Guide to Australia's National Security Capability

Contents

Introduction

The period since 2001 has been transformative for Australia's national security and our national security challenges continue to evolve. To meet these challenges, we need new ways to coordinate and develop our capability and to shape the national security environment.

Significant advances have been made in recent years to build greater collaboration and interoperability across the national security community. However, the increasing complexity of national security threats requires an even more consistent and connected approach to capability planning that complements existing individual agency arrangements.

To that end, the Government has developed a security classified National Security Capability Plan to provide a single consolidated picture of the capabilities that enable Australia to achieve national security outcomes.

This Guide offers an overview of Australia's national security capability planning. It identifies the functions performed by the national security community and how these achieve the objectives outlined in the *National Security Strategy (2013)*.

Capability planning is one of the tools that support Government to better consider how capabilities can be directed to meet national security objectives. This ensures that capability investment is focussed and that Government can give appropriate consideration to redirecting existing capabilities to meet new or emerging risks and opportunities. It also highlights areas where agencies' capabilities are interdependent, identifying focus areas for collaboration and interoperability.

Having a better understanding of our capabilities will help us to make more informed decisions about what we need.

Australia's national security arrangements are underpinned by a number of agencies working across areas such as diplomacy, defence, development, border protection, law enforcement and intelligence. Australia's national security agencies include:

- Attorney-General's Department (AGD)
- Australian Agency for International Development (AusAID)
- Australian Crime Commission (ACC)

- Australian Customs and Border Protection Service (ACBPS)
- Australian Federal Police (AFP)
- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Geospatial-Intelligence Organisation (AGO)
- Australian Signals Directorate (ASD)
- Department of Agriculture, Fisheries and Forestry (DAFF)
- Department of Defence (Defence)
- Department of Foreign Affairs and Trade (DFAT)
- Department of Health and Ageing (DoHA)
- Department of Immigration and Citizenship (DIAC)
- Department of Infrastructure and Transport (DIT)
- Department of the Prime Minister and Cabinet (PM&C)
- Office of National Assessments (ONA).

The Capability Plan brings together, for the first time, a single view of the capabilities maintained by these agencies with the exception of Defence capabilities. Defence has a separate established capability planning process that includes the *Defence White Paper (2013)* and *Defence Capability Plan (2012)*. Defence is a key contributor to Australia's national security arrangements including leading the coordination and delivery of national security science and technology and works in close cooperation with other national security agencies. Defence capabilities will continue to be managed through existing mechanisms, principally the *Defence Capability Plan*.

For the first time, the Capability Plan, and the accompanying Guide to Australia's National Security Capability, presents a unified picture of the capabilities that exist across non-Defence national security agencies. Together with other strategic planning tools, this work informs the broader national security planning cycle and supports the objectives and implementation of overarching policy documents such as the *National Security Strategy* and the *Australia in the Asian Century White Paper*.

The Capability Plan complements the Defence Capability Plan and does not seek to duplicate it.

It should also be noted that the Guide has not been designed to signal specific initiatives or tender opportunities. Such processes will continue to be managed by individual agencies.

Part 1: Australia's national security framework

Australia's *National Security Strategy* is the overarching policy document that guides our national security efforts over a five-year period. The National Security Capability Plan, as well as a number of other strategic documents such as the *Defence White Paper*, support this strategy.

In the *National Security Strategy*, Australia's vision is for 'a unified national security system that anticipates threats, protects the nation and shapes the world in Australia's interest'. This vision is supported by four national security objectives:

- protecting and strengthening our sovereignty;
- ensuring a safe and resilient population;
- securing our assets, infrastructure and institutions; and
- promoting a favourable international environment.

National security agencies work to achieve these objectives under the eight pillars of Australia's national security:

- countering terrorism, espionage and foreign interference.
- deterring and defeating attacks on Australia and Australian interests.
- preserving Australia's border integrity.
- preventing, detecting and disrupting serious and organised crime.
- promoting a secure international environment conducive to advancing Australia's interests.
- strengthening the resilience of Australia's people, assets, infrastructure and institutions.
- the Australia-United States Alliance.
- understanding and being influential in the world, particularly the Asia-Pacific.

Our national security capabilities enable our approach to the current national security environment as aligned with the *National Security Strategy's* pillars.

A better understanding of what capabilities we have allows the Government to consider what tasks it can perform to manage national security risks and pursue opportunities in Australia's national interest.

Part 2: Australia's approach to national security capability planning

Capability is what enables the Australian Government and its intelligence, law enforcement, border security, defence, diplomatic, development and emergency management agencies to achieve national security objectives.

Capability-based planning helps the Government to determine what capabilities are needed to respond to a broad range of risks. This results in better informed investment decisions. For example, the Capability Plan complements the *National Security Strategy* by providing an important evidence base to inform judgements about the capabilities available to manage national security risks. Capabilities developed by national security agencies are then employed to manage these risks or pursue opportunities in a range of environments—including domestically, at the border, offshore and in cyberspace.

