



## THE ATTORNEY-GENERAL'S PORTFOLIO

### **SECURITY ENVIRONMENT UPDATE**

The threat of terrorism remains real for all Australians. The events in New York, Bali, Madrid and London have changed the world forever and forced governments to continuously reassess their domestic national security strategies.

The Government's response to the terrorism threat continues to be decisive, comprehensive and proactive. The Government has already implemented more than 100 measures and injected additional funding in excess of \$6.7 billion since 2001–02 to fight terrorism and improve national security.

The National Counter-Terrorism Committee (NCTC) and National Counter-Terrorism Plan coordinate our domestic security arrangements. The Australian Government with State and Territory agencies is fully committed to an expanded capability development program which covers security, law enforcement, intelligence and emergency management. Australia continues to support its neighbours through regional capacity building and working with them in the development of regional counter-terrorism capabilities.

Intelligence resources have been increased, border security has been upgraded and new laws for maritime and aviation security made. The Government is tightening Australia's identity verification systems to make it harder for terrorists to cross borders and infiltrate security systems.

Comprehensive counter-terrorism legislation has been put in place to outlaw terrorist groups and terrorist financing.

### **ATTORNEY-GENERAL'S PORTFOLIO**

The Attorney-General's portfolio continues to play a lead role in ensuring Australia's counter-terrorism capabilities. There have been significant developments within the portfolio in response to this role. The 2006–07 Budget provides over \$1.2 billion to fund additional national security related measures in the Attorney-General's portfolio.

The Government has implemented new legislation to strengthen Australia's terrorism laws. Significant work has been undertaken to strengthen transport security and work is underway to address identity security.

The Government has enhanced its domestic focus on countering the financing of terrorism, and also made significant progress in cooperating with other countries to detect and prevent money laundering and terrorist financing.

## IDENTITY SECURITY

In the 2006–07 Budget, the Government has committed \$19.6 million over four years, for the establishment of three new multi-agency Identity Security Strike Teams (ISSTs), which will build on the success of the existing AFP-hosted Identity Crime Task Force. The ISSTs will provide significantly increased investigative focus on the growing area of identity crime - a significant criminal activity which cuts across a range of crime types and has the potential to conceal criminal identities, posing significant challenges to law enforcement and security agencies. Teams will include specialist investigative, intelligence and technical staff and will substantially increase the Australian Government's capability to detect, deter and investigate the manufacture and use of false identities.

The Attorney-General's Department continues to develop whole-of-government and cross-jurisdictional processes and open up dialogue with the private sector to explore:

- improved standards and procedures for enrolment and registration including identifying key proof-of-identity (POI) documents to be used by all appropriate organisations for the purposes of identifying and registering clients for services
- the identification of common advanced security features for inclusion on all key POI documents
- a secure national electronic document verification system for use by all key Commonwealth and State and Territory agencies
- development of a system to improve the accuracy of personal information held on government databases and to detect false identities and inaccurate records
- development of national authentication standards for physical and on-line transactions, and
- a supporting or enabling legislative regime, taking into account the need for appropriate privacy oversight and protection.

A central plank of the strategy is to provide authorised agencies with the ability to verify key identity documents presented by individuals when applying for high value benefits and services. In last year's Budget the Government committed \$5.9 million over two years to initiate the development of a national identity security framework that is strong, comprehensive and consistent. This included funding for a pilot prototype document verification service (DVS) to check Australian passports, Australian citizenship certificates, birth certificates and drivers' licences issued in Australia. The Government committed additional funding in the 2006-07 Budget totalling \$28.3 million to rollout a national service. The DVS will allow agencies to verify, online and in real time, that the details on these documents are accurate and also that the document is still valid. The DVS will also provide stolen and fraudulent document detection capabilities.

The Attorney-General's Department is also proceeding with another pilot from the 2005–06 Budget to examine measures for improving the accuracy of personal information held on existing government databases by identifying inaccurate records and false identities. Detailed technical and analytical papers have been completed for the conduct of the pilot and in-depth consultation is now occurring with Commonwealth and State agencies on the associated legal, privacy and technical issues.

The development of the identity security strategy will need to balance individual privacy and civil liberties with broader community interests. It involves consultation with the Privacy Commissioner and examination of the adequacy of national oversight and accountability arrangements to take account of cross-jurisdictional and public sector flows of personal information. New government identity documents, such as the new government services Access Card, will be developed to meet new identity security standards to protect the personal identity of individual and to deter fraud.

## LEGISLATION

Since 2001 the Australian Government has introduced extensive legislative measures addressing terrorism, national security and other multi-jurisdictional and transnational crime offences. This new legislation has been enacted to ensure Australia and Australians are protected from emerging threats. A review of national security legislative changes made since 2001 is available on the Attorney-General's Department's National Security website at [www.nationalsecurity.gov.au](http://www.nationalsecurity.gov.au).

During the past 12 months the Government has continued to build on and strengthen its national security legislation framework. In developing new legislation, the Government is always conscious to ensure that appropriate safeguards are put in place to maintain the balance between security and individual rights and freedom.

