of ONA in coordinating the activities of the foreign intelligence community and monitoring and evaluating its performance.

In addition, the Flood Inquiry recommended:

- amendments to the *Office of National Assessments Act 1977* and the *Intelligence Services Act 2001*
- a stronger role for the Department of the Prime Minister and Cabinet in assisting ministers in their management of the AIC, particularly in the areas of foreign intelligence policy and priority-setting, evaluation and advising on resource needs
- better coordination and management of cross-AIC issues, such as training, career development and language capabilities
- extension of the authority of the Inspector-General of Intelligence and Security to include a periodic review of the statutory independence of ONA and the authority to conduct its own inquiries into matters relating to all intelligence agencies.

### **The Australian Security Intelligence Organisation**

ASIO, Australia's security service, plays a key role in Australia's counter-terrorism arrangements. ASIO's functions include obtaining and assessing security intelligence, providing intelligence and advice to government on security (including protective security advice), and providing and maintaining elements of the counter-terrorism response capability. ASIO's intelligence focus is 'security intelligence'—that is, intelligence that will help protect Australia from terrorism and other forms of politically motivated violence, communal violence, espionage, sabotage, attacks on Australia's defence system, and acts of foreign interference. ASIO's work is not limited by geography—it is not a 'domestic' intelligence service—but extends to wherever in the world those activities might threaten Australia's interests. ASIO is both an intelligence collector and an intelligence assessor.

To this end, ASIO obtains and analyses information from published sources, interviews, surveillance, human sources, other Australian and international liaison partners,

and through the use of special powers authorised by legislation. ASIO works closely with the Australian Federal Police (AFP) and state and territory police on counter-terrorism operations, investigations and prosecutions. ASIO also assesses and provides advice on the security threats to Australia's critical infrastructure sectors and specific infrastructure facilities.

ASIO's engagement with international partners and its network of liaison officers overseas provide access to intelligence and shared capabilities that are vital to progressing investigations.

The government has significantly increased ASIO's resources since 2001 to meet the challenges of potential sources of terrorist threat to Australia, as well as the continuing threat of espionage and foreign interference. The additional resources will substantially strengthen ASIO's capability in a range of areas, including intelligence collection and assessment, surveillance, technical operations, border security and IT systems.

### **National Threat Assessment Centre**

ASIO has national responsibility for the preparation of threat assessments, a key element in Australia's protective security arrangements. In 2004, the Australian Government established a dedicated multi-agency, round-the-clock National Threat Assessment Centre within ASIO. The Centre's threat assessments are based on intelligence and other information available to Australian authorities from all sources. Threat assessments address broad national threat levels, threats against specific events and people, and threats to Australians and Australian interests both domestically and overseas. Threat assessments are an important tool for informing travel advisories prepared by the Department of Foreign Affairs and Trade (DFAT), for determining the national counter-terrorism alert level and for government decision-making about security measures. The National Threat Assessment Centre includes officers from ASIO and seconded officers from the Department of Transport and Regional Services (DOTARS), AFP, ASIS, DFAT, DIO, DSD and ONA.

### ***Australian Secret Intelligence Service***

ASIS is Australia's overseas intelligence agency. Its primary function is to gather intelligence not readily available by other means about the intentions, capabilities and activities of individuals or organisations outside Australia that may affect Australian interests. This may include reporting on violent extremism, weapons proliferation and other national security threats. ASIS also maintains a network of relationships with foreign intelligence agencies, thereby improving Australia's access to baseline and threat-related intelligence. Such international cooperation has also helped to strengthen the counter-terrorism capability of a number of countries in the Asia-Pacific region.

### **Intelligence cooperation**

The Australian Government's relationships with foreign intelligence counterparts represent an important national asset. Australia has intelligence-sharing arrangements with several countries. Long-standing relationships with intelligence agencies in the United States, the United Kingdom, Canada and New Zealand have historically been highly productive.

Australia also maintains a network of out-posted liaison officers stationed in key partner capitals to ensure effective intelligence cooperation on common issues that affect our collective national interests.

### ***Defence Intelligence Organisation***

DIO provides support for Defence and government decision-making, and assists with intelligence support to the planning and conduct of Australian Defence Force (ADF) operations.

DIO is responsible for assessing intelligence focusing on global security developments, defence economics, military capabilities, and science and technology with military applications. DIO also has a well developed terrorist and counter-terrorist assessment function supported by civilian and military analysts with in-depth experience across a range of related issues. DIO's intelligence products and services help inform its customers on military activities at home and abroad, defence acquisition processes, force readiness decisions, strategic policy, foreign relations and defence scientific developments.

### ***Defence Signals Directorate***

DSD is Australia's national signals intelligence agency. DSD collects and disseminates foreign signals intelligence to Australian Government agencies. Since 2001, DSD has received additional funding to increase its signals intelligence collection capabilities against terrorism.

DSD also provides a range of information security services and advice, including cryptographic services and products, information security advice and accreditation of secure systems to ensure that the Australian Government, ADF and other national communication and information systems are secure.

### ***Defence Imagery and Geospatial Organisation***

DIGO supports government and ADF operations through the collection and analysis of imagery and geospatial information. DIGO has a counter-terrorism intelligence collection capability to address the increased threat from terrorism.

### ***Accountability of the Australian intelligence community***

Australia has a number of safeguards in place to provide ongoing assurance that the intelligence agencies perform their functions within the parameters of Australian law and international norms.

The Inspector-General of Intelligence and Security (IGIS) is a key element of the accountability regime for the AIC. The IGIS is an independent officer who assists the government in overseeing and reviewing the activities of the AIC. The IGIS was set up under the *Inspector-General of Intelligence and Security Act 1986* to provide independent assurance to the Australian Government, the Parliament and the people that the intelligence agencies:



- conduct their activities within the law
- behave with propriety
- comply with ministerial guidelines and directives
- have regard to human rights.

The IGIS has strong investigative powers, similar to those of a Royal Commission. The Inspector-General can undertake an inquiry in response to a complaint or a reference from a minister, or act independently to initiate inquiries. To guarantee independence of the office, the IGIS is appointed by the Governor-General for a fixed term and can only be dismissed by him in certain circumstances. The Inspector-General is required to table an annual report to Parliament on the operations of IGIS.

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is another important mechanism for overseeing the intelligence agencies. The role of the PJCIS—previously known as the Parliamentary Joint Committee on ASIO, ASIS and DSD—is to provide parliamentary oversight of certain aspects of the six AIC agencies. In particular, the PJCIS is authorised under the *Intelligence Services Act 2001* to:

- review the administration and expenditure of the agencies, including annual financial statements
- review any matter in relation to the relevant agencies referred to the Committee by the responsible minister or a resolution of either House of the Parliament
- report the Committee’s comments and recommendations to each House of the Parliament and to the responsible minister.

The PJCIS prepares and tables an annual report on the AIC as soon as practicable after each financial year ending 30 June.

### ***Whole-of-government approach to counter-terrorism***

In addition to the AIC, several other Australian Government agencies are able to assist the government in its decision-making on security matters by providing valuable counter-terrorism information, in line with their respective areas of specialisation. These agencies include: DFAT, AFP, DOTARS, the Attorney-General’s Department, the Australian Customs Service (Customs), the Department of Immigration and Multicultural Affairs (DIMA), and the Australian Transaction Reports and Analysis Centre (AUSTRAC).

### **Law enforcement**

Although the law enforcement and intelligence functions complement each other, Australian law enforcement and intelligence agencies are separated by distinct legislative frameworks and operating cultures.

Each state and territory police force forms the front line for enforcement of criminal law and preservation of public order. In the event of a terrorist incident, the first responders will typically be state and territory police and emergency services, with investigative support potentially being drawn from Joint Counter-Terrorism Teams, which consist of the Australian Federal Police (AFP) and state and territory police. This will largely replicate responses to criminal acts or disasters unrelated to terrorism.

### ***Australian Federal Police***

The AFP is the Australian Government's principal law enforcement agency and Australia's international law enforcement and policing representative. It plays a critical role in the whole-of-government effort to combat terrorism. Working in partnership with other government agencies, including the intelligence community, and its state and territory counterparts, the AFP has specific responsibility to investigate terrorist offences. The AFP's capacity to investigate terrorist offences has steadily increased since 2001, with substantial investments from the Australian Government.

The Australian Government has significantly strengthened its law enforcement capabilities to deal with the emerging terrorist threat environment. To this end, key national law enforcement objectives are to:

- strengthen the investigative capability of, and relations between, federal, state and territory police through the Joint Counter-Terrorism Teams
- consolidate and build on the ability of law enforcement agencies to undertake investigations into transnational crime and terrorist activity
- ensure that Australia's legal framework supports the effective operation of law enforcement agencies
- increase the AFP's contribution to regional counter-terrorism capabilities
- respond rapidly to threats or events in the region, in partnership with international law enforcement agencies and supported by state and territory police services, to ensure the safety of Australian citizens.



### ***Australian Bomb Data Centre***

The Australian Bomb Data Centre is hosted by the AFP. The Centre collects, collates, interprets and disseminates data gathered from Australia and overseas about the illegal use of explosive and other incendiary devices, whether commercial, military or improvised. It provides critical support to the international deployment of AFP members in combating terrorism. The centre also helps establish and maintain regional bomb data centres, including one in the Philippines. See also 'CBRN Data Centre' on p63.

### ***Australian High Tech Crime Centre***

In 2003, the Australian Government established the Australian High Tech Crime Centre within the AFP. The Centre is the main national-level law enforcement body for the investigation of electronic security (e-security) incidents, including cyber-terrorism, in public and private sector organisations. It performs a national coordination role for the

law enforcement effort in combating serious, multi-jurisdictional crime involving complex technology. By drawing its staff from state and territory police, secondees from various Commonwealth agencies and the private sector, it has consolidated and strengthened the national investigative capability for high-tech crime.