At a strategic level, the national security community performs a number of national security functions. These functions provide a complete picture of the broad ranging capabilities the national security community maintains. While the *National Security Strategy's* pillars provide a thematic representation of our capabilities, the functions are focussed on how they operate.

Considering capability in this way also allows us to identify:

- where like capabilities are used across several functions
- which domains capabilities operate in
- where capability development is required in order to counter emerging threats
- areas where capability interoperability can be enhanced.

To meet Australia's national security objectives, the collective capabilities of agencies enable the Government to perform the following functions in support of the eight pillars of Australia's national security outlined in the *National Security Strategy*:

- **Threat detection, recognition, identification and monitoring**
  The ability to detect, assess and monitor potential threats.
- **Intelligence, information and knowledge sharing and dissemination**
  The ability to collect, analyse, assess and share timely and useable intelligence and

other information. This also includes the ability to develop and maintain knowledge management systems.

- **Horizon scanning, risk assessment, modelling and simulation**

  The ability to reduce uncertainty for decision makers by providing coordinated and analytical scientific and technological support around current and future trends, risks, interdependencies and vulnerabilities. This supports planning for capability development, options development and/or consequence assessments.

- **National oversight, command, control and coordination**

  The infrastructure and arrangements to enable awareness and management of national and inter-agency operations and/or crises.

- **Public engagement, media and warnings**

  The ability to communicate with the public and media (both locally and nationally) in a timely and coordinated manner, including to raise awareness and delivering emergency warnings and threat information.

- **Incident response, law enforcement, investigation and forensics**

  The ability to enforce the law, deliver tactical responses to security or unlawful incidents, and to support post-incident investigations and prosecutions.

- **Quarantine, containment, render safe, decontamination and disposal**

  The ability to identify, characterise, isolate and contain hazardous, contaminated or infectious material, organisms or sites. This covers human, animal and plant biohazards and both laboratory-based and disease-control measures.

- **Community and infrastructure resilience and recovery**

  The ability to work with communities and critical infrastructure owners to stabilise against national security risk, through building an awareness of risk and strengthening the capability to prevent, prepare, respond and recover from potentially harmful events. This includes temporary infrastructure for recovery.

- **Policy, national governance and capability development**

  The ability to provide strategic policy advice and implement legislation, policies and other forms of regulation to support national security objectives, as well as the ability to promote inter-agency operability and national interoperability. This includes the ability to undertake capability planning and development.

- **International engagement**

  The ability to promote and protect Australia's interests by supporting Australians overseas, engaging with foreign governments, other counterparts, and international organisations, enhancing national security through promoting growth and stability in

our region and strengthening strategic bilateral, regional and multilateral relationships.

- **Testing, exercise and evaluation**

  The ability to conduct single agency, multi-agency, national and international exchanges to share or assess current and potential capabilities to manage national security risk and inform the national interest.

- **Mass care, mass casualty and mass fatality management**

  The ability to shelter, feed and support displaced persons, provide sustained or surge medical treatment (in hospital or field), and manage victims in Australia and overseas, including disaster victim identification.

- **Stockpiles, logistics and distribution**

  The ability to procure, produce, store and disseminate equipment, treatments and supplies, including management and distribution systems, within Australia and in response to overseas events.

Within each of these functions, national security capabilities enable the Government to shape capabilities to act across a continuum of Prevent, Prepare, Respond and Recover (PPRR). Some of our capabilities are applied in order to prevent national security risks eventuating, while others are available to Government to respond effectively to an issue of national security concern. Understanding where capabilities are placed on the continuum allows Australia to take hold of capability development opportunities and consider where resources are best applied in order to support our national security objectives.

Capability planning provides decision makers with a collective view of where capabilities are directed along this continuum. This includes capabilities that shape the environment in positive ways to support Australia's national security objectives, including to promote social cohesion, the rule-of-law, economic prosperity and stability to prevent the emergence of future threats.

- **Prevent:** Measures to eliminate or reduce the incidence or severity of risk (this covers emergencies, activities, incidents or acts which are contrary to government achieving its national security objectives).
- **Prepare:** Measures to ensure that, should a crisis or emergent event occur, communities, resources and services are capable of coping with the effects; the state of being prepared to meet risks (through planning, resourcing, testing, and building resilience).

- **Respond:** Actions taken in anticipation of, during and immediately after a crisis or emergent event (threat, incident or act) to ensure that its effects are minimised, and that people affected are given immediate relief and support (this includes the prevention and minimisation of loss of life, injury, damage to property and disruption to infrastructure, facilitate investigations into the event, threat, incident or act – including the prosecution of offenders).
- **Recover:** The coordinated process of supporting affected communities in reconstruction of the physical infrastructure and restoration of emotional, social, economic and physical wellbeing.

