Australian Government

CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY

Australian Government

CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY

ISBN: 978-1-921725-25-8

TABLE OF CONTENTS

MINISTER'S FOREWORD 3

EXECUTIVE SUMMARY 4

1. INTRODUCTION 6

2. THE AUSTRALIAN GOVERNMENT'S APPROACH TO CRITICAL INFRASTRUCTURE RESILIENCE 8

Aim 8

Definition 8

Policy Rationale 9

Role of the Australian Government in CIR 11

3. POLICY OBJECTIVES 12

4. STRATEGIC IMPERATIVES TO ACHIEVE THE AIM AND OBJECTIVES 15

5. SUCCESS CRITERIA AND REVIEW OF THIS STRATEGY 25

6. CONCLUSION 27

GLOSSARY 28

APPENDIX A: SUPPORT FOR THE SHIFT TO RESILIENCE FROM PAST POLICY REVIEWS 30

APPENDIX B: ROLES OF AUSTRALIAN GOVERNMENT AGENCIES 31

MINISTER'S FOREWORD

The resilience of our critical infrastructure is vital to the Australian way of life that we know and value.

Critical infrastructure underpins the delivery of essential services such as power, water, health, communications systems and banking.

We are a vibrant, prosperous nation that enjoys the many benefits of modern living. But along with these benefits, there are a range of risks that also must be managed.

These risks – from natural disasters, to equipment failure and crime – can damage or destroy critical infrastructure as well as disrupt the essential services that are provided by these assets, networks and supply chains.

Such an incident could significantly affect all Australians because of our reliance on critical infrastructure, which is of major importance to businesses, governments and communities.

A resilience based approach to critical infrastructure is vital so we can better adapt to change, reduce our exposure to risk and learn from incidents when they occur.

The responsibility for the continuity of critical infrastructure is shared by all governments and by owners and operators.

This Strategy provides the Australian Government's approach to critical infrastructure resilience.

It has a strong focus on business-government partnerships. It also shows how committed the Australian Government is to working with owners and operators and State and Territory governments to achieve complementary and mutually beneficial outcomes.

I am sure you will find this Strategy informative, and that you share my enthusiasm and optimism as we move forward to create a more resilient Australia.

Robert McClelland

The Hon Robert McClelland MP

Attorney-General

EXECUTIVE SUMMARY

This Australian Government recognises the importance of critical infrastructure and the essential services for everyday life provided by parts of this critical infrastructure.

This Strategy describes the Australian Government's approach to enhancing the resilience of our critical infrastructure to all hazards. More resilient critical infrastructure will also help to achieve the continued provision of essential services, and support Australia's national security, economic prosperity and social and community wellbeing. This Strategy encourages and enables critical infrastructure organisations, through a range of initiatives and activities, to better manage both foreseeable and unforeseen or unexpected risks to their critical infrastructure assets, supply chains and networks (the objectives of this Strategy).

A significant proportion of Australia's critical infrastructure is privately owned or operated on a commercial basis. In most cases, the owners and operators of critical infrastructure are best placed to manage risks to their operations and determine the most appropriate mitigation strategies. The Australian Government recognises that the best way to enhance the resilience of critical infrastructure is to partner with owners and operators to share information, raise the awareness of dependencies and vulnerabilities, and facilitate collaboration to address any impediments. The Australian Government has established the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience (CIR) as its primary mechanism to build a partnership approach between business and government for CIR. The Australian Government has the unique ability to bring critical infrastructure sectors together in a non-competitive environment to discuss and address vulnerabilities within sectors on a national or cross-jurisdictional basis as well as enabling the identification of cross-sector dependencies. While the business-government partnership is the cornerstone of the CIR approach, there are a number of other important imperatives that contribute to the collective effort.

This Strategy has six complementary strategic imperatives to build CIR and achieve the Australian Government's aim and objectives:

- operate an effective business-government partnership with critical infrastructure owners and operators
- develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience
- assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies
- provide timely and high quality policy advice on issues relating to critical infrastructure resilience
- implement the Australian Government's Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators, and
- support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate.