### ***International Legal Cooperation and Law Enforcement***

Effective legal cooperation and law enforcement, particularly in South-East Asia and the South Pacific, are key dimensions of Australia's international counter-terrorism agenda.

Australia currently benefits from 34 bilateral extradition treaties and 24 mutual assistance treaties with countries in Europe, the Americas and in the Asia-Pacific region. Extradition ensures that criminals cannot evade justice by crossing borders. Mutual assistance ensures that criminals cannot escape prosecution and confiscation action simply because the evidence or proceeds relating to their crime is in a different country. We are actively seeking to expand our network of both extradition and mutual assistance treaties, particularly with Asia-Pacific countries. We provide technical assistance to partner countries to increase their capacity to make and receive extradition and mutual assistance requests.

The Australian Government has also established dedicated counter-terrorism advisor and liaison roles in strategically important locations in recent years. Future initiatives include the establishment of counter-terrorism advisor positions in India, Thailand and Cambodia and expansion of the AFP's commitment to offshore counter-terrorism exercises.

The AFP's international work is delivering tangible rewards. They include increased regional liaison and cooperation through an invitation for the AFP to attend, among others, the Regional Heads of Counter-Terrorism Forum—ASEANAPOL. The AFP has accepted invitations from foreign governments to establish joint in-country investigations teams, including at the Jakarta Operations Centre and the Manila Operations Centre. It has also been involved in high-profile international investigations into major terrorist incidents, and was recently invited to join the teams investigating the 2005 London bombings and the 2005 Bali bombings.

#### **Jakarta Centre for Law Enforcement Cooperation**

The Jakarta Centre for Law Enforcement Cooperation (JCLEC), established in July 2004, is a flagship for law enforcement training in South-East Asia. Several international governments contribute to the work of the JCLEC.

Australia contributed \$36.8 million over five years to support the joint Indonesian–Australian initiative to establish the JCLEC. The centre is an international education and training institution aimed at increasing the capacity of regional countries to manage complex multi-jurisdictional investigations into transnational crimes, with a focus on terrorism. It is building regional counter-terrorism capabilities and provides a hub of practical experience for responding to particular threats or incidents.

To date, the JCLEC has contributed to capacity-building in the region by training over 1200 professionals from countries around the region in courses as diverse as Islamic law and politics, security risk management, disaster victim identification investigations management, criminal intelligence and forensics.

### ***Australian Transaction Reports and Analysis Centre***

Australia is at the leading edge of the international effort to combat money-laundering and the financing of terrorism. The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's anti-money-laundering regulator and specialist financial intelligence unit. In its intelligence role, AUSTRAC provides financial transaction reports and information to Commonwealth, state and territory law enforcement and revenue agencies.

AUSTRAC's counter-terrorism work focuses on the research and analysis of terrorist financing typologies that reflect patterns and trends for the financing of terrorist groups. This information is used to build financial intelligence that identifies potential money flows directed toward terrorism and other major crimes.

Internationally, AUSTRAC works to facilitate the exchange of financial information and to build an environment hostile to money-laundering, major crime, revenue-evasion and the sponsorship of terrorism. AUSTRAC's bilateral relationships include both information exchange between AUSTRAC and other financial intelligence units globally, and technical assistance and training initiatives in which AUSTRAC seeks to help countries develop stronger anti-money-laundering and counter-terrorist financing regimes.

AUSTRAC also provides support to the Attorney-General's Department, which leads the Australian representation at the Financial Action Task Force on Money Laundering.

### **Critical infrastructure protection**

The Government's critical infrastructure protection strategy covers those systems we all rely on in our day-to-day lives—communications networks, banking, energy, water and food supplies, health services, social security and community services, emergency services and transport. These are the physical facilities, supply chains, information technologies and communication networks, which, if destroyed or degraded, would adversely impact on Australia's social or economic wellbeing, or affect our ability to ensure national security.

Infrastructure can be damaged, destroyed or disrupted by natural disasters, negligence, accidents, criminal activity as well as by acts of terrorism. The government's policy therefore seeks to protect Australia's critical infrastructure against a range of threats and hazards.

The primary responsibility for the protection of Australia's critical infrastructure rests with infrastructure owners and operators. Only a small amount of Australia's critical infrastructure is owned by the Australian Government, for example defence, intelligence and other national security facilities. The vast majority of our critical infrastructure is either owned by the private sector or owned and operated by state and territory governments on a commercial basis. Protecting Australia's critical infrastructure therefore requires high levels of cooperation between business and government at all levels.

### ***The role of the Australian Government in critical infrastructure protection***

The Australian Government's approach to critical infrastructure protection aims to ensure that there are adequate levels of protective security for national critical infrastructure,

minimal single points of failure and rapid, tested recovery arrangements. The government provides strategic leadership on the national critical infrastructure protection effort through the Attorney-General's Department. The department is responsible for providing national coordination in areas of joint Commonwealth, state and territory responsibility, producing and communicating relevant information to key government and non-government stakeholders, promoting critical infrastructure protection as a national research priority and leading Australia's international engagement on critical infrastructure protection issues.

### **National Guidelines for Protecting Critical Infrastructure from Terrorism**

Working closely with the states and territories, the National Counter-Terrorism Committee developed National Guidelines for Protecting Critical Infrastructure from Terrorism which were endorsed by the Council of Australian Governments in 2004. These guidelines provide a nationally consistent approach to helping critical infrastructure owners and operators protect their assets from terrorism.

The guidelines are designed specifically to help critical infrastructure owners and operators make informed decisions about risk management and security planning. They are also used by governments at the Commonwealth, state and territory, and local levels. They provide information on different areas of responsibility, critical infrastructure identification, and management of public information and the media.

### ***Working together—an effective business–government partnership***

The Australian Government is committed to a strong partnership with business in protecting our critical infrastructure. The government has strengthened this partnership through the creation of the Business Government Advisory Group on National Security. This high-level group, chaired by the Attorney-General, provides senior business leaders with an opportunity to discuss the strategic direction of our national security policy and provide advice and feedback on national security issues relating to critical infrastructure protection.



### ***Trusted Information Sharing Network***

The government has also established the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection, which forms the centrepiece of the business–government relationship. The TISN is made up of a Critical Infrastructure Advisory Council and a number of expert advisory and industry-based groups. The Council is the main coordinating mechanism of the TISN. It comprises key business leaders and relevant government agencies and provides a direct line of communication from the broader business community to the government on critical infrastructure protection issues. Importantly, it also has a direct link with the National Counter-Terrorism Committee (NCTC). In its first three years of operation, the TISN has made some significant achievements. Some examples include:

- establishment of a risk-management framework for the communications sector
- creation of an Energy Supply Chain Mapping Project, which details the dependencies and linkages in the energy sector
- development of the National Strategy for Enhancing the Safety and Security of Australia's Food Supply.

Underpinning the work of the TISN is the series of Infrastructure Assurance Advisory Groups that have been established across the following industry sectors: energy, water, banking and finance, communications, food chain, emergency services, transport, mass gatherings (see below) and health. These groups provide a forum for infrastructure owners and operators to share information on threats and vulnerabilities, and strategies and measures to mitigate risk.

#### **Critical Infrastructure Protection Modelling and Analysis (CIPMA) programme**

In 2004 the government commissioned a programme to identify and analyse the interdependencies between critical infrastructure sectors. The \$19 million CIPMA programme is developing a complex computer modelling and analysis capability unique to Australia. It uses a vast array of data and information from a range of public and private sector sources to model and simulate the relationships between critical infrastructure assets and networks.

The programme's initial focus is on the energy, communications, banking and finance, and water sectors, which underpin much of Australia's economy. This will allow government to better assess the potential flow-on effects of a disruption in one infrastructure sector to other industry sectors. This information will assist in the development of government policy, and to help owners and operators make more informed investment decisions to better protect their critical infrastructure.

### ***ASIO Business Liaison Unit***

The government has created a Business Liaison Unit within ASIO to help ensure that the owners and operators of critical infrastructure and other relevant members of the business community can access information on matters affecting the security of assets and staff for which they are responsible. The Unit has developed a secure website at <https://secure.blu.asio.gov.au> for business containing a range of other security-related information, including sector-specific business security reports.



### ***Places of mass gathering***

While places of mass gatherings are not considered infrastructure in the traditional sense, the government is working with their owners and operators to protect them against acts of terrorism. These places include sporting venues, shopping centres, business precincts, cultural facilities, hotels, public transport hubs and major planned events.

Protecting such places from a potential attack is an enormous and diverse task. The Australian Government is working with state, territory and local governments, as well as with business owners and operators, through groups such as the TISN and the NCTC, on this important national issue. For example, the NCTC has developed a document titled *National Approach for the Protection of Places of Mass Gathering from Terrorism*. This document has been developed to promote a nationally consistent approach across all states and territories by setting out the key roles and responsibilities of governments, security agencies and business to protect places of mass gatherings from terrorism.



### **Border security**

With a vast coastline and some 20 million people and 7 million cargo consignments crossing Australia's borders annually, border security is complex. This complexity will grow as global human, economic and information flows increase.

Australia's layered system of border control is regarded as world-class. However, we need to continuously improve to better secure our borders, particularly in the face of evolving terrorist threats. To this end, the Australian Government is investing \$1.1 billion over the 10 years from 2001 to increase the integrity and efficiency of our border security regime.

Since 11 September 2001, the government has strengthened border security in six key ways:

- tightening the legal framework and increasing enforcement powers for the Australian Federal Police (AFP), Australian Customs Service (Customs) and other border protection agencies
- enhancing immigration visa processing, information storage systems and airline liaison officer and overseas compliance networks
- increasing our capacity to detect fraudulent documentation and the development and use of biometrics to detect identity fraud
- bolstering security in the screening of air freight and sea-borne cargo
- enabling additional surveillance of seas to the north and northwest of Australia
- strengthening cooperation with regional countries.