The following legislation has been passed in the last 12 months that will assist the fight against terrorism:

- The *Anti-Terrorism Act 2005* clarified that it is not necessary to identify a particular terrorist act to prove an offence of terrorism.
- The *Anti-Terrorism Act (No. 2) 2005* introduced a number of new counter-terrorism measures including:
  - an extension of the definition of a terrorist organisation to enable listing of organisations that advocate terrorism
  - introducing 'control orders' that will allow for terrorist suspects who pose a risk to the community to be closely monitored
  - creating a new police preventative detention regime that will allow detention of a person for up to 48 hours without charge where it is reasonably necessary to prevent a terrorist act or to preserve evidence of such an act
  - updated sedition offences to cover those who urge violence or assistance to Australia's enemies
  - introducing a new regime of stop, question, search and seize powers that will be exercisable at airports and other Commonwealth places to prevent or respond to terrorism
  - creating a legal basis for the use of video surveillance at Australia's major airports and on aircraft, and
  - implementing additional Financial Action Task Force Special Recommendations covering criminalising financing of terrorism, alternative remittance dealers, wire transfers and cash couriers.

Start up costs of \$10.5 million has been provided for 2006–07 for initial implementation of the *Anti-Terrorism Act (No. 2) 2005*. This funding will enable the ten relevant portfolio agencies to begin implementation of the two key sets of provisions in the Act—the control order and preventative detention regimes covering the application, hearing and enforcement of control orders and preventative detention orders, and the strengthened anti-terrorist financing regime, covering public and industry awareness campaigns about the new reporting requirements and staff to capture and analyse the newly reported data.

- The *Law and Justice Legislation Amendment (Video Link and Other Measures) Act 2005* was passed in November 2005 to facilitate the use of video link evidence from overseas witnesses in proceedings for terrorism and other related offences. The Act also facilitates the use of foreign materials such as video tapes and transcripts of examinations as evidence in terrorism and related proceedings when video link evidence is not possible.
- In March 2006, amendments to the *Telecommunications (Interception) Act 1979* implemented a number of recommendations from the report by Mr Anthony Blunn AO on his Review of the Regulation of Access to Communications. The amendments enable interception of communications of a person known to communicate with the person of interest, and introduce a warrant regime for access to stored communications held by a telecommunications carrier, through overt means. The amendments also enable interception of telecommunications services on the basis of the telecommunications equipment.
- In 2004, Mr Philip Flood AO conducted the Inquiry into Australian Intelligence Agencies and submitted his report to the Prime Minister in July 2004. The Government agreed to accept most of the recommendations of the Flood Inquiry. The *Intelligence Services Legislation Amendment Act 2005* implements legislative recommendations from the Flood Inquiry, as well as the outcomes from a separate review of the operation of the *Intelligence Services Act 2001*. Some of the recommendations implemented in this Act include extending the terms of reference of the Parliamentary Joint Committee on Intelligence and Security (PJCIS), as it is now re-titled, to include all Australian intelligence agencies; clarifying the roles and functions of the Australian Secret Intelligence Service and the Defence Signals Directorate, and clarifying the functions of the Inspector-General of Intelligence and Security.

Other legislative initiatives recently introduced into Parliament include:

- The PJCIS recently reviewed the operation, effectiveness, and implications of ASIO's questioning and detention powers under Division 3 Part III of the *ASIO Act 1979*. In response to the recommendations of the PJCIS, the government has introduced a bill into Parliament on 29 March 2006. The Bill will improve the clarity and operation of the questioning, and questioning and detention, warrant regimes, and will also clarify rights of persons questioned or detained under the regime. The Bill seeks to extend the sunset clause on the questioning and detention powers by 10 years until 2016.
- The *Maritime Transport and Offshore Facilities Security Amendment (Maritime Security Guards and Other measures) Bill 2005* was introduced into Parliament in June 2005. The Bill seeks to secure the integrity of Maritime Security Zones by increasing the statutory powers of maritime security guards to question and remove unlawful person, vehicles and vessels.

- The Convention on the Marking of Plastic Explosives for the Purpose of Detection and its National Interest Analysis was tabled in Parliament on 11 October 2005. The Convention is currently being reviewed by the Joint Standing Committee on Treaties prior to introduction of legislation to implement the Convention obligations in Australia.

The Australian Government is reviewing and developing other important aspects of our counter-terrorism legislative framework:

- The Australian Government is reviewing Australia's international extradition and mutual assistance in criminal matters arrangements. These reviews are an important part of the fight against transnational crime and terrorism because fighting crime requires strong and effective international crime cooperation arrangements with other countries. In December 2005 the Minister for Justice and Customs released a discussion paper on extradition. The policy objective of the extradition review is to ensure that criminals cannot evade justice simply by crossing borders.
- The Government is developing comprehensive Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) legislation that will update Australia's AML/CTF regime to reflect the most recent FATF recommendations. The legislation is being developed in consultation with Australia industry to ensure that it will be both practical and effective. AUSTRAC has received \$8.9 million for AML/CTF regulation implementation funding. This funding will, amongst other things, enable AUSTRAC to assist industry to comply with the proposed legislative changes and new obligations scheduled for 2006–07.

In 2005, 11 organisations were re-listed as terrorist organisations under the *Criminal Code Regulations 2002* and two new organisations were listed.

### **NATIONAL COUNTER-TERRORISM LEADERSHIP**

In September 2005, the Government revised the National Counter-Terrorism Plan (NCTP) which outlines responsibilities, authorities and the mechanisms to prevent or if needed, manage acts of terrorism and their consequences within Australia. The revision took account of the lessons learned from Australia's first multi-jurisdictional counter-terrorism exercise *Mercury 04* held in March 2004 and other developments in the national arrangements since the Plan was first launched in June 2003.

The NCTP is maintained by the National Counter Terrorism Committee (NCTC) which was established in 2002 following a high-level review of Australia's security and counter-terrorism arrangements the previous year. The role of the NCTC is to contribute to the security of the Australian community through coordination of a nation-wide cooperative framework between the Australian Government and States and Territories, to counter terrorism and its consequences. A further security review was undertaken in 2004 to validate the existing arrangements and to identify any areas where these could be further strengthened.