Figure 1 below provides a representation of the relationship between capability planning, national security functions, the domains and continuum in which capabilities operate.
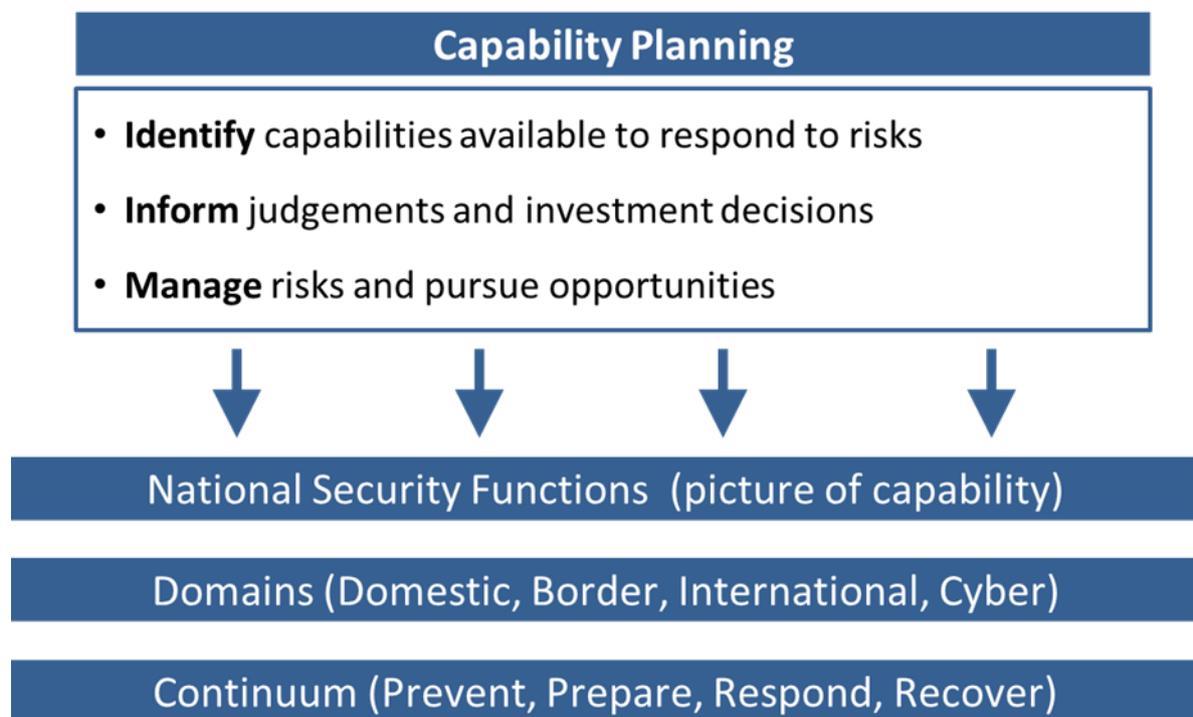
The following table identifies which national security agencies maintain capabilities in support of Australia's national security functions. Understanding connections between agency functions encourages flexibility, adaptability and interoperability when developing new whole-of-government capability approaches.

NATIONAL SECURITY FUNCTIONS	NATIONAL SECURITY AGENCIES WITH CAPABILITIES WHICH ALIGN TO FUNCTIONS
Threat detection, recognition, identification and monitoring	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Intelligence, information and knowledge sharing and dissemination	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Horizon scanning, risk assessment, modelling and simulation	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
National oversight, command, control and coordination	ACBPS, ACC, AFP, AGD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Public engagement, media and warnings	ACBPS, ACC, AFP, AGD, DAFF, Defence DFAT, DIT, DOHA, PM&C
Incident response, law enforcement, investigation and forensics	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C
Quarantine, containment, render safe, decontamination and disposal	ACBPS, AFP, DAFF, Defence, DFAT, DIT, DOHA
Community and infrastructure resilience and recovery	ACBPS, AFP, AGD, AGO, DAFF, Defence, DFAT, DIAC, DIT, DOHA
Policy, national governance and capability development	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
International engagement	ACBPS, ACC, AFP, AGD, AGO, ASD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIAC, DIT, DOHA, PM&C, ONA
Testing, exercise and evaluation	ACBPS, AFP, AGD, AGO, ASD, ASIO, ASIS, AusAID, DAFF, Defence, DFAT, DIT, PM&C, ONA
Mass care, mass casualty and mass fatality management	AFP, Defence, DFAT, DIAC, DIT, DOHA
Stockpiles, logistics and distribution	AFP, AGD, AusAID, Defence, DFAT, DIT, DOHA

Across the national security community, agencies perform a variety of roles to protect and promote our national interest. Our national security apparatus is increasingly interconnected across government, non-government and industry sectors. In the context of the national security functions, the following table provides a strategic expression of how capabilities are employed across the national security community in support of our national security objectives.