### ***Laws for border protection***

The capacity of our border control agencies to control the movement of people and goods across Australia's borders has been significantly increased. Legislation introduced in January 2003 makes it mandatory for operators of airlines and shipping lines to report to Customs and the Department of Immigration and Multicultural Affairs (DIMA) details of passengers and crew arriving on a flight or voyage from outside Australia, before they arrive. The legislation requires ships and aircraft to provide Customs with reports of cargo in-transit through Australia, and enables in-transit goods to be examined and, in certain cases, seized. It also allows our agencies to assess the bona fides of people and goods entering Australia and identify possible risks to Australia's security.

### ***Layered border processing***

The Australian Government, through DIMA, has a layered approach to air and sea border control. The system extends from the visa-issuing process overseas through to check-in and border processing at entry points at Australian air and sea ports. It includes:

- the Electronic Travel Authority system—the world's most advanced and streamlined travel authorisation system. The system links DIMA with approximately 300 000 travel agents and 75 airlines worldwide and allows Australia to check visitors when they book their travel.



- the Movements Alert List system, which stores data on people and travel documents of concern to immigration, law enforcement and security authorities. It is linked with DIMA's processing systems for visas, border clearance and citizenship.
- the Airline Liaison Officer network, which works closely with airlines, immigration and airport staff to detect and prevent passengers who do not have the right documents from travelling to Australia. The network is a visible deterrent to people smugglers and people of potential security concern who attempt to travel to Australia by indirect routes.
- the Advance Passenger Processing system, which forwards airline passenger information to a clearance system when a passenger checks in to depart for Australia. Passenger information is checked against current visa and passport databases and alert list systems in real time. Since January 2004, all passengers and crew of cruise liners have also been processed by the system before departing to Australia. DIMA is currently planning the rollout of the system to the commercial shipping industry.

### ***Combating identity fraud***

Identity security is of particular importance to border security. While the Australian passport has always been a document with world-class security design features, a new passport released in December 2003 has made it even more difficult to forge.

Australia's biometrics programme, which complements the biometric work under the National Identity Security Strategy, aims to increase border security through the development of systems for detecting and reducing identity fraud, as well as for advanced passenger processing. DIMA has developed a capacity to store and use digital biometric images to capture the identity of clients and to verify their identity each time they deal with the department. Customs has developed *SmartGate*—an automated border processing system that uses face-recognition technology to accurately match travellers against their travel documents. SmartGate will replace the face-to-passport check currently undertaken by Customs Officers.

### ***Screening of goods and people entering Australia***

Customs has a strong focus on physical and electronic screening of cargo, vessels and people to prevent dangerous goods and people entering Australia. To do this, Customs:

- assesses the risk of all commercial vessels through its intelligence and assessment techniques
- uses state-of-the-art x-ray container examination systems in all major Australian seaports, which have also significantly increased sea cargo inspection rates
- uses technology and training to examine 70 per cent of all imported air cargo
- employs the Integrated Cargo System, which, under the Cargo Management Re-engineering initiative, updated and streamlined the reporting process for assessing risk of air and sea cargo using a more powerful intelligence database
- uses explosives trace detection equipment, firearms and explosives detector dog teams, as well as mobile x-ray vans, to screen sea and air cargo
- assesses risk through heightened controls over export air cargo, including advanced reporting

- uses high-sensitivity radiation detectors in airports, mail-handling centres, and sea and air cargo examination facilities, giving Customs the ability to detect and locate radioactive explosive devices, including low-technology devices like dirty bombs and other illegal radioactive freight
- employs a layered national counter-terrorism training programme for Customs officers, other Australian Government officials and regional officials to help them to identify and report terrorist activity.



### ***Watching Australia's coastal approaches***

The Border Protection Command (BPC—previously known as the Joint Offshore Protection Command) was established in 2005 to provide an overarching capability for offshore civil maritime protection. This includes counter-terrorism prevention, interdiction and response to all offshore areas of Australia, including Australia's offshore oil and gas installations.

Through the BPC, the ADF and Customs work together to patrol Australia's coastline. In 2006, the government announced a comprehensive \$388.9 million package to strengthen Australia's response to maritime security in our northern waters. This represents a significant increase in whole-of-government efforts to ensure that people smugglers, illegal fishers, drug traffickers and other transnational criminals, including terrorists, are detected, detained and prosecuted.

### **Border Protection Command**

The Border Protection Command (BPC) controls and coordinates all operational responses to civil maritime security threats in the Australian Exclusive Economic Zone (EEZ) and adjacent areas. By combining the strengths, resources and expertise of all Commonwealth agencies with a responsibility for maritime security, BPC:

- controls and coordinates all 'on the water' operational responses to civil maritime security threats
- develops and maintains maritime awareness through the collation and fusion of all information and intelligence related to maritime security, and the development and maintenance of a comprehensive database of all known activity in the maritime domain
- develops and maintains an information analysis facility that is the central repository for maritime-related information and intelligence, and provides operational intelligence, as well as analysis of trends, assessments of effectiveness and estimates of maritime security threats.

Since September 2001, in response to an increase in unauthorised boat arrivals, the Australian Government has tasked the ADF to assist in the detection and interception of unauthorised boats entering Australian territorial waters off the northwest coast and offshore territories. The ADF's capabilities allow the government to have a continuous presence in our north, thereby helping to maintain border integrity.

In 2005, the government announced a \$139.3 million package for the ADF to protect Australia's offshore oil and gas facilities on the North West Shelf, including the purchase of two new Armidale Class Patrol Boats to undertake maritime surveillance. This package enables dedicated surveillance and monitoring of the North West Shelf to protect strategic national assets, and provides an enhanced quick-reaction capability to respond to potential threats, including terrorist attacks. As part of the government's 2005 commitment, Unmanned Aerial Vehicle system trials have also been conducted to assess their potential for long-duration maritime surveillance.

Additional resources have been provided for temporary detention, transport, investigation and prosecution of illegal foreign fishers. Other measures include improvements to surveillance capacity involving additional patrol boats, increased aerial surveillance and enhanced ocean surveying and charting. Quarantine risk management will also be improved through faster investigation of quarantine breaches, new purpose-built boat destruction facilities and the employment of extra Indigenous rangers.

### ***Quarantine controls***

Terrorists have demonstrated their willingness to consider employing a range of methods of attack. Among these is the introduction of material that could cause damage to Australia's agricultural sector, such as foot and mouth disease or exotic pests. In recent years, the government has substantially increased the capacity of the Australian Quarantine and Inspection Service and Customs to respond to the possible risk of exotic pests and diseases, including those used in a terrorist attack. Quarantine border intervention target rates have now increased to more than 80 per cent of passenger

baggage at international airports and 100 per cent at other border entry points. Similarly, 100 per cent of sea port containers are now externally inspected.

### ***Regional border cooperation***

Australia actively works in the region to promote effective, risk-managed border control—particularly because of the numerous islands making up many regional countries. In the 2006–07 Budget, the Australian Government allocated \$92.6 million for counter-terrorism efforts in the region. AFP, Customs, DFAT and DIMA have bolstered efforts to assist regional states to improve their border management. These efforts focus on delivering specialist training and equipment. They also include cooperative arrangements to help priority countries to detect, deter and investigate the movements and activities of terrorists.

For example, the regional training role of the Global Document Examination Network has been significantly expanded to strengthen regional identity security capabilities in order to curb movement by terrorists, people smugglers and other criminals. Seven new document examination experts have been recruited in the past year—five in Australia and two at overseas posts. Australian forensic examiners will work with host government agencies in Manila and Kuala Lumpur to build a regional approach to identity security and document fraud.

#### **Regional Movement Alert System**

The Regional Movement Alert System is an APEC counter-terrorism initiative. It strengthens the ability of border management agencies to detect the attempted use of lost, stolen or otherwise invalid travel documents by allowing countries in that region to directly access each other's lost, stolen and invalid passport databases.

DIMA received funding of \$3.5 million in 2004 for a pilot Regional Movement Alert System between Australia and the United States. New Zealand joined the trial in 2006. The 2006–07 Budget provided \$10.9 million over four years to upgrade the pilot system to a fully operational system that will aim to incorporate more APEC economies.

### **Transport security**

The attacks of 11 September 2001 in the United States, Madrid in 2004, London in 2005 and Mumbai in 2006 highlighted the vulnerability of transport systems as both a target and a potential weapon for terrorists. It is critical that our transport systems, and their physical assets, control systems, passengers and cargo are secure and protected.

#### ***National Transport Security Agenda***

Since 2002, the Australian Government has introduced a range of new measures to counter potential threats to the security of Australia's domestic and international transport networks. These measures have five key aims:

- to strengthen aviation security measures
- to implement a new maritime security regime
- to build a nationally consistent approach to transport security

- to provide leadership and assistance in setting priorities for strengthening Australia's land transport security
- to increase Australia's international cooperation and assistance to countries in the region.

Responsibility for transport security rests with all levels of government and the private sector. The Commonwealth, state and territory governments have an important role in encouraging national approaches to transport security. In 2004, they agreed to a National Transport Security Strategy. This complements the National Counter-Terrorism Plan and sets out Australia's approach to transport security. Increasingly, the private sector plays a role in building and operating land transport infrastructure, such as motorways and rail services. Sea ports are operated by state and territory governments or the private sector. Aviation infrastructure in Australia is largely a private sector responsibility.

### ***Office of Transport Security***

In December 2003, the Australian Government established the Office of Transport Security within the Department of Transport and Regional Services. The Office is responsible for regulating aviation and maritime transport security in Australia. It also works to ensure the transport sector receives important transport-specific security information.

### ***Inspector of Transport Security***

The Australian Government appointed an Inspector of Transport Security in November 2004. The role of the Inspector is to independently investigate, when required by the Minister for Transport and Regional Services, security incidents or a pattern or series of incidents that point to weaknesses in transport security systems or failures in aviation or maritime regulation. If the Minister is concerned about an incident, systemic weakness or failure in the transport sector for which another jurisdiction has transport security regulatory responsibility, the Minister can seek the agreement of that state or territory government to have the Inspector carry out an inquiry.