### *National Counter-Terrorism Exercises*

The NCTC's enhanced counter-terrorism capability development exercise program involves the Australian Government and all States and Territories. The program includes discussion exercises, tactical response exercises, investigation and consequence management exercises and multi-jurisdictional exercises. The Protective Security Coordination Centre (PSCC), within the Attorney-General's Department, is responsible for coordinating the exercises. They provide a strong framework for testing and evaluating Australia's counter-terrorism arrangements, at both the national and State and Territory levels.

### *Refocused Counter-Terrorism Exercise Program*

On 27 September 2005, a special COAG meeting on counter-terrorism agreed to refocus Australia's national counter-terrorism exercise program. The Australian Government subsequently committed \$9.3 million over four years from 2006–2007 for the implementation of the refocused program.

The refocused counter-terrorism program will put greater emphasis on exercising Australia's ability to manage mass casualty incidents, particularly in places such as transport hubs, major city precincts and other places of mass gathering. It will include a stronger focus on high profile exercising, the conduct of regular 'drill style' exercises in all major Australian cities and the engagement of communities, local government and the private sector.

### *Government Communications during a Crisis*

The Australian Government has committed \$20.3 million over four years from 2006–07 on measures designed to enhance government communications during a crisis. The measures include:

- a mobile telephone priority access system for key government personnel
- a service to facilitate messages to and from multiple government recipients
- a secure gateway to interconnect Government secure networks
- a national forum to share information and develop best practice for the dissemination of emergency warnings in Australia
- national media protocols for the request and broadcast of emergency warnings and announcements to the public, and
- an upgrade of the national security website [www.nationalsecurity.gov.au](http://www.nationalsecurity.gov.au).

### *Emergency Management*

The Australian Government, through Emergency Management Australia (EMA), supports a comprehensive approach to emergency management. EMA seeks to encourage an "all agencies", "all hazards" approach to the prevention or mitigation of disasters, preparedness for their impact, response to that impact and recovery from the consequences. In this way EMA works closely with security and law enforcement agencies to ensure that all agencies have complementary plans and arrangements so that, should there be an incident, the response will be efficient and effective.

Recognising the importance of a resilient, self-reliant community in emergencies, the Government provided a \$14 million boost in 2005–06 in the inaugural funding round of the Working Together to Manage Emergencies initiative. This initiative supports communities, local governments and volunteer organisations in the development of strategies to improve community safety and to improve training for volunteers involved in emergency management. In the coming financial year, more than 400 successful projects across Australia will receive grants designed to develop self-reliance at both the community and local government levels.

#### *The PSCC Watch Office*

The PSCC Watch Office is a dedicated national security coordination facility which operates 24 hours a day, seven days a week.

Under the National Counter-Terrorism Plan, the Watch Office performs a critical role in national crisis management arrangements which operate in the event of a threat or incident of terrorism. The Watch Office also forms the nexus of an established and effective national coordination and information-sharing network incorporating all Australian Government, State and Territory police and security agencies.

#### *National Security Hotline*

The National Security Hotline (1800 123 400) was established by the Australian Government in December 2002 to provide a single point of contact for members of the public wishing to provide information to government agencies regarding national security. The Hotline also provides information and reassurance to the public on the arrangements for preventing, deterring and detecting terrorism in Australia.

The Government's objectives in establishing the Hotline have been met, for example in the weeks prior to the Melbourne Commonwealth Games there was a significant increase in calls to the Hotline from members of the public providing security information. Since it was established the Hotline has received over 71,000 calls, of which more than 37,000 have provided authorities with information that has increased understanding of threats facing Australia. It is encouraging that so many Australians have taken the trouble to pass on their concerns to the authorities via the Hotline. The Government maintains its commitment to providing this important avenue for public input on national security.

#### *Chemical, Biological, Radiological and Nuclear Data Centre*

The Government provided funding over five years in September 2005 to establish a Chemical, Biological, Radiological and Nuclear (CBRN) Data Centre, as well as an enhanced national capability to analyse materials suspected of involving chemical warfare agents, the Chemical Warfare Agent Laboratory Network. The CBRN Data Centre will operate on a 24 hour, seven days per week basis, will be administered by the Australian Federal Police and be co-located with the Australian Bomb Data Centre. The Centre will be a contact point for CBRN technical issues and provide a mechanism for access to the expertise which presently exists within Australian Government Agencies and State and Territory facilities.

## *APEC 2007 Security Arrangements*

Australia is hosting the 2007 Asia Pacific Economic Cooperation (APEC) forum. The provision of security for APEC 2007 will be the most significant dignitary protection ever in Australia's history. There will be up to 100 days of ministerial, officials' and business meetings and events across Australia culminating in the leaders' week in Sydney. The Government previously provided funding of \$216.3 million over four years to cover organisational, logistical and security measures associated with APEC meetings and events to be held throughout 2007. As part of the Government's commitment to providing coordinated national security for this event, the PSCC is managing security arrangements. The APEC 2007 Security Branch has been created within PSCC to coordinate protective security arrangements in partnership with event host departments, Australian Government security service providers, and State and Territory police. Extra funding of \$22.7 million has been provided in the 2005–06 Additional Estimates, and \$70 million in the 2006–07 Budget, for specific security costs associated with the hosting of APEC Leaders' Week in Sydney in September 2007, including funding to cover APEC specific security costs incurred by the NSW Police Service.