National Security Function	National Security Capabilities Statement
Threat detection, recognition, identification and monitoring	Australia's diplomatic network and international legal frameworks, law enforcement and border protection networks, liaison partnerships and foreign intelligence collection and assessment capabilities support the detection, monitoring and surveillance of offshore threats that may affect Australia or pose a risk to Australian or allied nations, operations and interests offshore. Australian law enforcement and national security capabilities act to reduce the threat and impact of terrorism, espionage and foreign interference and serious and organised crime, including cyber crime, on the community through intelligence collection and analysis, surveillance, law reform, coercive powers, forensics, data centres and engagement with the public and private sector. Australia's border systems enable pre-travel screening of non-citizens through the universal visa, biometrics, and Advanced Passenger Processing systems and border screening on arrival. This mitigates the risk of national security issues arising at the border and within Australia. Protection capabilities held by Commonwealth, State and Territory law enforcement agencies provide the ability to detect and deter threats against diplomatic, official and defence establishments, dignitaries and major national events both in Australia and offshore. Border, aerial, maritime and port surveillance and controls are supported by investigation, intelligence collection and risk assessment capabilities to ensure regulation and compliance of movement of goods and people across the Australian border. These capabilities also support detection of transnational crime, such as illegal fishing and logging, and together with quarantine capabilities, allow for the detection and monitoring of human, plant or animal health threats.

Intelligence, information and knowledge sharing and dissemination	Australia's security and foreign intelligence capabilities support the ability to collect, analyse and assess potential onshore and offshore threats to Australians, Australia and our interests.

Our fusion capabilities, open source collection, technical solutions, data centres and domestic and international information sharing networks enable the timely sharing of critically important intelligence, information and knowledge across all levels of government and with other key stakeholders so that the right people have access to the right information when they need it.

Sharing of information, intelligence and knowledge is governed by a legislative and policy framework which strikes a balance between the need to share information and the need to protect the privacy and rights of Australians and Australian entities.

Partnerships with private industry, the community and academia enable the sharing of relevant intelligence, information and knowledge through capabilities such as the National Computer Emergency Response Team (CERT), the Trusted Information Sharing Network, the ASIO Business Liaison Unit and the National Security Hotline. |
| **Horizon scanning, risk assessment, modelling and simulation** | Horizon scanning, strategic risk assessments, critical infrastructure geospatial modelling and analysis, situational awareness, forecasts of current and emerging threats to Australia or its allies supports government decision makers to focus and prioritise efforts.

The *National Security Strategy* outlined the Government's intention to undertake ongoing improvements to the coordinated national security budget process based on this analytical work. These arrangements provide a mechanism through which the national security community can better support the Government to make strategic, centrally coordinated judgements in response to a wide range of risks and opportunities. |
| **National oversight, command, control and coordination** | National oversight and command and control of whole-of-government responses to national security threats are coordinated through the Australian Government Crisis Committee or the Inter-Departmental Emergency Task Force (IDETF) for events overseas. Coordination with State and Territory governments occurs through the National Crisis Committee and a range of national committees depending on the scale and nature of the event.

These oversight mechanisms provide the capability to shape policy responses, development activities and to build national cooperation and communication to meet the challenges faced in preventing and preparing for threats facing our national security. This creates critical linkages between Commonwealth and State and Territory agencies that have responsibility for frontline operational response capabilities. |

Public engagement, media and warnings	The Australian Government communicates with the public and media on national security matters through capabilities which raise awareness of threats, conducts community outreach through education and awareness programs, provides for the collection of public information and maintains alert systems to warn of security incidents. These arrangements enable the effective and timely provision of accurate information to the public. Government engagement with industry on national security matters, including cyber security and critical infrastructure resilience, is achieved through the Trusted Information Sharing Network and disaster resilience programs. These provide industry with an understanding of current and emerging national security issues and industry compliance. Public information and warning systems, such as DFAT Travel Advice, Emergency Alert and the National Terrorism Public Alert System, assist the community in preparation and planning through the provision of emergency advice to minimise risks to their safety.
Incident response, law enforcement, investigation and forensics	Australian Government agencies provide incident response, law enforcement, investigation and forensics capabilities and work with State and Territory law enforcement agencies in joint operations to detect and disrupt serious and organised crime and counter terrorism related activities. These capabilities enable disruption of illegal activities and include the use of coercive powers, explosive bomb appraisal, tactical intelligence, protective security operations, cyber security operations, evidence collection to support serious and organised crime prosecutions, and post-incident investigations. At the border, capabilities to assist investigations include cargo examination and traveller assessments. Offshore capabilities include maritime response to illegal fishing and people smuggling activities. Additionally, Australia has the capability to provide a coordinated response to offshore humanitarian incidents. Internationally, specialist response teams, including Commonwealth, State and Territory law enforcement, Australian Civilian Corps, Commonwealth liaison officers, Consular Emergency Response and Disaster Assessment Teams, Urban Search and Rescue Teams together with Defence capabilities can be deployed to support an Australian response to an offshore disaster or emerging security threats.
Quarantine, containment, render safe, decontamination and disposal	Australia's national laboratory, diagnostic and characterisation capabilities enable the detection of current and emerging human, animal and plant biohazards. These capabilities also allow for the investigation of infectious diseases and biological agents when processing international passengers, cargo, mail, and animal or plant products arriving in Australia. The Security Sensitive Biological Agents Regulatory Scheme aims to minimise access to biological agents of security concern and limit the opportunities for acts of bioterrorism or biocrime to occur using harmful biological agents.