Implementation of this Strategy is achieved through each strategic imperative and its related activities (see the CIR Strategy Supplement for more details). While some of these activities are a continuation of the previous Critical Infrastructure Protection Program, there have been enhancements to the approach and the addition of an important new strategic imperative, organisational resilience. A resilience approach to managing the risks to our critical infrastructure encourages organisations to develop a more organic capacity to deal with rapid-onset shock. This is in preference to the more traditional approach of developing plans to deal with a finite set of scenarios, especially in the context of an increasingly complex environment.

While this Strategy presents the Australian Government's approach to CIR, it acknowledges that achieving CIR is a shared responsibility across governments and the owners and operators of critical infrastructure.

1. INTRODUCTION

"The time has come for the protection mindset to be broadened – to embrace the broader concept of resilience ... The aim is to build a more resilient nation – one where all Australians are better able to adapt to change, where we have reduced exposure to risks, and where we are all better able to bounce back from disaster".

The Hon Robert McClelland MP, Attorney-General, 9 December 2009,
Critical Infrastructure Advisory Council.

The security environment that we face today and into the future is increasingly fluid and shaped by a dynamic mix of continuing and emerging challenges and opportunities. The concept of national security has evolved and broadened to include non-traditional threats such as organised crime, natural disasters and pandemics.[1] These threats impact on all aspects of national security, including critical infrastructure and the continuity of essential services. This new, complex and interconnected national security environment necessitates a broader approach to risk management which is achievable through a resilience paradigm.

National Security Statement

On 4 December 2008, the Prime Minister delivered Australia's inaugural National Security Statement to the Parliament. The Statement outlines five enduring national security interests that constitute the Australian Government's national security objectives:

- maintaining Australia's territorial and border integrity
- promoting Australia's political sovereignty
- preserving a cohesive and resilient society and strong economy
- protecting Australians and Australian interests both at home and abroad, and
- promoting a stable, peaceful and prosperous international environment, particularly in the Asia-Pacific region, together with a global rules-based order which enhances Australia's national interests.

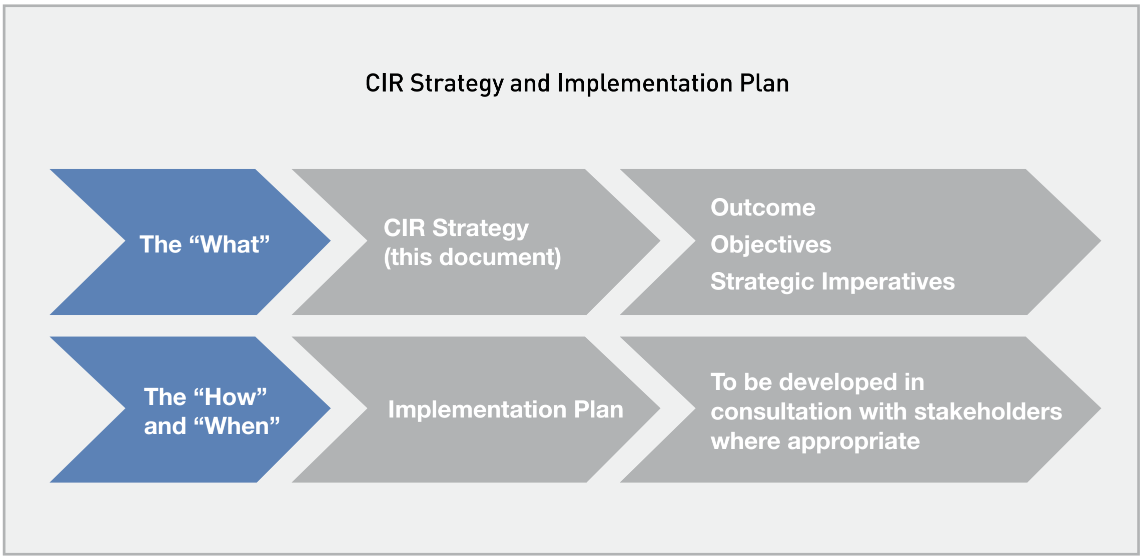
Parts of our critical infrastructure provide essential services on which business, government and the community depend. The Statement recognises that a significant proportion of our critical infrastructure is owned by the private sector or operated on a commercial basis. It identifies the need for governments to work with business to ensure the resilience of critical infrastructure in the face of all hazards and makes an important contribution to preserving a cohesive and resilient society and economy.