Expert AFP personnel will be deployed to key APEC meeting sites, supported by the provision of criminal history checks, investigative, forensic and other security support services. The AFP will also provide a Firearms and Explosives Detector Canine capability for the 2007 APEC year, which will allow firearms and explosives searches to be conducted in support of the relevant State jurisdiction at the numerous meetings across Australia. ASIO is providing security advice and intelligence to police and Australian Government agencies involved in APEC security.

Responsibility for the development and delivery the whole-of-APEC integrated accreditation and access control system will be with the APEC Taskforce in the Department of Prime Minister and Cabinet. The system will integrate border control and other security checks, as appropriate, from several agencies. It will gain efficiencies by using tried and proven technology and include several levels of redundancy. To cope with changes in the threat or security environment, the system will be flexible to accommodate increased security measures that may be applied at short notice.

## **ASSISTING OUR NEIGHBOURS**

### *Strengthening regional legal frameworks*

Australia has a strong interest in promoting security in our region by helping neighbouring countries to develop comprehensive legal frameworks to counter terrorism.

In July 2005, the Australian Government established a specialist Regional Legal Assistance Unit within the Attorney-General's Department to assist countries in the South East Asian Region to develop legislation to implement their obligations under the international counter-terrorism instruments and related Security Council Resolutions, and to promote legal cooperation in the region. The Unit was established with funding provided in the 2005–06 Budget for a period of four years.

The Unit has assisted the Royal Cambodian Government to draft a comprehensive law implementing Cambodia's obligations under the international counter-terrorism instruments.

The Unit has also received requests from several other countries in the region and is working closely with those countries to identify the assistance they require.

In addition to this legislative and policy assistance role, the Unit is responsible for taking forward the work of the Bali Legal Issues Working Group (LIWG). The establishment of the LIWG (chaired by Australia) and the Law Enforcement Working Group (LEWG), chaired by Indonesia, was a key outcome of the Regional Ministerial Meeting on Counter-Terrorism held in Bali in February 2004.

Initial meetings of the LIWG focused on fostering an increased awareness among countries in the region of their obligations under the international counter-terrorism instruments to criminalise terrorist acts in their domestic laws and improving implementation. Another focus of the LIWG is on improving the efficiency of international cooperation in the region. In 2005, the AFP co-chaired an information sharing workshop at the Jakarta Center for Law Enforcement Cooperation (JCLEC) under the auspices of LEWG. AUSTRAC has also provided financial intelligence expertise to the JCLEC training programs.

In December 2005, the LIWG and the LEWG held a joint regional workshop at JCLEC focusing on practical aspects of international cooperation. Australia sponsored representatives from nine developing countries to attend the workshop. The workshop strengthened the capacity of officials from regional countries to initiate and manage requests for mutual legal assistance and extradition.

#### *Regional capacity building*

The Australian Government continues to contribute to regional and international stability and security through international deployments and regional assistance missions. Australia's response to the recent civil unrest in Honiara, the capital of the Solomon Islands has been decisive and comprehensive.

Within 24 hours of the outbreak of violence in Honiara on 18 April 2006, Australia deployed a further 72 AFP personnel to Honiara to assist the Royal Solomon Islands Police Service and Regional Assistance Mission to the Solomon Islands (RAMSI) police personnel already stationed there. 110 military troops from the Australian Defence Force (ADF) were also immediately deployed to support the police and provide a visible presence on the ground. On 21 April 2006, a further 110 military troops were deployed.

These additional AFP and ADF personnel supported their Solomon Islands and RAMSI counterparts to enforce the rule of law, restore order and stability in Honiara and ensure the safety of Australian and other RAMSI personnel.

Given the limited availability of commercial flights out of Honiara, the Australian Government also facilitated the voluntary departure of Australians and other nationals to Australia during the civil unrest.

This response reinforced the message that Australia is committed to the democratic process and long-term stability of the Solomon Islands.

Since the withdrawal of Australian police from Papua New Guinea in May 2005, the Australian Government has continued discussions to develop a mutually acceptable form of a Revised Policing Component for the Enhanced Cooperation Program (ECP). In the meantime a wide range of assistance continues to be provided—for example, the customs component aims to improve border security controls in PNG including airport and waterfront operations, customs control of logging vessels, land border management, supply chain security and cooperation with counterpart agencies responsible for immigration and transportation security.

The AFP provides a Commissioner of Police and staff to the Nauru Police Force as part of a whole-of-government assistance package, which commenced in 2004. AFP staff are internationally deployed to the Vanuatu Police Force Capacity Building Program as part of a five year, \$28 million program, which commenced in January 2006 and is funded by AusAID. The Program aims to assist in creating a safe and secure environment for all citizens and visitors to Vanuatu through the provision of excellent policing services. The AFP is also involved in the Timor Leste Police Development Program, which is a \$33.1 million package aimed at strengthening the law and justice sector in Timor Leste. The Program is a joint Australian and UK Government capacity building initiative, which will continue until December 2008.

The AFP's Law Enforcement Cooperation Program is also currently undertaking numerous other projects focussing on regional and global capacity development activities.

AUSTRAC provides capacity building assistance to 10 South East Asian jurisdictions under the South East Asia Counter Terrorism (SEACT) program; Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Singapore, Thailand, the Philippines and Vietnam. Under this Program AUSTRAC assists counterpart organisations in South East Asia to enhance capacity to detect and deal with terrorist financing and money laundering. Customized technical assistance and training programs are being provided and include in-country mentoring, IT advice, training and typologies development.