Community and infrastructure resilience and recovery	The Australian Government's implementation of arrangements and strategies for providing communities and critical infrastructure owners with an awareness of national security risk implications, including the Critical Infrastructure Program for Modelling and Analysis, enables the strengthening of non-government capability to prevent, prepare, respond and recover from potentially harmful events. Additionally, the Australian Government works closely with at-risk communities to build resilience to violent extremism, promote and support programs which build social cohesion and provides community awareness of disaster resilience through education, research and training including offshore. The security, resilience and betterment of Australia's infrastructure, both physical and cyber based, is also supported through domestic and international fora that focus on information sharing, strategic dialogue on cyber policy, and cyber crisis management arrangements and relief and recovery funding assistance through Natural Disaster Relief and Recovery Arrangements.
Policy, national governance and capability development	Australia's national security legislative framework, policies and regulations govern the work of the intelligence community, law enforcement agencies and other agencies with responsibility for national security. This framework supports the safety of Australians and the protection of Australia's democratic values such as the rule of law and human rights. Commonwealth capabilities provide accurate, relevant, comprehensive and timely national and international law advice to support decision makers on matters of national security which allows Australia to manage national security threats and promote the rule of law. Australia coordinates its national security capability planning and development through a comprehensive suite of white papers, strategic plans and reviews, including the National Security Capability Plan. National security agencies respond to the Government's strategic direction by building capabilities in line with national security risks and priorities. Additionally, national arrangements for counter–terrorism and emergency management are coordinated through interoperable capabilities developed in partnership between Commonwealth, State and Territory governments, non-government organisations and private enterprise.

International engagement	Australia has strong relationships with international partners through our diplomatic and defence networks and active engagement in a wide range of regional and international fora to promote a secure international environment conducive to achieving Australia's interests. Australia engages in international law and justice, border security, intelligence and emergency management capacity building, provides international development assistance and coordinates health emergency arrangements with our international partners. As well as implementing United Nations Security Council (UNSC) resolutions, including those imposing UNSC and autonomous Australian sanctions, government agencies also engage in bilateral, multilateral and regional fora on emergency management, critical infrastructure, counter-proliferation, counter-terrorism, transnational crime, combating corruption, international crime cooperation and cyber security. Additionally, Australia maintains international defence, intelligence, diplomatic security, aid and law enforcement networks, provides protection services for visiting dignitaries and resident diplomatic/consular missions in Australia, Australians travelling officially overseas and retains a number of operational capabilities for international deployments including in support of defence, aid and disaster relief operations offshore and rapid responses to assist other nations during a crisis, such as the Australian Civilian Corps.
Testing, exercise and evaluation	Engagement in multilateral national and international exercise activities assists with the identification and subsequent management of national security risk. Exercises support continuous improvement through the maintenance, development and evaluation of capability as well as enhancing interoperability across the national security spectrum. Consistent with the Critical Infrastructure Resilience Strategy, exercising with critical infrastructure owners/operators, and the private sector generally, provides the opportunity to explore interdependencies and increase communication between business and government. Issues identified as a result of operational and exercise activities inform risk assessments and contribute to the ongoing development of national security policy, planning and capability.
Mass care, mass casualty and mass fatality management	The National Health Arrangements and supporting capabilities ensure the Australian health sector can provide a coordinated response to, and recovery from, emergencies of national consequence and meet the needs of displaced Australians and arrangements for the protection of places of mass gatherings. The Disaster Response Plan provides a coordinated response across the Commonwealth, States and Territories for the positioning of Commonwealth resources and the establishment of Australian Medical Assistance Teams which provide assistance and care during and post a security incident within Australia and overseas. Additionally, during a crisis, the National Critical Care and Trauma Response Centre as well as Commonwealth, State and Territory agencies provide a surge capability to manage mass care and Disaster Victim Identification.