Box 1.1

[1] While many of these issues were previously addressed through other areas of work, the broadening of national security has meant that they have only recently been brought under the national security umbrella.

This Strategy articulates the various critical infrastructure activities the Australian Government undertakes, ranging from how it engages with business, through to its interactions with other governments (international and domestic). While this Strategy presents the Australian Government's approach to critical infrastructure resilience (CIR), it also acknowledges that CIR is a shared responsibility across governments and the owners and operators of critical infrastructure.

A separate implementation plan will be developed which will describe, in detail, how the Australian Government plans to execute this Strategy. Development of the implementation plan will be coordinated by the Attorney-General's Department (AGD), in consultation with business and government stakeholders, as appropriate.



CIR Strategy and Implementation Plan

Box 1.2

2. THE AUSTRALIAN GOVERNMENT'S APPROACH TO CRITICAL INFRASTRUCTURE RESILIENCE

The Australian Government recognises the importance of critical infrastructure, including those parts that provide essential services for everyday life (such as energy, food, water, transport, communications, health and banking and finance). A disruption to critical infrastructure could have a range of serious implications for business (including other critical infrastructure), governments and the community.

Aim

The aim of this Strategy is the continued operation of critical infrastructure in the face of all hazards, as this critical infrastructure supports Australia's national defence and national security, and underpins our economic prosperity and social wellbeing. More resilient critical infrastructure will also help to achieve the continued provision of essential services to the community.

Definition

The Australian, State and Territory governments define critical infrastructure as:

> *those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.*[2]

It is important to note that some elements of critical infrastructure are not assets, but are in fact networks or supply chains. For example, bringing food from the paddock to the plate is dependent not only on particular key facilities, but also on a complex network of producers, processors, manufacturers, distributors and retailers and the infrastructure supporting them.

In the context of critical infrastructure, resilience refers to:

- coordinated planning across sectors and networks
- responsive, flexible and timely recovery measures, and
- the development of an organisational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly.[3]

In this way, building capacity in organisations to be agile, adaptive and to improve by learning from experience is part of the concept of CIR.

[2] In this context, significant means an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia's international competitiveness, or impedes the continuity of government and its services

[3] Council of Australian Government's Senior Officers' Meeting Review of National CIP Arrangements, Final Report 2009

Policy Rationale

It is vital that owners and operators of critical infrastructure, both the private sector and government organisations, are able to plan for, withstand and respond to a broad range of threats and hazards, including pandemics, negligence, accidents, criminal activity, cyber attack, and natural disasters that have the potential to disrupt their operations. Further, a disruption to critical infrastructure in one sector could have severe cascading impacts on critical infrastructure in other sectors. The critical infrastructure networks and systems are themselves growing in complexity, and are operating in an increasingly complex environment. In this environment, the owners and operators of critical infrastructure need to be able to respond and adapt to foreseeable and unforeseen or unexpected risks and be able to continue to support other businesses, governments and the community.

Community Expectations

The community expects that the Australian Government is engaged on issues that could, or do in fact, significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security. To meet the national interest, the actual extent of the Australian Government's role or interest in a particular issue will often depend on the likelihood and consequence of the risk or the actual incident.

Accordingly, the Australian Government is a key stakeholder in understanding the vulnerabilities and dependencies in and across critical infrastructure sectors, and the risk mitigations being applied. The Australian Government also facilitates national coordination where there are cross-jurisdictional issues, international treaty obligations, or where an incident would have national consequences or require a national response.

Disaster Resilience

Given the regularity and severity of natural disasters, the Council of Australian Governments (COAG) recognised at their meeting in December 2009 that a national, coordinated and cooperative effort is required to enhance Australia's capacity to withstand and recover from emergencies and disasters.

Development of a National Disaster Resilience Strategy

On 7 December 2009, the Council of Australian Governments (COAG) agreed to adopt a whole-of-nation resilience-based approach to disaster management which recognises that a national, coordinated and cooperative effort is required to enhance Australia's capacity to withstand and recover from emergencies and disasters. This agreement recognises that disaster resilience is a shared responsibility for individuals, households, businesses and communities, as well as for governments.