In addition to bi-lateral initiatives, AUSTRAC has developed and delivered four regional workshops to date under the SEACT program dealing with such issues as intelligence analysis, terrorist financing typologies, information technology capabilities and alternative remittance systems. A further regional workshop is planned for 2006.

EMA also conducts a range of capacity building activities in the region in the areas of emergency preparedness, response and recovery. These activities have a deterrent effect in the sense that they reduce the impact and therefore effectiveness of potential deliberate actions. They are also a vehicle for joint activities with a more direct security focus.

#### *Law enforcement cooperation and counter-terrorism*

A number of new and ongoing initiatives have also strengthened the AFP's capacity to prevent and investigate terrorist activity both here and overseas.

The AFP is working with other agencies to provide a range of measures aimed at strengthening the capacity of Australia and countries in the region to combat the threat of terrorism, which remains very real in our region, despite the strong relationships built with some of Australia's regional partners. This will build on a number of other regional counter-terrorism assistance measures adopted by the Government over the past four years. The AFP will continue to consolidate work undertaken to date to ensure Australia is able to derive maximum benefit from existing capacity building initiatives, including through the JCLEC and broader work in Indonesia and the Philippines.

The AFP's existing counter-terrorism liaison network will be strengthened, providing core scientific equipment to Thailand and establishing a Thai Bomb Data Centre. The AFP is also in the process of creating two dedicated counter-terrorism advisors for Cambodia and Thailand to assist in boosting their counter-terrorism capabilities in the short to medium term. This is an expansion of the successful posting of a Counter-Terrorism liaison officer in the Philippines, which will continue.

In addition, the AFP is establishing a liaison officer position in India taking into account Indian (particularly Kashmir) vulnerabilities to extremism that may pose risks to regional security in the future. This officer will liaise with foreign counterparts in India on counter-terrorism in and around India.

The AFP's ability to monitor and access electronic surveillance in an effort to pre-empt and target terrorist activity will also be significantly enhanced as a result of funding of \$35 million over four years, allocated in the 2006–07 Budget. Until now, electronic surveillance has been undertaken locally by investigators close to the collection points. A centralised system for monitoring, managing and storing electronic surveillance will now be established, allowing more timely information retrieval and exchange between the AFP and its law enforcement and national security partners. This will include the development of advanced investigative tools and an enhanced capacity to counter the use of new technologies by terrorists.

#### *Improved Border protection in the region*

As part of RAMSI, Customs is delivering a Customs Modernisation Program to the Solomon Islands Customs and Excise Division. The Program aims to develop improved procedures in areas including cargo control, warehousing, intelligence, investigations, border controls, maritime security and passenger processing, through the modernisation of procedures, skills transfer and training.

From 2006–07, Customs will receive an additional \$7.1 million from the Government over three years for 'Improved Border Controls in Southeast Asia'. This new program will build on the early progress made in the Sulu and Celebes Seas area including training assistance activities: intelligence, ship search, precursor chemicals (explosives and drugs), commodity identification, passenger control, counter-terrorism awareness and the use of appropriate border technologies. It also includes the installation and implementation of various border technologies in high risk regional ports, including dual purpose (explosives and drugs) trace detection systems. It will extend similar activities to other high risk ports in the same three countries (Philippines, Malaysia, Indonesia) plus Thailand. Customs will continue to work with border control agencies in the region to develop and implement additional strategies that will improve the control of movements in the border regions and will also foster the exchange of vital information between authorities in each country.

## STRENGTHENING AUSTRALIA'S TRANSPORT SECURITY

The Australian Government's commitment to strengthening transport security has seen some significant developments over the past 12 months.

### *Strengthening Australia's Offshore Maritime Security*

The Government introduced a series of linked initiatives in 2005 to strengthen Australia's offshore maritime security. These measures build on previously announced border protection and maritime security initiatives. They focus, in particular, on protecting Australia's offshore petroleum facilities and ensuring that any terrorist threat to Australia's maritime assets and the Australian coastline can be quickly detected and defeated.

The Attorney-General's Department, together with other relevant agencies, has been tasked with developing international arrangements to strengthen offshore maritime security and counter-terrorism measures. Additional funding over three years from 2005–2006 has been allocated to Attorney-General's Department to enable it to carry out its role in further developing international arrangements in support of the Government's offshore maritime security initiatives.

Australia played a leading role in the adoption by the International Maritime Organisation in October 2005 of a protocol to each of the Convention for the Suppression of Unlawful Acts against the Safety of Navigation and its Protocol concerning Fixed Platforms on the Continental Shelf. The protocols will greatly advance international efforts to fight terrorism and prevent the spread of weapons of mass destruction. The protocols will bolster and compliment existing strong measures taken by the Government relating to offshore maritime security and Australia's commitment to the Proliferation Security Initiative. The Attorney-General signed both protocols, subject to ratification, on 7 March 2006.

### *Aviation Security*

Since the events of 11 September 2001, the Government has adopted substantial measures to strengthen aviation security. Measures introduced since 2001 include: hardened cockpit doors to prevent access by intruders, armed air security officers on domestic and international flights, passenger screening for all regular passenger jet flights, upgraded CCTV and monitoring capability, and enhanced cargo security clearance and checked baggage screening arrangements.

Aviation security has also been strengthened through the AFP deployment of Regional Rapid Deployment Teams which, since their inception, have visited some 87 different airports throughout regional Australia. The Teams have participated in counter-terrorism exercises at Broome, Kalgoorlie, Toowoomba and Cambridge airports, with future exercises planned for the Northern Territory, Queensland and New South Wales during the second half of 2006.

The Australian Government signed a bilateral agreement to provide Air Security Officer Operations with the Philippines in March 2006, with deployments commencing in shortly.