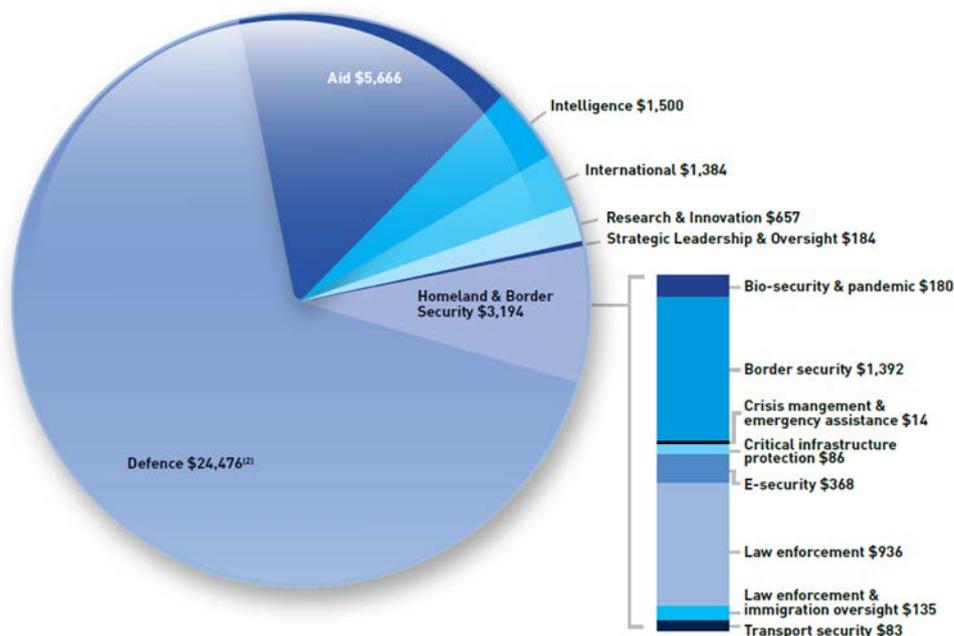|	
Stockpiles, logistics and distribution	The Australian Government has a coordinated approach to providing assistance to State and Territory governments and maintains a national stockpile of essential equipment, medical treatments and supplies required to respond to a crisis. Government also partners with the transport industry and the food sector to ensure the continuation of resource availability and food supply chains during a crisis or disruption. Internationally, Australian disaster assistance for developing countries is enabled by the deployment of personnel, provision of humanitarian assistance, and deploying humanitarian stores through Rapid Response Teams. Australia also maintains stocks of critical equipment at strategic sites for rapid overseas deployment.

Part 3: Enhancing national security capability

The Australian Government has made a strong commitment to Australia's national security capability.

To ensure the best possible capability outcomes, decision-makers need to have the most comprehensive information available when considering how best to direct available resources.

In 2013-14 the Australian Government will spend over $12.5 billion on national security, directed towards intelligence, diplomacy, aid, border and aviation security, counter-terrorism, cyber and identity security, law enforcement, and emergency management. The Government will also spend over $24 billion on defence.

Figure 2 2013-14 National Security Budget ($m)[1]

Aid $5,666
Intelligence $1,500
International $1,384
Research & Innovation $657
Strategic Leadership & Oversight $184
Homeland & Border Security $3,194
Defence $24,476[2]

Bio-security & pandemic $180
Border security $1,392
Crisis mangement & emergency assistance $14
Critical infrastructure protection $86
E-security $368
Law enforcement $936
Law enforcement & immigration oversight $135
Transport security $83

(1) Figures sourced from the 2013-14 Budget.
(2) The total funding for Department of Defence is $25,386 million, however the Department of Defence contribution to Intelligence, Research and Innovation has been captured in total spends of their respective categories.

The *National Security Strategy* highlights Australia's increasingly complex and interconnected strategic environment. The eight pillars outlined in the strategy encapsulate activities across this environment and reflect the concerted and

coordinated effort across government, business and the community to achieve national security objectives.

The Government will continue to apply effort across all eight pillars of Australia's national security. However, in support of these objectives, the Government has identified three priorities to which national security agencies will dedicate additional effort over the next five years:

- **Enhanced regional engagement** in support of security and prosperity in the Asian Century.
- **Integrated cyber policy and operations** to enhance the defence of our digital networks.
- **Effective partnerships** to achieve innovative and efficient national security outcomes

The strategy also outlined two near-term areas of focus for the national security community: Afghanistan and the United Nations Security Council. To ensure we meet our national security objectives and fulfil our international obligations a concerted whole-of-government effort will be required on both these fronts over the next two years.

The following sections and supporting case studies highlight ways in which we are applying our efforts across the national security community in support of the National Security Strategy's five year priorities.

Enhanced regional engagement

As identified in the *National Security Strategy* and the *Australia in the Asian Century White Paper*, Australia's strategic and economic future is tied to the Asia-Pacific region. The continued stability of the region remains a priority for the Australian Government.

To ensure we continue to be well placed to contribute positively to the regional security environment, we will place a greater emphasis on intensifying our regional relationships over the next five years - this will rely on our strong liaison networks.

Australia will continue to strengthen our capability and support to fragile and at-risk areas to promote regional stability.

Australia's regional engagement efforts are underpinned by strong multidimensional relationships with our international partners and our significant personnel, security and

physical infrastructure including our international network of diplomatic and consular posts.

Case study: The Jakarta Centre for Law Enforcement Cooperation (JCLEC)

The Jakarta Centre for Law Enforcement Cooperation (JCLEC) is one of the most effective counter-terrorism capacity building projects in the South-East Asian region.