COAG also agreed to establish a new National Emergency Management Committee (NEMC), providing a clear mandate to drive and coordinate national policies and capability development in relation to emergency management. This mandate includes the ability to influence and facilitate decisions beyond the remit of the traditional emergency management portfolio. The first task of the NEMC is to bring together the representative views of all governments, business, the non-government sector and the community into a comprehensive National Disaster Resilience Strategy.

Disaster resilience would be strengthened where communities have continued access to essential services provided by some critical infrastructure organisations. This is the link between the CIR Strategy and disaster resilience.

Box 2.1

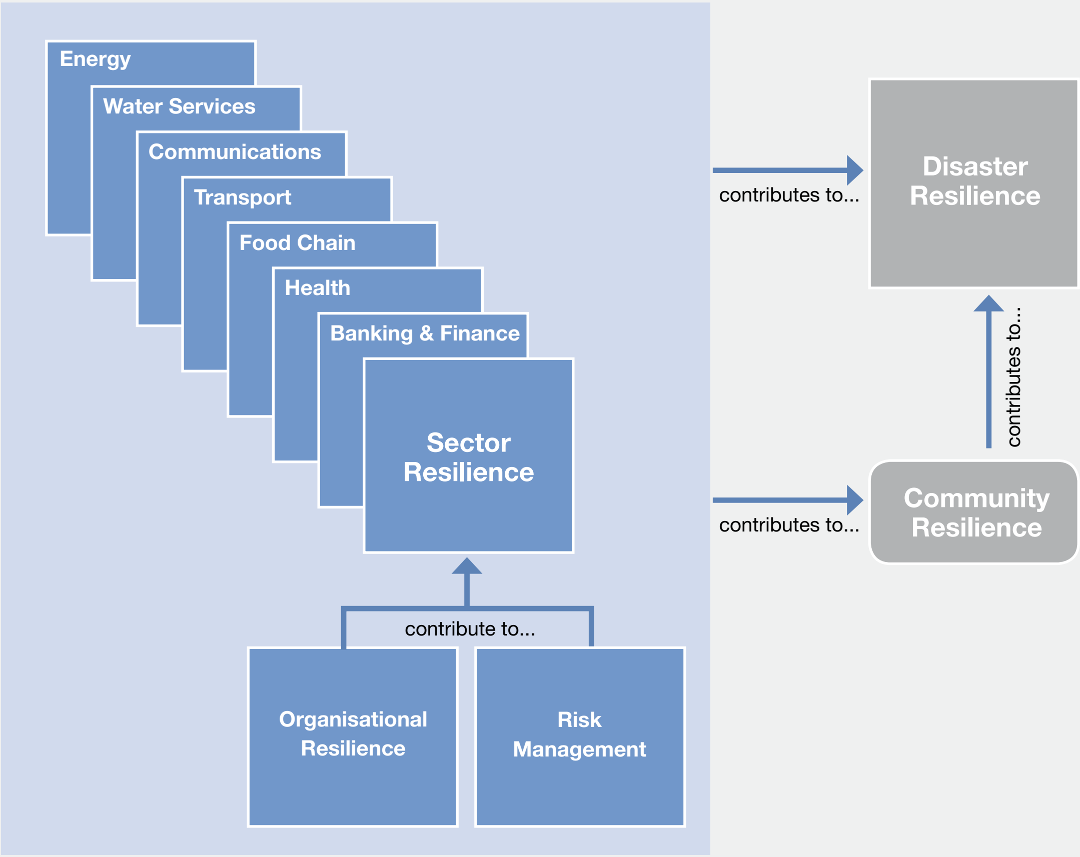
There are direct benefits to business in being more resilient to hazards. These include improved reputation, minimisation of loss of revenue from failure to provide a service, minimisation of contractual penalties from supply disruption and a reduced exposure to litigation. Therefore, it can be argued that enhancing resilience is good business.