### ***Aviation security***

More than 99 per cent of Australia's international passenger movements are by air transport. In the year ending April 2006, some 21 million airline passengers entered and left Australia, and there were 42 million passenger movements within Australia. The Australian Government is constantly working to increase the security of Australia's aviation system in response to current and evolving threats.

The *Aviation Transport Security Act 2004* came into force on 10 March 2005, strengthening Australia's aviation security system. Under the new law, security measures have been expanded to provide more protection to the travelling public and aviation industry from unlawful interference with aviation. The Act provides a world-class aviation security framework able to adapt to evolving threats. It brings our aviation security into line with International Civil Aviation Organisation standards introduced after 11 September 2001. The Act allows the Australian Government to use a range of up-to-date regulatory practices, such as auditing the industry's security measures, and enforcing compliance with our aviation laws.

### **Securing our regional skies**

Under the \$48 million Securing Our Regional Skies package announced in August 2004, several aviation security measures were introduced to improve our ability to manage incidents at regional airports and on regional airlines. These measures include:

- a closed-circuit television (CCTV) trial at selected regional airports
- training and kitting out 149 regional airports with hand-wand metal-detection systems
- security training for regional airline and airport staff
- a joint training and exercise programme involving state and territory police and the AFP
- building public awareness in regional communities
- creating and deploying four AFP Protective Service Regional Rapid Deployment Teams.

### ***Wheeler Review of Airport Security and Policing***

Sir John Wheeler presented his report, *An independent review of airport security and policing for the Government of Australia*, on 12 September 2005. The report examined the threat of serious and organised crime at airports, the integration of ground-based security and law enforcement arrangements, and the adequacy of existing security requirements.

The report made 17 recommendations dealing with a range of issues, including policing roles and responsibilities at airports, the procedures for background checking, and the flow of information and intelligence to airport operators as well as Australian Government agencies.

The Australian Government accepted the thrust of the Review's recommendations and agreed to provide funding of \$886 million over five years from 2005–06. The key measures announced from the Wheeler Review include:

- increased airside Customs border patrols
- a further upgrade to the CCTV capabilities, including assistance for airport operators and additional cameras at major airports
- strengthened air cargo security arrangements, including the introduction of improved technology for the detection of explosives
- improved security and crime information exchange arrangements for the aviation sector
- further tightening of background checking for the issue of Aviation Security Identification Cards
- a new national aviation security training framework to support the aviation industry.

Of the \$886 million, \$679.5 million has been committed for improved policing at airports. This supports a range of policing functions at major airports, including:

- counter-terrorism first response capability
- five new Joint Airport Investigation Teams to address serious and organised crime
- new Joint Airport Intelligence Groups
- Unified Police (community policing)
- Airport Police Commanders.

The Australian Government also established AusCheck, a new Division in the Attorney-General's Department, which will commence operations on 1 July 2007. AusCheck will be responsible for conducting background checks on those who work in the secure areas of air and sea ports—that is, those who are required to hold Aviation Security Identification Cards and Maritime Security Identification Cards (see below). AusCheck will strengthen national security arrangements by providing a centralised and nationally consistent approach to ensuring that unsuitable individuals are not able to work in security-sensitive areas of air and sea ports.

### ***Maritime security***

Over 99 per cent of Australian imports and exports (by weight) are carried by sea. A terrorist attack against Australian maritime transport could have devastating consequences for Australians, including our economic interests and our marine environment. Maritime security is an area of policy and operational focus for the Australian Government domestically, in our region and beyond.



### ***Maritime Transport and Offshore Facilities Security Act 2003***

The Australian Government has put in place a robust and world-class maritime security regime to help safeguard Australia's maritime transport system and offshore facilities from terrorism. Australia's domestic maritime security regime is regulated by the *Maritime Transport and Offshore Facilities Act 2003*. Under this Act, all security-regulated ports, port facilities, offshore facilities and ships undertake risk assessments and prepare security plans to address risks.



The Office of Transport Security is responsible for assessing, approving and checking compliance of these security plans. It also security assesses and checks compliance of all security-regulated ships wanting to enter Australian ports.

### ***Maritime Security Identification Cards***

In 2004, the Australian Government announced measures to further strengthen maritime security arrangements in Australia. One of these measures was the introduction of a Maritime Security Identification Card. The Card is a nationally recognised security identification card. It shows that a person has been security-checked and is cleared to enter the secure areas (that is, maritime security zones) of our ports, ships and offshore oil and gas facilities. All personnel needing unmonitored access to maritime security zones will need to hold and display a valid card.

### ***International maritime security***

The Australian Government is increasingly involved in maritime security work overseas. Australia recently signed new international protocols on maritime security to strengthen international efforts to counter terrorism. The protocols created new offences on the use of vessels and fixed platforms to transport or detonate weapons of mass destruction. They also set up a regime for boarding vessels suspected of being used for certain criminal activity, including terrorism.

Australia is working with several regional countries to increase maritime security and has played a critical part in helping regional countries meet their obligations under the International Shipping and Port Security Code.

### **International Ship and Port Facility Security (ISPS) Code**

In November 2001, the international community through the International Maritime Organisation (IMO) resolved to improve the security of maritime transport worldwide, to reduce the possibility of maritime terrorist attacks. In December 2002, the IMO adopted the International Ship and Port Facility Security (ISPS) Code, which is now mandatory for all passenger vessels and cargo vessels of over 500 gross tonnage.

While the ISPS Code built a framework for preventative security for ships and ports, it was recognised that more work was needed to respond to intelligence about planned attacks and to prevent attacks occurring. To address this need, the international community updated an existing maritime instrument—the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation 1988 (the SUA Convention) and included a range of terrorism-related offences and provisions for boarding ships on the high seas. The SUA Convention is implemented in Australia through the *Crimes (Ships and Fixed Platforms) Act 1992*.

### ***Surface transport security***

The security of Australia's surface transport networks depends on strong cooperation between all levels of government, business, employees in the industry, as well as the Australian public.



Approximately 1.5 billion tonnes of freight is moved on the Australian road network every year. Rail also moves significant amounts of freight. Approximately 550 million passengers travel by rail every year; 97 per cent of them use urban rail networks.

Following the 2004 Madrid attacks, Australian governments moved quickly to review the threat to land transport in Australia. On 3 June 2005, COAG signed the Intergovernmental Agreement on Surface Transport Security. The Agreement sets out arrangements to protect Australians and the surface transport system through the implementation of national protective security planning and preventative measures. Australian governments have also agreed to:

- further develop and implement technological and other solutions for the security of surface transport
- broaden the ability of transport operators, their staff and the public to contribute to the security of surface transport
- help operators plan and prepare for security incidents
- support an integrated approach to transport precinct security.

### *Closed circuit television*

At its special meeting on counter-terrorism in September 2005, COAG agreed that CCTV has the potential to assist terrorism investigations involving Australian interests, and also agreed to a national, risk-based approach to enhancing the use of CCTV for counter-terrorism purposes. This includes the development of a National Code of Practice for CCTV systems for the mass passenger transport sector.

The National Code was adopted by COAG on 14 July 2006. The code is voluntary and sets out how to use CCTV systems to support post-terrorist incident responses and investigation. The code allows each jurisdiction, based on an appropriate risk analysis, to determine its own CCTV requirements.



## **Identity security**

Identity security is central to Australia's national security, law enforcement and economic interests because it underpins public confidence and trust in government and business processes and preserves the integrity of those processes.

The growing global problem of identity fraud—involving the theft of real identities or the fabrication of fictitious identities—affects all Australians and all levels of Australian government. The potential nexus between identity fraud, terrorist financing and terrorism has significant implications for Australia's national security.

### ***National Identity Security Strategy***

On 14 April 2005, the Australian Government announced the development of a National Identity Security Strategy (NISS) to combat the misuse of stolen or assumed identities in the provision of government services. The NISS aims to strengthen identity security through rigorous enrolment and authentication processes, while ensuring personal privacy. It will be developed in partnership with state and territory governments in recognition of their responsibility for primary identification documents, such as birth certificates, fact-of-death data and drivers' licences. The private sector will also be consulted.

The key objectives of the strategy include:

- improving standards and procedures for enrolment and registration, including identifying key Proof of Identity documents to be used by all appropriate organisations for the purposes of identifying and registering clients for services
- enhancing the security features on key Proof of Identity documents to reduce the incidence of successful forgery
- establishing mechanisms to enable organisations to verify the data on key Proof of Identity documents provided by clients when registering for services
- improving the accuracy of personal identity information held on organisations' databases
- enabling greater confidence in the authentication processes for individuals using online services
- providing appropriate legislative support.

At its special meeting on counter-terrorism in September 2005, the Council of Australian Governments (COAG) agreed to the development and implementation of NISS and a national document verification service to combat the misuse of false and stolen identities, and to investigate the means by which reliable, consistent and nationally interoperable biometric security measures could be adopted by all jurisdictions.

The Australian Government allocated \$5.9 million in the 2005–06 Budget to advance the NISS, as well as for two key pilot programmes—a pilot document verification service and a data integrity pilot. The document verification service will allow approved government agencies to check online in real time whether a document presented to them as a proof-of-identity was issued by an appropriate department or agency, and that the details on the document are accurate. The data integrity pilot is designed to identify key data-matching

elements that could be used to improve the accuracy of identity information held on government databases.

The NISS will also be underpinned by an Intergovernmental Agreement on Identity Security that will establish an agreed set of high-level standards to govern the issue of identity documents and governance of identity systems across jurisdictions. It will contain agreements on enrolment procedures, security features and technologies embodied in key documents, as well as on shared use of document verification and authentication systems.

### **National Document Verification Service**

The Australian Government announced in the 2006–07 Budget that the identity of Australians will be further protected with the rollout of the national Document Verification Service (DVS). Funding of \$28.3 million has been allocated to develop and implement the national DVS.