JCLEC is an international law enforcement and training institution located within the Indonesian National Police Academy in Semarang (central Java) and established by the governments of Indonesia and Australia in 2004. It is jointly operated by the Indonesian National Police and the Australian Federal Police, with bilateral and multilateral assistance from foreign donor countries.

It provides a wide range of training and capacity-building courses for law enforcement officers from Indonesia and other South-East Asian countries, including post blast analysis, management of serious crime, financial investigations, and criminal intelligence training. These activities are often facilitated by subject matter experts from the Australian law enforcement community.

The Centre has state-of-the-art training facilities together with high quality staff and student accommodation.

Although JCLEC was established as a bilateral initiative between Australia and Indonesia, Australia has contributed over $36 million since 2004 to support the Centre's development and operations. On the strength of its international reputation as a counter-terrorism centre of excellence, it has provided a valuable entry point to South-East Asia for international counter-terrorism donors:

- several other donors have provided valuable support, including financial assistance, funding specific counter-terrorism courses or seconding law enforcement training officers to run counter-terrorism courses
- contributors have included the United Kingdom, Canada, Denmark, the European Commission, Italy, France, Germany, the Netherlands, New Zealand, Spain, Sweden, the United States and other countries.

As at 30 April 2013 JCLEC has provided training to more than 13,225 officials from 68 countries.

JCLEC is a regional resource, and Australia and Indonesia encourage the involvement of third countries from the region.

As a key regional counter-terrorism centre, JCLEC has also supported a range of multilateral initiatives to enhance counter-terrorism capacity and to counter the regional terrorist threat.

JCLEC's mandate is principally to build counter-terrorism cooperation and capacity in South-East Asia. However, South Asian and Pacific law enforcement officials and officials from other parts of the world have also trained there.

Integrated cyber policy and operations

The increasing availability and low cost of new technologies means our adversaries are becoming more sophisticated. Our national security agencies must develop new ways of working, and continue to invest in and develop technology solutions and analytical capability to ensure our situational awareness, legislative framework and response capability remain ahead of the threat. This will require not only close cooperation across government and strong links between government and the private sector.

Cyber operations and intrusions can be relatively easy and cheap to conduct. Because of this it is imperative that our agencies have the security intelligence and cyber expertise to develop protection against such possibilities. This will require close cooperation with the private sector—both in the general commercial world and from cyber service providers.

Australia must be a hard target for malicious cyber activity, promote responsible digital citizenship and sustain our constructive contribution to the international security dimensions of cyber, in particular the debate about norms of behaviour for cyberspace.

Case study: Australian Cyber Security Centre

Every day, Australian governments, businesses and individuals face a range of cyber-related threats. If left unchecked, these have the potential to undermine confidence in our social and economic stability and our prosperity. On 23 January 2013, the Australian Government announced that an Australian Cyber Security Centre (ACSC) would be established. Located in the Ben Chifley Building, the ACSC will form the hub of the Government's cyber security efforts and will boost Australia's ability to protect against cyber-attacks.

The ACSC will bring together existing cyber security operational capabilities from the Australian Signals Directorate, Defence Intelligence Organisation, Australian Security Intelligence Organisation, the Attorney-General's Department's Computer Emergency

Response Team (CERT) Australia, Australian Federal Police and the Australian Crime Commission.

The centre will analyse the nature and extent of cyber threats, and lead the Government's response to cyber incidents. It will work closely with critical infrastructure sectors and industry partners to protect valuable networks and systems. The centre will also provide advice and support to develop strategies to counter cyber threats.

Effective partnerships

Australia's *National Security Strategy* encourages agencies to develop innovative and effective approaches to how they use information and engage with partners, including industry and the wider Australian community, to better harness our capabilities to combat evolving threats and achieve national security outcomes.

The Australian Government will continue to foster cooperation at all levels of government and in the private sector and will support our international partners through developing complementary legislation, policy and procedures to meet national security objectives.

National security agencies will continue to strengthen inter-agency collaboration to improve information sharing. Agencies will be better connected, work more cooperatively, foster innovation and harness existing capabilities.

The Government's ability to prevent and disrupt terrorist attacks within Australia relies on coordinated and cooperative relationships between our intelligence, security and law enforcement agencies and with international partners, business and communities. National security agencies must be able to seamlessly integrate efforts to detect, investigate and disrupt plots from would-be adversaries and establish productive relationships based on mutual interest.

The Government has made significant progress in strengthening the information sharing capabilities and promoting interoperability among national security agencies. This is occurring both within the Australian Government and between Commonwealth and State and Territory agencies with responsibility for law enforcement and managing emergencies within their jurisdictions.

Fusion centres have been an important step toward greater collaboration between Government agencies. Recent developments in this area include establishing the

National Criminal Intelligence Fusion Capability in July 2010. This capability brings together people from a range of Government agencies to provide a comprehensive picture of the targets, risks, threats and vulnerabilities associated with organised crime.