Sector and Cross-Sector Engagement

The Australian Government's sectoral focus in engaging with the owners and operators of critical infrastructure also provides substantial benefits to critical infrastructure businesses in each sector. This is because of the issue of shared risk. For example, if one food company is affected by a contamination or extortion incident, spill-over impacts are likely to occur to critical infrastructure businesses in the same sector. By working together on common issues, businesses within a sector, and across sectors, can enhance their resilience to various hazards.

The Australian Government also has the unique ability to bring critical infrastructure sectors together in a non-competitive environment to discuss and address cross-sectoral vulnerabilities within supply chains on a national and cross-jurisdictional basis. This cross-sectoral work makes a significant contribution to critical infrastructure resilience by recognising and addressing the cascade or knock-on impacts that can spread from one sector to another.

**Relationship Between Critical Infrastructure Resilience,
Disaster Resilience and Community Resilience**



Box 2.2

The policy rationale for shifting to CIR is supported by a number of recent reviews of critical infrastructure arrangements, as summarised in **Appendix A.**

Role of the Australian Government in CIR

While the majority of critical infrastructure in Australia is owned or operated by the private sector and the States and Territories, the Australian Government has a complex set of roles, responsibilities and interests in CIR. The Australian Government is:

- an owner and operator of critical infrastructure
- the regulator of security in some industries (i.e. aviation and maritime)
- the industry regulator in other sectors but not necessarily for the 'protection' of critical infrastructure from acts of terrorism
- responsible for operating the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience (see Box 4.1), which provides national level forums for owners and operators of critical infrastructure to discuss critical infrastructure vulnerabilities with relevant government agencies
- the primary source of security threat assessments, and
- a source of research, scientific and technical advice relevant to the protection and resilience of critical infrastructure.

The initiatives under this Strategy assist critical infrastructure organisations to better prevent, prepare, respond to and recover from an incident. However, this Strategy does not focus on the existing response arrangements that are in place in the Australian Government, the States and Territories, and critical infrastructure organisations.

AGD is the lead agency for critical infrastructure policy across the Australian Government. A range of agencies directly contribute to the Australian Government's CIR Strategy. A description of the role of relevant Australian Government agencies in this Strategy is at **Appendix B.**

3. POLICY OBJECTIVES

The Australian Government's policy objectives for CIR build on the solid foundation provided by the previous Critical Infrastructure Protection (CIP) Program. In addition, the CIR Strategy adds a new dimension – organisational resilience – to help achieve the resilience of critical infrastructure in the face of unforeseen or unexpected hazards. The objectives of the CIR Strategy are:

1. Critical infrastructure owners and operators (including the Australian Government) are effective in managing foreseeable risks to the continuity of their operations, through an intelligence and information led, risk informed approach.

This intelligence and information led, risk informed approach seeks to ensure there are adequate levels of protective security for Australia's critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements.

The owners and operators of critical infrastructure are responsible for managing the risks to their operations that might have a material, financial or reputational impact on the organisation, or harm staff, customers or other parties. They do this through appropriate risk management practice including the development and review of business continuity plans, and the provision of adequate security for their assets.[4]

In the context of the Government's all hazards approach, the application of protective security measures is not always the most appropriate nor feasible measure to mitigate risk. For example, it is not possible to protect every kilometre of linear assets such as pipelines or high voltage electricity transmission cables. Therefore, the all hazards approach to CIR requires an intelligence and information led, risk informed methodology, where the application of protective security measures is regarded as contributing to a more complex and dynamic equation for adequately managing the risks to critical infrastructure.

The premise behind the approach is that through the provision of intelligence and information, owners and operators of critical infrastructure are given the opportunity to adjust protective security and other arrangements to mitigate risks in a changed threat environment. A key benefit of this all hazards, intelligence and information led, risk informed approach is the ability to clearly differentiate security environments (for example, remote rural critical infrastructure versus inner city installations and facilities) and the appropriateness of different measures and responses. This approach offers a basis to deal with enduring threats such as terrorism and climate change, as it is affordable and manageable for the owners and operators and thereby builds more resilient critical infrastructure.

[4] The Australian Government advocates the use of the Australian and New Zealand Standard for Risk Management (AS/NZS ISO 31000:2009) by owners and operators of critical infrastructure.