The DVS will be a secure electronic national online system accessible by all key Commonwealth, state and territory government agencies, and potentially by the private sector. This service will allow authorised government agencies to check key identity documents presented by individuals applying for high-value benefits and services.

### **e-security**

Like all countries, Australia's capacity to participate in the global economy increasingly depends on information communications technologies. Our growing dependence on the information economy increases our vulnerability to acts of cyber-terrorism and other e-security threats.

The online security environment has changed significantly since 2001, with the emergence of new technologies and more sophisticated e-security threats. The government is committed to building a robust e-security policy framework to maintain a secure online environment that promotes trust and confidence in the information economy. This framework is designed to:

- enhance e-security awareness and practices amongst home users and the business community
- promote the security of Australia's national information infrastructure through information sharing and collaboration with the private sector
- ensure the government's electronic systems are appropriately secure
- promote the security of the global information economy through international engagement.

### ***National information infrastructure***

Australia's national information infrastructure consists of those critical infrastructure systems that underpin a range of day-to-day activities. These systems include banking and finance, telecommunications, energy and utilities and emergency services. Responsibility for the protection of this infrastructure is shared between the private sector, which owns most of it, and the government. The Australian Security Intelligence Organisation (ASIO), Defence Signals Directorate (DSD) and Australian Federal Police (AFP) have formal arrangements for identifying, assessing and responding to threats to Australia's national information infrastructure.

The *Cybercrime Act 2001* gives federal law enforcement agencies the authority to investigate and prosecute groups who use the internet to plan and launch cyber-attacks that could seriously interfere with the functioning of the government, financial sector and industry. A suite of offences, with tough penalties, provides a strong deterrent to people who engage in cyber-attacks, such as hacking, computer virus propagation and denial of service attacks.

The Australian Government has also established the Computer Network Vulnerability Assessment Programme, which provides co-funding on a dollar-for-dollar basis to help owners and operators of critical infrastructure identify major vulnerabilities within computer systems and dependencies between computer networks, and to test the ability of systems to resist exploitation.

Australia is also working internationally to improve our ability to manage cyber-attacks and cyber-crimes. The government participated in Exercise Cyberstorm, a multi-jurisdictional international exercise coordinated by the United States Department of Homeland Security. The exercise simulated a cyber-attack by a politically motivated group and tested our e-security systems and capabilities.

The international community of Computer Emergency Response Teams (CERTs) plays an important role in the global effort to keep computer systems secure from e-security threats and vulnerabilities. Australia's team, known as AusCERT, is a not-for-profit body operated by the University of Queensland. To enhance Australia's CERT capability, the Australian Government Computer Emergency Readiness Team (GovCERT.au) has been established in the Attorney-General's Department. GovCERT.au develops and coordinates government policy for computer emergency preparation, preparedness, response, readiness and recovery for major national information infrastructure incidents. It also acts as a point of contact within the Australian Government for foreign governments on CERT issues, and coordinates any foreign government requests.

Australia is leading an Asia-Pacific Economic Cooperation (APEC) initiative to build CERT capacities in developing economies. Working through APEC's Telecommunications and Information Working Group, the Attorney-General's Department has sponsored CERT training in Mexico, Chile and Peru. It has obtained funding to provide CERT training to Papua New Guinea, the Philippines, Thailand, Vietnam and Indonesia. Other international activities include strengthening our bilateral linkages with the United States and ongoing work with the Organisation for Economic Co-operation and Development (OECD) to implement national information infrastructure protection and risk-mitigation initiatives.

### **Australian High Tech Crime Centre**

The Australian High Tech Crime Centre, hosted by the AFP, is the main national-level law enforcement body involved in the investigation of e-security incidents in public and private sector organisations. The Centre performs a national coordination role for the law enforcement effort in combating serious, multi-jurisdictional crime involving complex technology. In addition to state and territory police forces, the Centre has secondees from a range of relevant Australian Government agencies and AusCERT. The Centre's multi-agency approach has consolidated and strengthened Australia's investigative capability.

### **Chemical, biological, radiological and nuclear security**

Terrorist interest in chemical, biological, radiological and nuclear (CBRN) weapons remains a concern. Although explosives are the most common terrorist weapon, attempts have been made by Al Qaida and others to acquire and develop CBRN materials for use in attacks. In response, governments are seeking to protect against the potential 'leakage' of CBRN materials and expertise from military and civilian facilities to terrorist groups as a result of poor security, theft or official corruption.

A successful CBRN attack would have serious consequences. The government is making every reasonable effort to prepare for and prevent such an attack, and to ensure that it has adequate capability to both respond to and recover from such an attack should it take place.

#### ***National CBRN security strategy***

Following the agreement reached by the Council of Australian Governments (COAG) in September 2005, a national CBRN security strategy is being developed by the National Counter-Terrorism Committee to enhance the protection of Australians and Australian interests from CBRN threats.

The security strategy is whole-of-government in nature and focuses on terrorist CBRN threats. The main focus of the strategy is on domestic capabilities. It recognises that the Commonwealth is responsible for national policy coordination and the international elements of CBRN issues, as well as CBRN incidents in its areas of responsibility. State and territory governments have primary operational responsibility to respond to CBRN threats and incidents in their jurisdictions. The Australian Government is also working with regional and international partners to ensure that CBRN materials are not accessible to terrorist groups.

The strategy relies on security intelligence and advice from ASIO to inform the government of the nature of CBRN terrorist threats. The CBRN Data Centre provides technical intelligence advice on the nature of CBRN agents that terrorists may seek to develop as weapons.

The strategy is being developed as an integral component of existing counter-terrorism and emergency management, health and agriculture arrangements. It seeks to accommodate the preventative measures needed to secure CBRN material without restricting legitimate users' access to, or movement of, those materials.

### **CBRN Data Centre**

The Australian CBRN Data Centre was established by the Australian Government within the AFP as part of the national response to CBRN threats. The centre provides a coordinating function for information relating to the potential use of CBRN materials, including by terrorists. Key aspects of the charter of the CBRN Data Centre are:

- provision of national real-time technical information and advice within the existing counter-terrorism arrangements in support of operations, intelligence and occupational health and safety for government and relevant parts of the private sector
- identification of key policy issues and provision of strategic advice to government
- provision of information for outreach and education programmes
- support and regular review of the lists of hazardous materials identified by the COAG Review of Hazardous Materials
- support to the National Institute of Forensic Science in the establishment of the Chemical Warfare Agent Laboratory Network.

### ***Review of hazardous materials***

In December 2002, COAG agreed to a national review of the regulation, reporting and security surrounding the storage, sale and handling of hazardous materials, with the aim of minimising the risk of these materials being used for terrorist purposes. The review seeks principally to identify a list of hazardous materials of security concern and develop controls that balance security concerns against the legitimate needs of users. The list consists of four parts:

- ammonium nitrate
- radiological sources
- harmful biological materials
- hazardous chemicals.

The review of ammonium nitrate has been completed and is being implemented. The review of radiological, biological and chemical materials is continuing.

### ***Chemical Warfare Agent Laboratory Network***

The Chemical Warfare Agent Laboratory Network is a network of accredited laboratories designed to be capable of conducting analysis of suspected chemical warfare agents and/or their precursors. Its aim is to provide a local facility for the initial analysis of such agents. The network is being developed under the guidance of the National Institute for Forensic Science with the support of the Defence Science and Technology Organisation (DSTO), which retains national centre of excellence status for the analysis of these agents and materials. The network consists of government laboratories in each state or territory.

### *Proliferation Security Initiative*

The Proliferation Security Initiative (PSI) is a practical response to the growing challenge posed by the worldwide spread of weapons of mass destruction (WMD) and their delivery systems and related materials. PSI aims to prevent illicit WMD-related trade to and from states of proliferation concern and terrorist groups through increased cooperation between participant states and harmonisation of domestic legal frameworks. The initiative was launched by US President Bush in May 2003. In addition to the United States, participants include Australia, Canada, France, Germany, Italy, Japan, the Netherlands, Norway, Poland, Portugal, Russia, Singapore, Spain and the United Kingdom. More than 70 countries have expressed their support for the initiative.

Under the initiative, countries agree to work together within the bounds of existing domestic and international law to disrupt the illicit trade in WMD, including by interdicting vessels, aircraft or other modes of transport in their territory or territorial waters that are reasonably suspected of carrying suspicious cargo. In October 2003, the United States, United Kingdom, Germany and Italy, acting under the auspices of the PSI, stopped an illegal cargo of centrifuge parts for uranium enrichment destined for Libya.

Australia has been a key driver of the initiative since its inception, and has actively participated in all PSI meetings. Australia hosted and chaired the second plenary meeting in Brisbane in July 2003, which advanced an operational framework called the Statement of Interdiction Principles. The Statement was formally adopted at the third plenary meeting in Paris in September 2003.

Australia led the first interdiction training exercise, the highly successful Pacific Protector, in the Coral Sea in September 2003. In April 2006, Australia hosted Exercise Pacific Protector 06, a mock air interdiction. The exercise involved 17 Australian Government departments and agencies, as well as the United States, United Kingdom, New Zealand, Singapore and Japan.





## **Security-related science and technology research**

Science and technology, which fuel much of Australia's prosperity and social progress, also form part of the dynamic mix of counter-terrorism capabilities at our disposal. The application of a strong and focused science and technology programme has benefits across the whole spectrum of prevention, preparedness, response and recovery.

Australian Government agencies are increasingly harnessing science, engineering and technology capabilities to provide solutions to a wide range of national security threats and vulnerabilities as the threat from terrorism evolves and becomes more complex. Australia has a strong and diverse national research base housed in the Commonwealth, state and territory government agencies, universities and the private sector.

Australia's research community is developing a range of new technologies to help meet modern security challenges, including:

- detection of explosives
- protection of people and equipment in the event of an incident
- forensic analysis
- critical infrastructure protection.