The *National Security Information Environment Roadmap: 2020 Vision* sets out the Australian Government's ten-year plan to transform the way agencies organise, analyse and share information. This will ensure the right people can access the right information quickly, securely and from the right sources, providing decision makers with the best possible advice.

The Australian Government's approach to enhancing the resilience of our critical infrastructure continues through effective engagement with business and the owners and operators of critical infrastructure. The Trusted Information Sharing Network for Critical Infrastructure Resilience provides an environment where business and government can share vital information on security issues relevant to the protection of our critical infrastructure and the continuity of essential services in the face of all hazards.

In partnership with business, the Australian Government continues to share information on priority risks with key industry sectors via the Trusted Information Sharing Network, the ASIO Business Liaison Unit and the Business Government Advisory Group.

In partnership with communities, the Australian Government is working to address factors that make people vulnerable to extremist influences, including recruitment by terrorists. While there is no one particular path that leads to violent extremism, extremists often exploit social and economic conditions and individual vulnerabilities to recruit and motivate others.

The overwhelming majority of Australians reject violent extremism but many may not have the information they need to challenge it. The Government's *Countering Violent Extremism Strategy (2011)* is designed to build Australia's resilience to extremist ideologies. It focuses on promoting the role community leaders can play in preventing radicalisation before a law enforcement response might be needed.

Case study: National Border Targeting Centre

As international trade and travel grows, it is increasingly important that agencies share data, information and intelligence to target high risk passengers and goods crossing our borders.

Around 30 million passengers passed through our international airports last year. That number is expected to increase to 40 million by 2017. Incoming air cargo is expected to increase by 125% over the same period.

Australian law enforcement agencies have advised that intelligence and targeting is the key to seizing drugs and other contraband on the streets and at the border. For example, 85% of seizures of firearms and firearm parts and over 90% of drug and precursor seizures at the border are the result of intelligence developed by Customs and Border Protection and other law enforcement agencies in Australia and overseas.

To enhance this work, the Government is establishing a National Border Targeting Centre. It will provide a basis for the Australian Customs and Border Protection Service to work more closely with the Department of Immigration and Citizenship to target high risk international passengers and cargo, using an intelligence-led, risk-based approach.

The centre will also provide a base for co-locating staff or connecting information systems of agencies such as the Australian Federal Police, the Australian Security Intelligence Organisation, the Australian Crime Commission, the Department of Foreign Affairs and Trade (Australian Passport Office), the Department of Agriculture, Fisheries and Forestry and the Department of Infrastructure and Transport. Staff in the centre will also work alongside staff from targeting centres in the United States, Canada, the United Kingdom and New Zealand.

The National Border Targeting Centre will improve the ability of all agencies to work together to identify and deal with the border risks posed by the growing number of travellers and goods. It will ensure border and law enforcement agencies have the information and intelligence they need to target threats to the border and the community.

Conclusion

As the economic and strategic influences in our region of the world continue to shift, Australia's approach to national security must vary accordingly. Our changing domestic and international environment presents important national security challenges as well as opportunities that we must seize. Ensuring that our capability planning remains flexible and innovative and supports robust policy development is key to achieving this objective.

Under the strong strategic direction set by the *National Security Strategy*, national security capability planning will continue to support the strategy's eight pillars with additional effort guided toward the priorities of enhanced regional engagement, integrated cyber policy and operations, and effective partnerships. Capability planning provides Government with a clear picture of our existing capability and where effective partnerships can be made to achieve these priorities. The Australian Government's approach also enables opportunities for collaborative research and development activities across the national security community.

Capability planning adds an important layer to the strong foundation of Australia's national security, enabling the Australian Government to consolidate and strengthen its existing capability, while also allowing new and emerging opportunities to be pursued to ensure a safe and secure Australia and to shape and promote a more stable, prosperous and secure region and world.

Useful links

Australia in the Asian Century White Paper (2012)
www.asiancentury.dpmc.gov.au

Australian Emergency Management Handbook Series - Disaster Health (2011)
www.em.gov.au

Australian emergency management arrangements
www.em.gov.au

Australian Government Natural Disaster Relief and Recovery Arrangements
www.disasterassist.gov.au

Australian Government's Critical Infrastructure Resilience Strategy (2013)
www.tisn.gov.au

CERT Australia - national computer emergency response team
www.cert.gov.au

Commonwealth Organised Crime Strategic Framework Overview
www.ag.gov.au

Defence Capability Plan (2012)
www.defence.gov.au

Defence White Paper (2013)
www.defence.gov.au

National Counter-Terrorism Plan (3rd Edition, 2012)
www.nationalsecurity.gov.au

National Health Emergency Response Arrangements (2011)
www.health.gov.au

National Security Science and Innovation Strategy (2009)

www.dpmc.gov.au

National Security Public Information Guidelines (2011)

www.nationalsecurity.gov.au

National Terrorism Public Alert System

www.nationalsecurity.gov.au

Strong and Secure: A Strategy for Australia's National Security (2013)

www.dpmc.gov.au