## *Wheeler Report*

In 2005, the Wheeler Review of Airport Security and Policing assessed the adequacy of Australian aviation security requirements and arrangements put in place in response to the threat from terrorism and organised crime. The review, which was released in September 2005, made seventeen recommendations to reform and refine security and policing at Australia's airports. The Australian Government has announced its in-principle acceptance of these recommendations, and implementation is proceeding.

- ***AusCheck***

In 2005, the Government agreed to establish a new division of the Attorney-General's Department, which will be responsible for conducting background checks on those who work in the secure areas of air and sea ports, namely, those who are required to hold Aviation Security Identification Cards and Maritime Security Identification Cards. The division will be known as AusCheck.

The decision to establish AusCheck is consistent with a recommendation of the Wheeler Review and is part of the Government's ongoing commitment to improve aviation and maritime security. AusCheck will strengthen national security arrangements by ensuring that unsuitable individuals are not able to work in security sensitive areas of airports and sea ports.

The Government has provided the Attorney-General's Department with \$22.3 million to establish AusCheck. Once fully established the division will operate on a cost recovery basis. AusCheck will commence operations from 1 July 2007.

- ***Review of Information Sharing in the Aviation Sector***

The Attorney-General's Department has engaged a consultant to prepare a review on Recommendation 1 of the Wheeler Report, examining legislation that affects the sharing of information between Commonwealth agencies, between States and Territories and the Commonwealth, and between government and business in aviation security. The review will identify impediments to the exchange of information and assess those impediments against the need to maintain adequate standards of accountability, transparency and privacy. The review will also identify processes and safeguards across jurisdictions for the collection and sharing of information which will protect national security and commercially sensitive information.

- ***Closed Circuit Television***

In September 2005 COAG agreed to the development of a National Code of Practice for CCTV systems in the Mass Passenger Transport Sector. A COAG working group chaired by the Victorian Department of Infrastructure has been established to develop the Code. The Attorney-General's Department is represented on the working group.

The Code will include protocols and requirements for the use of CCTV systems to enhance counter-terrorism arrangements. It will also contain national guidelines for the collection, storage, access, use, privacy, disclosure, protection and retention of CCTV information.

Additional funds of \$75,000 were allocated to the Office of the Privacy Commissioner in PAES 2005–06 to assist the Office of the Privacy Commissioner in the development of the Code of Practice for CCTV.

As part of the Government's response to the Wheeler Review, Customs will receive funding of \$14.0 million over four years to expand and modernise its airport CCTV capability.

#### *Unified Policing Model at designated airports*

The Wheeler Report recommended the establishment of a single police command structure at Australian airports. COAG agreed to establish a unified policing model at eleven designated airports including: an Airport Police Commander, a dedicated Joint Intelligence Group, a Counter-Terrorism First Response (CTFR) capability and a permanent community policing presence. In addition, it was agreed that at each of the five major international airports, (Sydney, Melbourne, Brisbane, Perth and Adelaide) a Joint Airport Investigation Team would be established.

The AFP received funding for Airport Police Commanders and Joint Airport Investigation Teams prior to consideration of the Wheeler Report. Following COAG consideration for the Wheeler Report, additional funding was received for Joint Airport Intelligence Groups, CTFR, and phase 1 Airport Uniformed Policing. Ongoing funding for Protective Security Liaison Officer Network continues until 2007-08.

Additional funding of \$242 million is now being provided to fund phase 2 of Airport Uniform Policing. This funding brings the Government's total funding commitment to the Unified Policing Model over the five years from 2005-06 to 2009-10 to \$679.5 million.

Airport Police Commanders have commenced at the designated airports and have been positively received by the aviation industry and government agencies. As part of the implementation of the Unified Policing Model, existing CTFR capability and Protective Security Liaison Officers report directly to the Airport Police Commander at their respective airports. Joint Airport Investigation Teams (JAIT) have commenced operations in the five major international airports.

Personnel will be provided by all jurisdictions to staff uniformed policing at each designated airport. Negotiations with the States and Territories are progressing, with approximately half the Airport Uniformed Policing complement to be deployed by the end of 2006, and the remainder deploying during 2007.

### **STRENGTHENING INTELLIGENCE CAPABILITIES**

Australia relies upon a strong intelligence-led prevention and preparedness regime to support its counter-terrorism strategy.

Since 11 September 2001 there have been increased demands on the Australian Security Intelligence Organisation (ASIO) to identify and investigate terrorist threats to Australia and Australian interests overseas, and to provide protective security advice, including for national critical infrastructure.

Funding to ASIO has more than doubled in the five years since 2001. ASIO is set to grow further to 1860 staff by 2010–11 following the commitment of additional funds in the 2006–07 Budget to meet the challenges of known and unknown sources of terrorist threat, as well as the continuing threat of espionage and foreign interference.

ASIO has been recruiting and training additional staff for intelligence collection, investigation and analysis, expanding its capacity to provide border control security advice, threat assessments and critical infrastructure protection advice, and increasing its capability to deliver security assessments. Key parts of ASIO now operate 24 hours a day, seven days a week, including the Communications Centre, the multi-agency National Threat Assessment Centre, the Research and Monitoring Unit and the visa security checking area.

ASIO has enhanced counter-terrorism cooperation with other intelligence agencies and with law enforcement, border control agencies and other relevant parts of Government. It has extended and deepened international links through increased representation overseas, heightened cooperation with overseas agencies and involvement in regional capacity-building initiatives.