The Australian Government promotes collaboration on research on terrorism through the National Security Science and Technology (NSST) Unit in the Department of the Prime Minister and Cabinet, the Safeguarding Australia national research priority, and programmes such as the Publicly Funded Agencies Collaborative Counter-Terrorism Research Programme.

### ***National Security Science and Technology Unit***

The NSST Unit provides strategic coordination of scientific research and support for counter-terrorism within the Australian Government and across Australia. The Unit actively supports a range of research projects with other agencies through its Research Support for Counter-Terrorism programme. The objective of the programme is to commission and deliver strategically focused research and development to enhance our national counter-terrorism capabilities. The programme brings together specialists in the Australian science and technology community to collaborate with the counter-terrorism community.

The NSST Unit also manages our international collaborative arrangements to improve access to the benefits of international research, for Australia. To this end, the NSST Unit is responsible for:

- the Treaty-level Agreement between the United States of America and Australia on Cooperation in Science and Technology for Homeland/Domestic Security Matters
- the Memorandum of Understanding for Combating Terrorism Research and Development, signed by the Department of Defense of the United States of America and the Australian Government Department of the Prime Minister and Cabinet.

The NSST Unit has connections with universities, private research bodies and Australian Government research agencies, such as the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and the Defence Science and Technology Organisation (DSTO).



### **National Security Science and Technology Unit**

The NSST Unit has four broad capability areas focused on delivering enhanced capabilities to Australian Government security departments and agencies. These capability areas are:

- chemical, biological, radiological and nuclear (CBRN): research into real-time, broad-spectrum detection technologies; technologies for the decontamination of people, equipment and facilities; and technological developments in the protection of first responders and the general public
- explosives: enhancing Australia's capability to prevent, respond to, and recover from the threat of Improvised Explosive Devices, focusing on improved explosive detection, blast mitigation and render safe such devices
- physical and information security: enhancing the protection of Australia's critical infrastructure, focusing on screening technologies for transport, improvements in infrastructure modelling, identity management and the protection of physical and information infrastructure
- intelligence, surveillance and operations: advancing Australia's capacity to provide situation awareness in order to prevent, respond to, and recover from a terrorist threat, including developing Australia's ability to collect, analyse and disseminate intelligence, and to provide forensic analysis and tactical response.

## RESPONSE AND RECOVERY

Response and recovery refer to the range of measures undertaken to address the short and long-term consequences of a terrorist incident. Foundations for these measures are often in place well before a terrorist incident occurs, and may be linked with, or flow from measures taken in the prevention and preparedness phases of the counter-terrorism planning continuum.

Key aspects of response and recovery include:

- first response arrangements
- defence support
- public health
- recovery arrangements
- the prepared and resilient community.



## First response arrangements

In Australia, state and territory governments and their agencies, particularly state and territory police and emergency services, are responsible for operational response to terrorist incidents occurring in their jurisdictions. These responses are, in many cases, 'all hazards' in nature and largely replicate responses to non-terrorism-related criminal acts or disasters. Since 2001, state and territory governments have invested considerable resources to enhance and test their first response capabilities.

Commonwealth agencies provide support to the states and territories as requested and appropriate to the nature of the incident. Emergency Management Australia (EMA) is the lead Commonwealth agency involved in consequence management.<sup>3</sup> It works closely with other Commonwealth agencies—particularly the Department of the Prime Minister and Cabinet, the Protective Security Coordination Centre (PSCC), the Australian Federal Police (AFP), Australian Security Intelligence Organisation (ASIO) and the Australian Defence Force (ADF)—as well as state and territory police forces, fire and ambulance services, emergency services and public health authorities to ensure that appropriate consequence management arrangements are established to support the affected states and territories.

At the request of the affected state or territory, the Australian Government may also provide other, more specialised, operational support from agencies such as the Department of Immigration and Multicultural Affairs (DIMA), Department of Transport and Regional Services (DOTARS), Customs and the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA).

The primary goals across levels of government in the aftermath of a terrorist incident are to:

- minimise the loss of life
- minimise damage to critical infrastructure and vital national assets
- prevent further attacks
- conduct investigations to arrest those responsible for the attacks
- manage a rapid and effective recovery.

As soon as there is reasonable suspicion that an incident is terrorism-related, state or territory police will assume control of the incident site, and the PSCC will be notified. The response arrangements as outlined in the National Counter-Terrorism Plan (discussed in Part I) are then activated.

The Australian Government supports a comprehensive approach to emergency management through three key interdepartmental mechanisms. These are:

- the Australian Emergency Management Committee (AEMC), Australia's peak consultative emergency management forum. It is chaired by the Secretary of the Attorney-General's Department and comprises chairpersons and executive officers of state and territory emergency management committees and the President of the Australian Local Government Association. The AEMC provides advice and direction on

<sup>3</sup> Consequence management refers the measures taken to protect public health and safety, restore essential government services and provide emergency relief to government, businesses and individuals affected by the consequences of natural or man-made disasters, including terrorism.

the coordination and advancement of Commonwealth, state and territory interests in emergency management issues.

- the Australian Government Counter-Disaster Task Force, which is chaired by the Department of the Prime Minister and Cabinet, and consists of representatives of Australian Government agencies with a significant role in the provision of disaster/emergency relief or rehabilitation assistance
- the Australian Government Disaster Recovery Committee, which is chaired by the Department of Families, Community Services and Indigenous Affairs (FaCSIA), and consists of representatives of Australian Government agencies and ex officio representatives, including a state or territory government representative, all with significant roles in the provision of disaster recovery assistance.

## **Defence support**

The first responsibility of the Australian Government is to protect Australia, its people and interests. Defence contributes a range of capabilities to a comprehensive, nation-wide approach to counter-terrorism.

### ***Defence policy***

Australian defence policy has two major imperatives with respect to counter-terrorism:

- to shape and build a defence capability that is potent, appropriately structured, versatile and adaptable, and which links easily with other arms of the Australian Government
- to build strong security relationships both regionally and globally, consistent with Australia having a capacity to lead or contribute to coalitions.

Maintaining and supporting the primacy of the civil authority in a domestic security incident is the cardinal principle governing defence assistance in an emergency.

Use of the military on Australian sovereign territory is governed by legislation and intergovernmental agreements. Part IIIAAA of the *Defence Act 1903* governs the use of the ADF in situations where the use of force is likely. The use of the ADF in such circumstances is strictly limited. The ADF can only be called out in an incident that is beyond, or is likely to be beyond, the capacity of the civil authorities to resolve. The guidelines for these call-out arrangements are:

- the civil authority has primacy
- the ADF is used as a last resort
- the military chain of command is retained
- ADF personnel remain subject to the law and accountable for their actions
- the authorised use of force is reasonable and necessary.

### **Defence call-out**

Part IIIA of the *Defence Act 1903* provides a clear legislative basis for the use of the ADF as a last resort in aid to the civil authority to protect the interests of the Commonwealth, states and territories against domestic security incidents in Australia.

In 2006, the government amended Part IIIA of the Act to meet the needs of the current security environment. The key amendments were designed to:

- improve coordination mechanisms for responding to a terrorist incident
- enhance operational flexibility for situations in which the ADF may be required to respond to domestic security incidents to support civil authorities
- clarify the legal powers and protections for ADF personnel when they are conducting operations in support of domestic security.

The amendments also expand the circumstances under which the ADF can provide assistance to the civil authorities, such as aviation and maritime security and the protection of critical infrastructure where there is a direct or indirect threat to life.

### ***Defence capabilities***

There has been significant investment in the capacity of the ADF to respond to the terrorist threat since 11 September 2001. Defence is enhancing command and control mechanisms to coordinate its domestic security capability, doctrine, tactics, training and procedures.



Department of Defence

Potential Defence responses could involve recapturing buildings, freeing hostages, cordoning off areas or responding to a chemical, biological, radiological, nuclear or explosive attack. They could also involve the protection of designated critical infrastructure, offshore security and aspects of aviation security.

The Army contributes special forces, helicopters and heavy-lift capabilities to meet Australia's counter-terrorism needs. For example:

- The Incident Response Regiment is able to respond to chemical, biological, radiological, nuclear or explosive incidents both domestically and in support of Australian forces deployed overseas in high-threat environments. The Regiment includes intelligence, signals, medical, ordnance, transport, electrical and mechanical engineers, scientists and catering officers.
- The Tactical Assault Group provides a world-class counter-terrorism capability to react at short notice to state or territory requests for support made to the Australian Government. The Group conducts offensive and recovery operations including recapturing structures, freeing hostages and supporting high-risk search teams.
- The Reserve Response Force was established to enhance the ADF's domestic security capabilities. It undertakes support tasks such as establishing cordons, providing technical, administrative, logistics and communications support to standing civil command and control arrangements, static protection, vehicle and facility searches and traffic control.

## **Public health**

A terrorist attack against Australians or Australian interests would almost certainly result in physical and/or psychological harm to individual Australians and Australian communities. Accordingly, Australia's health system plays a major part in our national counter-terrorism response arrangements.

State and territory governments are primarily responsible for delivering health services. State disaster planning assets such as the National Trauma Centre at the Royal Darwin Hospital, which responded effectively to both the 2002 and 2005 Bali bombings, are critical to the national public health response capacity.

The Office of Health Protection, established in 2006 within the Department of Health and Ageing (DoHA), provides national health infrastructure for improving Australia's ability to respond to significant health threats, including terrorism. DoHA partners with other Commonwealth agencies and state and territory health departments to build and strengthen national emergency health plans and deliver a nationally coordinated health response in the event of a terrorist incident. This response is supported by national disease surveillance and early warning systems.

The private health sector also has an important role in counter-terrorism planning in Australia. The Health Infrastructure Assurance Advisory Group forms part of the Trusted Information Sharing Network, and provides a forum for sharing information on private health sector threats, vulnerabilities and risk mitigation. The Group's membership includes private hospitals, pathology laboratories, blood and pharmaceutical suppliers and DoHA representation.