2. Critical infrastructure owners and operators enhance their capacity to manage unforeseen or unexpected risk to the continuity of their operations, through an organisational resilience approach.

It could be argued that all organisations should strive to be more resilient. However, many critical infrastructure organisations are different from other organisations in their role of providing essential services on which the community depends. Generally, other organisations are able to take out insurance or put in place other 'hedging' arrangements to manage risk. If there was an unforeseen or unexpected threat or hazard, other organisations could make a decision to discontinue normal operations until the threat dissipated or things returned to normal. However, given the reliance of business, governments and the community on the essential services provided by many critical infrastructure organisations, this approach is not appropriate and the Government has a role to assist critical infrastructure organisations enhance their ability to manage unforeseen or unexpected hazards.

Traditional approaches to risk management require a good understanding of likelihood and consequence. However, because of the growing complexity of critical infrastructure systems and networks and the environments in which they operate, including zero inventory systems and global supply logistics, it is difficult for individual owners and operators to fully comprehend all relevant vulnerabilities and threats. As complexity increases, owners and operators are forced to make decisions on increasingly imperfect information. An approach that builds organic capacity in organisations to unforeseen risks and threats is therefore necessary to expand the way all hazards are managed by critical infrastructure owners and operators.

The Australian Government's approach to CIR goes beyond risk management and business continuity planning (which to a large extent only addresses *reasonably foreseeable* risks) to also address hazards and risks that are *unforeseen or unexpected* (see Box 3.1). The resilience approach builds capacity within organisations to not only effectively respond to a crisis, but also be able to learn and adapt from an event.

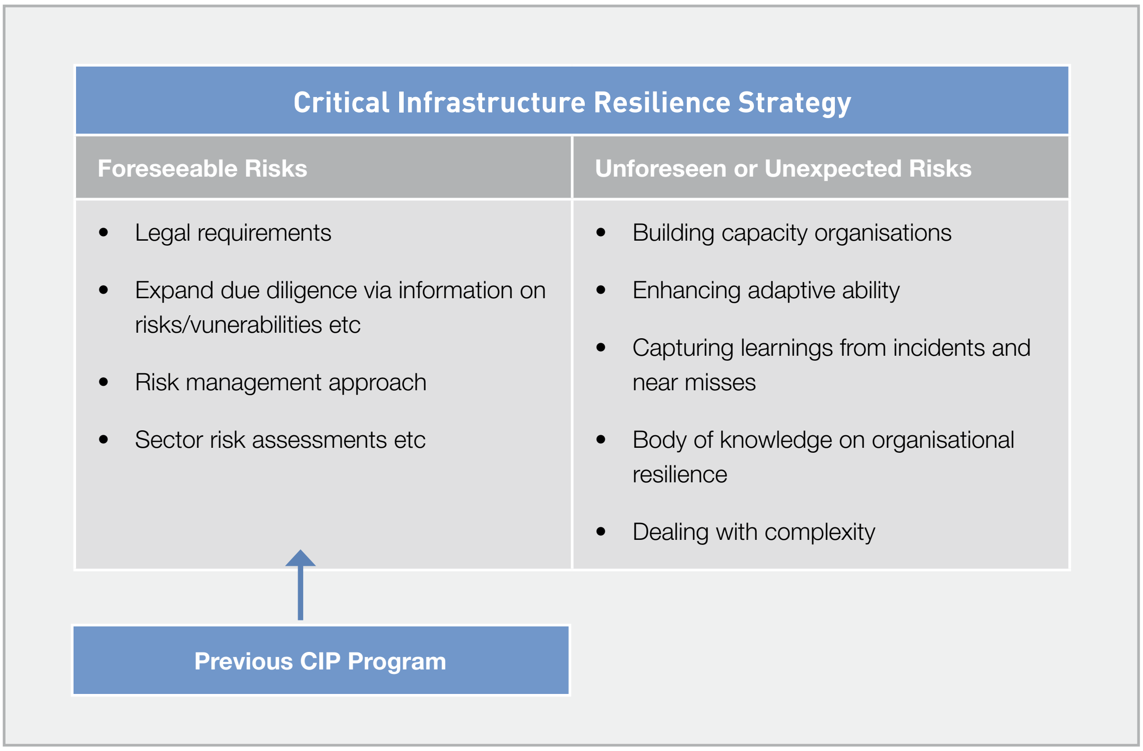
A resilience approach to managing the risks to critical infrastructure encourages organisations to develop a more organic capacity to deal with rapid-onset shock. This is in preference to the more traditional approach of developing plans to deal with a finite set of scenarios.