The AFP and Australian Intelligence Community (AIC) are increasingly co-dependent, with the AFP relying on information sourced by AIC agencies in criminal investigations, and the AIC relying on the AFP to provide criminal intelligence and threat-related information to fill the gaps in the overall national security picture.

With additional funding of \$51.6 million over four years, commencing in the 2006–07 Budget, the AFP will significantly upgrade its capacity to collect, assess, store and share sensitive threat-related information and criminal intelligence within the AFP and with its partner agencies, in a time critical manner. This will bring the AFP's intelligence systems in line with the AIC and enable the AFP to better conduct investigations, particularly counter-terrorism investigations, which rely heavily on sharing intelligence with the AIC.

## **CRIMINAL AND FINANCIAL INTELLIGENCE**

AUSTRAC continue their commitment to creating a financial environment hostile to money laundering, major crime and tax evasion. The work AUSTRAC initiated after the events of 11 September 2001 has continued to expand. As well as enhancing its domestic focus on countering the financing of terrorism, AUSTRAC is also making progress internationally.

### *Financial Intelligence and Anti-Money Laundering*

Due to the nature of money laundering and major crimes, international cooperation and financial intelligence exchange with international counterparts has been an important function of AUSTRAC since its inception. AUSTRAC is working bilaterally with countries in our region and AUSTRAC's multilateral relationships include involvement in the Egmont Group of Financial Intelligence Units, leading Australia's involvement in the Asia Pacific Group on Money Laundering.

AUSTRAC has enhanced its intensive analytical support provided to ASIO, providing for more effective information exchange and the targeting of financial intelligence into key areas of ASIO's work.

AUSTRAC has recently reviewed its memoranda of understanding with state and territory police services to enable staff within counter-terrorist units to have online access to AUSTRAC's financial intelligence database. AUSTRAC will increase the level of access and number of designated personnel who can access the TRAQ Enquiry System from within the Australian Taxation Office, Centrelink, the Child Support Agency and the New South Wales Crime Commission.

AUSTRAC has increased its international instruments to exchange financial intelligence with counterpart agencies overseas from 14 in 2002–03 to 45. It now exchanges financial intelligence with Argentina, The Bahamas, Bermuda, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Cook Islands, Croatia, Cyprus, Denmark, Estonia, France, Guernsey, Hong Kong (China), Indonesia, Ireland, Isle of Man, Israel, Italy, Korea, Latvia, Lebanon, Malaysia, Marshall Islands, Mauritius, the Netherlands, New Zealand, Panama, Philippines, Poland, Portugal, Romania, Singapore, Slovakia, Slovenia, South Africa, Spain, Thailand, the United Kingdom, the United States of America, Vanuatu and Venezuela.

#### *Anti-Money Laundering eLearning*

In April 2005, AUSTRAC introduced an Internet-based anti-money laundering eLearning application. It is designed to assist cash dealers, industry associations, solicitors, members of the public and other interested stakeholders in understanding the various reporting and "Know Your Customer" obligations under the *Financial Transaction Reports Act 1988* (FTR Act).

The application and its content complement AUSTRAC's existing education program. The primary intent of the AML application is to provide a user-friendly, internet-based resource to enhance industry and public awareness of the broader anti-money laundering/counter-financing of terrorism environment and the various obligations imposed by the FTR Act, and to inform them of AUSTRAC's role in this process. In the first three months alone, the AML eLearning application webpage was accessed on 15,439 separate occasions. AUSTRAC has received very positive feedback, particularly from the financial sector, on the value of this service.

#### **GOVERNMENT-BUSINESS LIAISON ON NATIONAL SECURITY**

The protection of the private sector from national security threats is the responsibility of both government and the owners and operators of business enterprises. The Government is committed to working with business representatives and assisting them to meet national security related objectives.

### *Trusted Information Sharing Network (TISN)*

The Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection has a key role in the business-government partnership. The TISN enables the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management and threats and vulnerabilities on a national level. The TISN consists of a number of Infrastructure Assurance Advisory Groups for different business sectors, Expert Advisory Groups, and the Critical Infrastructure Advisory Council. New Infrastructure Assurance Advisory Sub-Groups were formed for the maritime, rail and aviation sectors. A Futures Expert Advisory Group was also established to provide long term strategic thinking on critical infrastructure protection issues.

The Critical Infrastructure Advisory Council oversees the Infrastructure Assurance Advisory Groups and provides advice to the Attorney-General on the national approach to protecting critical infrastructure. The Council consists of representatives from each of the States and Territories, the critical infrastructure business sectors, relevant Australian Government agencies and the NCTC. The Attorney-General launched the TISN Secure Website on 13 April 2005, allowing TISN members to share information in a secure environment.

Standards Australia has been engaged to develop a framework for collaboration between the Attorney-General's Department, the TISN and Standards Australia to develop an integrated security standards framework which businesses can use to protect critical infrastructure.

### *Business-Government Advisory Group on National Security*

The Business-Government Advisory Group on National Security is chaired by the Attorney-General and gives senior business leaders an opportunity to input into the strategic direction of Australia's national security policy. It also gives the Government a forum to discuss shared interests in the context of the business community, proposed new security initiatives and developments with the business community.

### *Business Liaison Unit*

The ASIO Business Liaison Unit (BLU) was established in late 2005 to provide a direct interface between business and the Australian intelligence community. The BLU will assist in ensuring that the owners and operators of critical infrastructure, and other relevant members of the Australian business community, can access timely information on matters affecting the security of assets and staff for which they are responsible. In providing this information, the BLU aims to help business efficiently respond to the current security environment. This initiative is intended to complement other current national security arrangements.