The Australian Government has measures and mechanisms in place to support the protection of human health from a wide range of threats. These include:

- the Australian Health Protection Committee
- the National Health Incident Room
- the National Medical Stockpile
- regular public health emergency exercises.

### ***Australian Health Protection Committee***

The Australian Health Protection Committee (AHPC) helps maintain cross-jurisdictional coordination and planning arrangements, and enables the Commonwealth to work with state and territory governments to boost overall national response capacity during and in the aftermath of a terrorist incident. Chaired by a Deputy Secretary of DoHA, the AHPC consists of public health experts, jurisdictional Chief Health Officers, key Commonwealth agencies such as Emergency Management Australia and the Department of Defence and specialists in mental health, burns and disaster management.

The AHPC is charged with identifying Australia's level of preparedness to respond to the consequences of a deliberate or naturally occurring disaster and to coordinate the national health response. As well as meeting regularly to plan and develop health emergency policy, the AHPC and its subcommittees—the Communicable Diseases Network of Australia, the Environmental Health Committee and the Public Health Laboratory Network—have the ability to support health system surge response, both locally and nationally.

The AHPC coordinated planning and response for the treatment of people affected by the Bali bombings, the Indian Ocean tsunami, the Java earthquake and the recent evacuation of people from East Timor following the outbreak of severe civil unrest. Following the 2004 Madrid and 2005 London terrorist attacks, the AHPC conducted comprehensive debriefing at all levels of government and undertook audits of Australia's health emergency response capability.

### ***National Incident Room***

The DoHA National Incident Room, established following the Bali bombings, enables efficient coordination of the department's emergency response capacity and provides a capability for rapid liaison with other Commonwealth agencies, state and territory health authorities and international agencies such as the World Health Organization. The National Incident Room has a key role in coordinating the national health response to local/national/international disasters through deployment of disaster medical assistance teams. In recent months Australian Disaster Medical Assistance Teams were deployed in response to the Java earthquake and following the Indian Ocean tsunami.

The AHPC is developing a national structure for Disaster Medical Assistance Teams to enhance Australia's capacity to deploy teams nationally or internationally. DoHA is also developing a list of disaster medical supplies for emergency use by Teams in response to health disasters in Australia and overseas. It will work with the AHPC on the composition and location of strategic caches of medical and pharmaceutical supplies for use in an emergency.

### ***National Medical Stockpile***

The National Medical Stockpile was established in 2002 in response to the potential threat of bioterrorism and the enduring threat of a global outbreak of pandemic influenza. Since this time the Australian Government has allocated more than \$345 million for the Stockpile.

The contents of Australia's Stockpile are consistent with those of stockpiles held in other countries. Items for purchase are determined by an advisory committee with broad representation, using information about specific risks from intelligence sources, appropriate clinical data and the impact of the agent.

Deployment plans are being finalised and tested for getting stockpile supplies out to states and territories within 24 hours of a request being approved by the relevant Chief Medical Officer.

### ***Public health exercises***

DoHA participates in the national counter-terrorism exercise programme along with state and territory health and emergency services. The health system was tested in Mercury 05, a national multi-jurisdictional counter-terrorism exercise with a focus on mass casualties. Mercury 05 demonstrated how emergency management arrangements can be activated in a disaster during the surge phase (the first 12 hours after a disaster) to enhance overall capacity when operating within a nationally coordinated framework. Another Mercury exercise will be conducted in 2008.

In the meantime, a number of 'investigation and consequence management' exercises are being held in 2006 in states and territories, involving their health systems. A major national pandemic influenza simulation was conducted by DoHA in October 2006. While an outbreak of pandemic influenza is unlikely to occur due to a deliberate terrorist act, DoHA will nonetheless exercise the same health systems and intra- and intergovernmental decision-making processes that will be called on in a terrorist attack. The lessons learnt will be invaluable for the continuous task of reviewing and improving national health emergency preparations and response capabilities.

### ***Recovery arrangements***

Recovery is the coordinated process of supporting communities affected by disasters or emergencies, including terrorist incidents, in the reconstruction of the physical infrastructure and the restoration of their emotional, social, economic and physical wellbeing.

Recovery incorporates consequence management and extends to the long-term rebuilding of a community. Invariably, recovery involves close community consultation and participation. Effective recovery programmes address five key interrelated elements in supporting individuals and communities to manage their own recovery:

- community recovery, which involves rebuilding community bonds and identity following emergencies
- psychosocial recovery, which addresses the major personal stresses caused by traumatic events



- infrastructure recovery, which aims to restore both public and private infrastructure disrupted by accidents, natural disasters or terrorism
- economic recovery, which touches on the various economic impacts of emergencies for individuals and communities
- environmental recovery, which tackles aspects such as air quality, water quality, soil contamination and the aesthetic quality of the affected environment.

Recovery is planned for and managed in a structured manner. The broad needs created by the impact of a terrorist incident on a community can only be met through a range of integrated services. These are provided by a combination of government and non-government organisations.

### ***State and territory recovery arrangements***

Recovery arrangements are based on the well developed emergency management arrangements of state or territory governments and a series of less formal links between agencies and organisations with a role in recovery. These arrangements have proved effective; they are internationally recognised and reflect the experience of government and non-government organisations over many years. The existing arrangements were initiated to formalise support services following events such as bushfires, cyclones or floods.

The nature of recovery activities remains relatively consistent. Events such as the 2002 and 2005 Bali Bombings and 2006 Cyclone Larry have demonstrated that individual and community impacts and needs are similar for natural, man-made or terrorist incidents—all resulting in complex, lengthy and resource-intensive recovery programmes.

State and territory recovery committees comprise representatives from the state or territory government, local government agencies, non-government organisations and when required, the Australian Government. The role of a state or territory committee includes:

- developing policy on recovery management planning and operations
- overseeing the implementation of recovery policy throughout the state or territory
- providing advice to government
- preparing state or territory plans
- monitoring agency preparedness.

### ***Local level***

The focus of recovery planning and management at the local level is on community input. Most local government authorities also provide a range of human and community services to individuals and the community.

### ***Australian Government level***

While primary responsibility for disaster recovery rests with the states and territories, the Australian Government is committed to supporting the states and territories to develop their capacity for dealing with emergencies and disasters. When states or territories cannot reasonably cope in an emergency, they may, and routinely do, request assistance from the Australian Government. The Australian Government supports a

comprehensive approach to emergency management through Emergency Management Australia and through recovery efforts supported by the Australian Government Disaster Recovery Committee.

The role of Australian Government agencies has generally been one of support for the jurisdiction(s) involved. However, in the recovery process following the 2002 Bali bombings, Australian Government agencies and a number of national non-government organisations performed a significant role. The attack affected Australians from a number of jurisdictions, and necessitated coordination of recovery and support services at the Australian Government level, through the Department of Families, Community Services and Indigenous Affairs and Centrelink.

### ***Terrorism insurance***

The Australian Government established a terrorism insurance scheme to minimise the wider economic impacts that flowed from the withdrawal of terrorism insurance following the terrorist attacks on 11 September 2001.

The scheme began on 1 July 2003 and applies to insurance for commercial property in Australia and associated business interruption losses and public liability claims. It operates by deeming terrorism exclusions in eligible insurance contracts to have no effect. In turn, insurers can reinsure relevant terrorism risks with the Australian Reinsurance Pool Corporation.

A review of the scheme in 2006 concluded that there was still a need for the scheme to continue given that insufficient terrorism insurance is currently available commercially on reasonable terms.

### **The prepared and resilient community**

Australia's approach to emergency management is designed to ensure that the efforts of all relevant government agencies at all levels, organisations and affected communities can be coordinated effectively in the development of safer and more resilient communities. When major emergencies or disasters, including terrorism, occur, individual and community self-help can often provide the most readily available and effective means of recovery, as assistance from external sources may be limited or delayed by competing demands on resources. This is particularly true for remote communities.

Local government and community organisations, with their understanding of local needs and capabilities, provide a ready basis for organising effective and immediately available community self-help. The key requirements for a prepared community are:

- alert, informed and active citizens
- effective community organisations with identified and positive roles in local emergency management arrangements
- local governments that acknowledge their lead roles in community safety issues, and which have well established, widely understood and well practised arrangements for discharging their community safety responsibilities.

Individuals, for their part, can do much to help themselves and others in their community by:

- being aware of local hazards and the risks that may result from them
- taking appropriate individual precautions against such risks
- being actively involved in community-based voluntary organisations
- helping to ensure that local government has effective arrangements in place.

### ***Volunteers and the prepared community***

Local volunteer organisations, when effectively integrated into local emergency management arrangements, can play a vital part in emergency management at the community level. They can provide a community with additional resources and expertise, and can act as a link in the information chain between the affected community, local government and emergency management agencies.

More than 500 000 volunteers are involved in the emergency management sector in Australia. These volunteers provide response and recovery services associated with approximately 80 per cent of major emergencies in Australia, whether natural or man-made. They are an integral part of Australia's local recovery programmes in all states and territories. In 2004 the Australian Government announced the Working Together to Manage Emergencies initiative that provided \$49 million over four years to local governments and volunteer organisations, to help them to better prepare to deal with emergencies or disasters.

## AUSTRALIA'S FUTURE CAPABILITY

Terrorism requires us to maintain a clear strategic focus, underpinned by robust and sustainable capabilities. Australia's enduring national counter-terrorism aim is to protect Australians and Australian interests. The Australian Government will continue to seek to achieve this by:

- working with state, territory and local governments, businesses and the community to build an effective nation-wide counter-terrorism capability
- contributing to regional and wider international counter-terrorism efforts.

The pursuit of these objectives will continue to be guided by the principles of constitutionality, proportionality, comprehensiveness and sustainability.