Perception bias can often permeate an organisation's thinking about foreseeable risk. This bias tends to discount scenarios that have not occurred in the recent experience of the decision maker, and bypasses a serious attempt to prove or disprove their plausibility. The constantly changing nature (and accelerating rate of change) of the economy, technology and society mean that past events are not an adequate guide to determining plausible future hazards. For example, the importance of the internet to business has grown exponentially since the 1990's, so any historical analysis is unlikely to be an absolute guide for future planning.

Similarly, an approach based on writing plans for specific events can lead to an overly rigid response that emphasises centralised decision making, which in turn demands leaders to have complete knowledge and expertise and constant communication with responders. It is argued that organisations that build organisational resilience through distributed decision making, unified by a strong sense of ownership and purpose over the response priorities, and aided by adaptable tools and techniques, can give those organisations an enhanced ability to deal with both the foreseeable and unforeseen events.

Scenario based planning still plays an important part in assessing whether organisations have developed an adequate resilience capacity and in choosing the best value-for-money tools. All decision makers, however, need to see all hazard risk mitigation and response as part of their role, and be empowered to carry it out. Tools and techniques that are part of normal business will be more successful than those that are only used when a specific plan is activated. This gives organisations a greater ability to adapt to events that may have been unforeseen or excluded from planning as being very low likelihood.

In this way, CIR is achieved by undertaking traditional risk management/business continuity practices AND organisational resilience initiatives.



Critical Infrastructure Resilience Strategy

Foreseeable Risks	Unforeseen or Unexpected Risks
• Legal requirements • Expand due diligence via information on risks/vunerabilities etc • Risk management approach • Sector risk assessments etc	• Building capacity organisations • Enhancing adaptive ability • Capturing learnings from incidents and near misses • Body of knowledge on organisational resilience • Dealing with complexity

Previous CIP Program

Box 3.1

The Non-Regulatory Approach

To achieve these objectives, the Australian Government generally takes a non-regulatory approach to critical infrastructure. This approach recognises that in most cases, the owners and operators of critical infrastructure are best placed to manage risks to their operations and determine the most appropriate mitigation strategies. Although certain sectors of critical infrastructure are regulated to strengthen security of specific assets against certain hazards and to comply with international treaty obligations, generally regulation is not suitable for critical infrastructure as the identification of minimum security benchmarks or regulations across industry can be difficult, even within specific sectors.

4. STRATEGIC IMPERATIVES TO ACHIEVE THE AIM AND OBJECTIVES

AGD coordinates the implementation of the CIR Strategy in partnership with a number of Australian Government agencies, and in tailored collaboration with State and Territory governments and the private sector. Implementation is achieved through six complementary strategic imperatives (or work streams). Further, a range of activities have been identified to help achieve each strategic imperative (see the CIR Strategy Supplement).

Strategic Imperative 1: Operate an effective business-government partnership with critical infrastructure owners and operators

A significant proportion of Australia's critical infrastructure is privately owned or operated on a commercial basis. As such, a business-government partnership is required to help build confidence and reliability in the continued operation of critical infrastructure that supports Australia's national security, economic prosperity, and social and community wellbeing, in the face of all hazards. It is important that the business-government partnership offers value and mutual benefit to the parties involved.

TISN Activity

The Australian Government has established the TISN for CIR (see Box 4.1 and the TISN Diagram). It comprises relevant business and government representatives, to raise the awareness of risks to critical infrastructure, share information and techniques required to assess and mitigate risks, and build resilience capacity within organisations. Through the TISN, business is also able to bring issues to government that are seen as impediments to achieving CIR. The TISN is the most visible component of the business-government partnership and provides an important mechanism to foster cooperation between public and private stakeholders on mutually important issues.