### *Critical infrastructure protection*

The Australian Government's policy on critical infrastructure protection (CIP) seeks to ensure there are adequate levels of protective security on critical infrastructure, minimum single points of failure and rapid, tested recovery arrangements.

The Attorney-General's Department provides national leadership and coordination of critical infrastructure protection. The Australian Government also provides intelligence, ensures protection arrangements are in place for offshore critical infrastructure assets and multi-jurisdictional critical infrastructure, and assists owners and operators in the Australian Government regulated sectors.

The Australian business community must consider a range of threats and hazards that put their operations, staff and customers at risk. Critical infrastructure can be damaged, destroyed or disrupted by natural disasters, human error, accidents, criminal activity (including computer hacking and malicious damage) as well as by acts of terrorism. An all-hazards approach to the protection of critical infrastructure enables more cost-effective common mitigation strategies to be applied. These reduce the degree of risk from a wider range of potential threats, allowing for additional attention to be focused on areas of greatest risk.

The NCTC has requested that ASIO prepare threat assessments for each piece of infrastructure assessed to be 'nationally vital'. COAG has agreed that the private owners of each asset in this category will be encouraged to develop appropriate security plans, informed by having direct access to the ASIO threat assessment. In addition, ASIO is preparing threat assessments for each sector of critical infrastructure, which will be used as the basis for wider industry consultation. These assessments may identify specific issues that government will need to address in partnership with the private sector.

The Attorney-General's Department officially launched the national CIP Modelling and Analysis (CIPMA) Program in February 2006. The CIPMA capability uses detailed sector infrastructure data provided by industry to model, simulate and analyse the dependencies and relationships between national critical infrastructures and the flow-on consequences of a failure in a particular sector. This information is used to support strategic decision making in CIP, counter-terrorism and emergency management. The Australian Government has committed an additional \$19 million to the CIPMA Program over four years, with the initial focus on three priority critical infrastructure sectors—Banking and Finance, Energy, and Communications. Good coverage of the three priority sectors will be achieved by June 2007.

#### *Places of mass gathering*

In addition to the efforts to protect critical infrastructure, the Attorney-General's Department is working with the business community to help protect places of mass gathering.

As part of the TISN, the Mass Gatherings Infrastructure Assurance Advisory Group (IPG-IAAG) aims to strengthen communication between government and business in a heightened security environment and provide stakeholders with the information and tools needed to identify, manage and reduce risk in an all hazards context. In November 2005, the IPG-IAAG launched its Business Plan for 2005–06 which includes the development of a counter-terrorism toolkit and a model for government-business communication with places of mass gathering.

The Australian Government is also working with the NCTC to finalise the National Approach for the Protection of Places of Mass Gathering from terrorism. This will ensure that a nationally consistent approach is taken by all Australian jurisdictions in the development of their own guidelines for the protection of places of mass gathering from terrorism.

## *Protection of the national information infrastructure*

Rapid changes in information technology have immense implications for how our critical infrastructure works and for how owners and operators manage their security. While there is no evidence that there has been an act of cyber-terrorism in Australia to date, our vulnerability to such attacks is increasing. Like other developed economies, Australia is increasingly dependent on the information economy and this creates significant new threats and vulnerabilities.

The Computer Network Vulnerability Assessment (CNVA) Program has been developed to help secure critical infrastructure from cyber threats. Under the CNVA Program the Attorney-General's Department provides co-funding on a dollar for dollar basis to help owners and operators of critical infrastructure to identify major vulnerabilities within computer systems and interdependencies between computer networks, and test the ability of systems to resist exploitation. The Australian Government has made over \$5 million available over four years to assist owners of critical infrastructure.

The Government is working closely with business, including via the TISN, to help secure Australia's critical infrastructure from cyber threats. The Information Technology Security Expert Advisory Group is providing TISN members with valuable advice and information on emerging IT security issues and strategic advice on technical solutions to e-security problems that have the potential to impact across all industry sectors.

The Attorney-General's Department provides funding to support the Australian Computer Emergency Response Team, AusCERT, which is based at the University of Queensland. AusCERT operates a free email subscription alert service that provides evaluation of global computer network threats and recommended protection and mitigation strategies. This free service allows businesses access to information about threats to computer security. In addition, AusCERT also provides an IT Incident Reporting Scheme which is able to assess and gauge the level and nature of computer network attack in Australia.

GovCERT was formed in 2005 to develop and coordinate Government policy for computer emergency preparation, preparedness, response, readiness and recovery. GovCERT acts as a point of contact within the Australian Government for foreign governments on CERT issues, and coordinates any foreign government requests. GovCERT is responsible for preparing and coordinating Australia's readiness for major incidents affecting the national information infrastructure. The Attorney-General's Department provides policy and logistical support to GovCERT.

The Australian Government is currently undertaking a review of the E-Security National Agenda. The E-Security National Agenda addresses the integrity and security of the online environment for both public and private sectors. The review is being undertaken to ensure that Australia's policy and operational framework continues to be responsive to the changing e-security environment now and into the future.

### *Protective Security Services*

The AFP continues to provide close personnel protection (CPP) to the Commonwealth at the level required in the post September 11 threat environment. Continued funding from the Government has allowed the AFP to manage and deliver comprehensive CPP services as and when they are required. This includes current principals, as well as affording the same capacity for general requirements, such as official visits by VIPs, and the ability to address protective security issues arising from specific threats. In addition, the AFP will contribute CPP services to the Department of the Prime Minister and Cabinet sponsored cross-portfolio measure on the Australian involvement in Anzac Day ceremonies overseas.