The Australian Government has systematically reviewed the critical components of Australia's strategy against terrorism. The best weapon against terrorism is prevention, which is necessarily intelligence-led. The government has refined the national strategic counter-terrorism framework to put in place comprehensive prevention and preparedness capabilities, and effective response and recovery capabilities. A great deal has already been done at all levels of government, by the private sector and by members of the public to give effect to these priorities.

### *Planning for the future*

Australia cannot be complacent. The terrorist threat to Australia is very real and will be with us for some time. The legislative framework put in place with broad parliamentary support and the additional resources committed by the Australian Government since 2001 have provided a sound foundation for countering the threat of terrorism for many years to come. The key principles underpinning the government's planning for the future are:

- intelligence capability that can provide comprehensive and accurate assessments about the threat we face
- sound risk-management approaches that deliver the maximum level of security by making best use of the resources available to us
- a coordinated approach to developing our counter-terrorism arrangements and capabilities across the whole of government
- effective partnerships with the states and territories and the private sector and continued engagement of the Australian public in the counter-terrorism effort
- close regional and international cooperation in ways that complement and strengthen our capacity to fight terrorism.

Taken together, these elements provide for a strong and flexible national counter-terrorism framework that allows for an appropriate and resolute response to the terrorist threat. There can be no guarantees that we will always be able to prevent an act of terrorism. That said, the Australian Government will continue to take resolute action, domestically and internationally, to advance our national interests, to counter the threat of terrorism and prevent those who seek to endanger the lives of our citizens from achieving their goals.

## Acronyms

---

ADF	Australian Defence Force
AEMC	Australian Emergency Management Committee
AFP	Australian Federal Police
AGCTC	Australian Government Counter-Terrorism Committee
AGD	Attorney-General's Department
AHPC	Australian Health Protection Committee
AIC	Australian intelligence community
ALGA	Australian Local Government Association
APEC	Asia-Pacific Economic Cooperation
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
BPC	Border Protection Command
CBRN	chemical, biological, radiological and nuclear
CCTV	closed-circuit television
CERT	Computer Emergency Response Team
CIPMA	Critical Infrastructure Protection Modelling and Analysis
COAG	Council of Australian Governments
CSIRO	Commonwealth Scientific and Industrial Research Organisation
Customs	Australian Customs Service
DFAT	Department of Foreign Affairs and Trade
DIGO	Defence Imagery and Geospatial Organisation
DIMA	Department of Immigration and Multicultural Affairs
DIO	Defence Intelligence Organisation
DoHA	Department of Health and Ageing
DOTARS	Department of Transport and Regional Services
DSD	Defence Signals Directorate
DSTO	Defence Science and Technology Organisation
DVS	Document Verification Service
EEZ	exclusive economic zone
EMA	Emergency Management Australia
FaCSIA	(Department of) Families, Community Services and Indigenous Affairs
IGIS	Inspector-General of Intelligence and Security
ISPS	International Ship and Port Facilities Security (Code)
JCLEC	Jakarta Centre for Law Enforcement Cooperation
JI	Jemaah Islamiyah
MOU	memorandum of understanding
NATO	North Atlantic Treaty Organisation
NCTC	National Counter-Terrorism Committee
NCTP	National Counter-Terrorism Plan
NISS	National Identity Security Strategy
NSC	National Security Committee of Cabinet
NSST	National Security Science and Technology (Unit)
OECD	Organisation for Economic Co-operation and Development
ONA	Office of National Assessments
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PSCC	Protective Security Coordination Centre
PSI	Proliferation Security Initiative
TISN	Trusted Information Sharing Network
WMD	weapons of mass destruction

# Index

---

- Advance Passenger Processing 50
- Airline Liaison Officer 50
- Al Qaida 1, 8, 9, 10, 11, 26, 62
- Ambassador for Counter-Terrorism 2, 22
- Anti-Terrorism Act 3, 33
- Asia-Pacific Economic Cooperation 22, 61
- Attorney-General's Department 4, 17, 37, 42, 45, 46, 56, 61, 68
- Australian Bomb Data Centre 43
- Australian Customs Service 4, 42, 49, 50, 51, 52, 53, 55, 68
- Australian Defence Force 22, 41, 51, 52, 68
- Australian Emergency Management Committee 16, 68
- Australian Federal Police 3, 17, 34, 40, 42, 43, 49, 61, 68
- Australian Government Counter-Terrorism Committee 16, 17
- Australian Government Counter-Terrorism Policy Committee 16
- Australian Government Counter-Disaster Task Force 69
- Australian Government Disaster Recovery Committee 6, 69, 75
- Australian Health Protection Committee 6, 16, 72
- Australian High Tech Crime Centre 43, 62
- Australian intelligence community 3, 30, 37, 38, 39, 41, 42
- Australian Local Government Association 14, 16, 68
- Australian Quarantine and Inspection Service 52
- Australian Radiation Protection and Nuclear Safety Agency 68
- Australian Secret Intelligence Service 38, 40
- Australian Security Intelligence Organisation 21, 26, 30, 33, 36, 38, 39, 40, 42, 47, 61, 62, 68
- Australian Transaction Reports and Analysis Centre 42, 45
- Aviation Security Identification Card 4, 55, 56
- Aviation Transport Security Act 54
- Bali 8, 9, 10, 12, 14, 21, 44, 71, 72, 74, 75
- Border Protection Command 51, 52
- Border security 4, 14, 32, 40, 48, 49, 50
- Business Government Advisory Group 29, 46
- CBRN Data Centre 63
- Chemical Warfare Agent Laboratory Network 63
- Chemical, biological, radiological and nuclear 5, 10, 15, 32, 38, 62, 66, 71
- Chemical, biological, radiological and nuclear (CBRN) security 32, 62
- Closed circuit television 4, 15, 55, 58
- Commonwealth Scientific and Industrial Research Organisation 65
- Computer Emergency Response Team 61
- Council of Australian Governments 2, 14, 15, 16, 18, 28, 33, 58, 59, 62, 63
- Counter-Terrorism Intelligence Training Programme 21
- Counter-terrorism legislation 3, 32, 37
- Criminal Code Act 3, 33
- Critical infrastructure protection 3, 4, 16, 30, 32, 45, 46, 65
- Critical Infrastructure Protection Modelling and Analysis Programme 47
- Defence Imagery and Geospatial Organisation 38, 41
- Defence Intelligence Organisation 38, 41
- Defence Science and Technology Organisation 63, 65
- Defence Signals Directorate 38, 41, 61
- Defence support 5, 67, 69
- Department of Defence 72
- Department of Foreign Affairs and Trade 2, 17, 22, 26, 39, 40, 42, 53
- Department of Health and Ageing 6, 17, 71, 72, 73
- Department of Immigration and Multicultural Affairs 28, 42, 49, 50, 53, 68
- Department of the Prime Minister and Cabinet 5, 14, 17, 39, 65, 68, 69
- Department of Transport and Regional Services 17, 40, 42, 68
- Document Verification Service 4, 59, 60
- Electronic Travel Authority 49
- Emergency Management Australia 2, 5, 17, 68, 72, 75
- e-security 5, 32, 43, 60, 61, 62
- Families, Community Services and Indigenous Affairs 69, 75
- Flood Inquiry 38, 39
- Financial intelligence unit 45
- Health Infrastructure Assurance Advisory Group 71
- Incident Response Regiment 71

Identity security 4, 15, 32, 50, 53, 59  
 Indonesia 20, 22, 61  
 Infrastructure Assurance Advisory Group 47, 71  
 Inspector General of Intelligence and Security 39, 41, 42  
 International Ship and Port Facilities Security Code 57  
  
 Jakarta Centre for Law Enforcement Cooperation 21, 44  
 Jemaah Islamiyah 1, 9, 10, 20  
 Joint Counter-Terrorism Teams 3, 42, 43  
  
 Law enforcement 3, 4, 14, 19, 21, 28, 32, 42, 43, 44, 45, 50, 55, 59, 61, 62  
 London 8, 12, 14, 15, 18, 24, 26, 29, 33, 37, 44, 53, 72  
  
 Madrid 8, 18, 29, 37, 53, 58, 72  
 Maritime Security Identification Card 57  
 Movements Alert List 50  
  
 National Counter-Terrorism Alert Level 24, 25, 40  
 National Counter-Terrorism Committee 2, 5, 14, 15, 16, 46, 47, 48, 62  
 National Counter-Terrorism Plan 14, 15, 18, 54, 68  
 National Guidelines for Protecting Critical Infrastructure 3, 46  
 National Identity Security Strategy 4, 15, 50, 59  
 National information infrastructure 60, 61  
 National Medical Stockpile 72, 73  
 National Security Committee of Cabinet 16, 19, 38  
 National Security Hotline 18, 24, 25  
 National Security Public Information Campaign 2, 24  
 National Security Science and Technology Unit 5, 65, 66  
 National Terrorist Situation 17  
 National Threat Assessment Centre 40  
  
 Office of Health Protection 6, 71  
 Office of National Assessments 38, 39, 40  
 Office of Transport Security 54, 57  
 Organisation for Economic Cooperation and Development 61  
  
 Parliamentary Joint Committee on Intelligence and Security 36, 42  
 Proliferation Security Initiative 64  
 Protective Security Coordination Centre 17, 18, 68  
  
 Public health 5, 6, 33, 67, 68, 71, 72, 73  
  
 Regional Movement Alert System 53  
 Reserve Response Force 71  
  
 Science and technology research 5, 32, 65  
 Secretaries' Committee on National Security 16  
  
 Tactical Assault Group 71  
 Transport security 4, 16, 21, 32, 53, 54, 57, 58  
 Trusted Information Sharing Network 4, 30, 47, 71  
  
 United Kingdom 8, 21  
 United States 1, 2, 8, 11, 20, 21, 32, 41, 53, 61, 64, 65  
  
 Weapons of mass destruction 21, 39, 57, 64  
 Wheeler Review 4, 15, 55

## NOTES

---



## NOTES

---