Trusted Information Sharing Network

The TISN was established by the Australian Government in April 2003 as a forum in which the owners and operators of critical infrastructure work together and share information on threats and vulnerabilities and develop strategies and solutions to mitigate risk.

The TISN operates on an all hazards basis. Under the CIR Strategy, it comprises seven critical infrastructure Sector Groups and two Expert Advisory Groups. TISN members include owners and operators of critical infrastructure, Australian, State and Territory government agency representatives, and peak national bodies. The TISN, through its Sector and Expert Advisory Groups, seeks to promote CIR to owners and operators, including promoting the need for investment in resilient, reliable infrastructure with market regulators.

Sector Groups

Sector Groups form the bridge between government and the individual owners and operators of Australia's critical infrastructure. Their purpose is to assist owners and operators to share information on issues relating to generic threats, vulnerabilities and to identify appropriate measures and strategies to mitigate risk.

Expert Advisory Groups (EAGs)

EAGs provide advice on broad aspects of critical infrastructure requiring expert knowledge. EAGs comprise subject matter experts from both within and outside the TISN.

Communities of Interest (CoI)

CoI provide an opportunity for cross-sectoral consultation between owners and operators and government on specific matters. CoI are convened when a specific critical infrastructure issue demands attention, and may be disbanded once the issue has been adequately addressed.

Box 4.1

Other Business-Government Partnership Activity

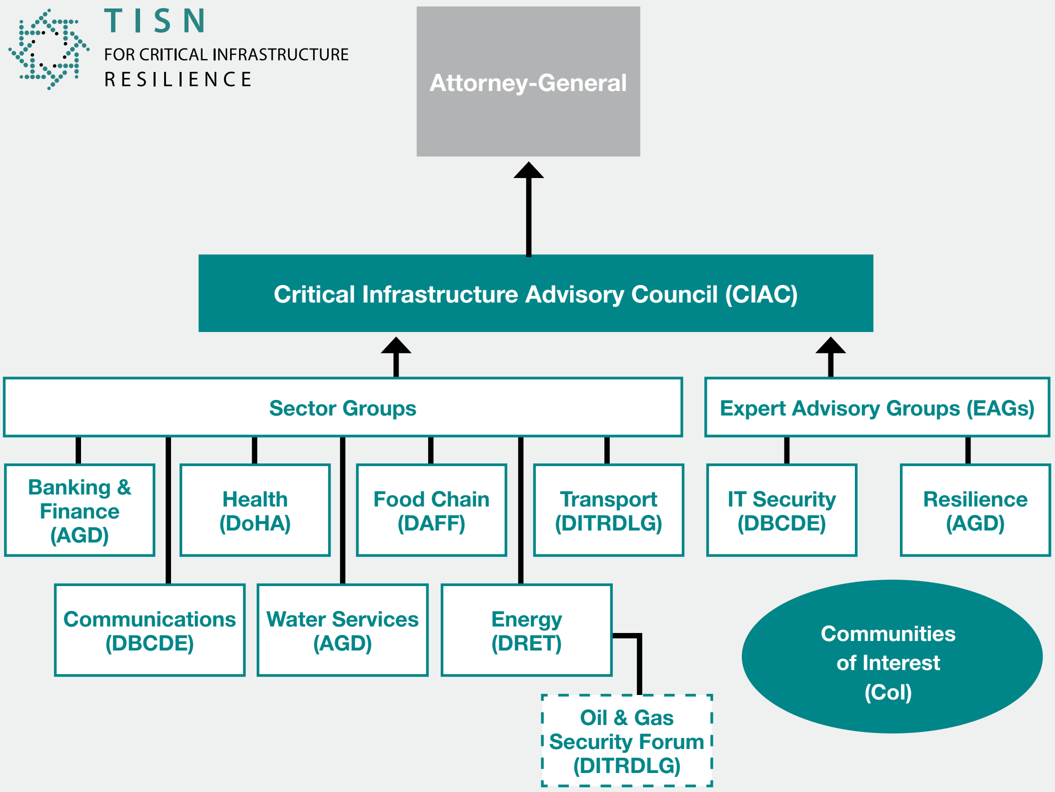
There are also a range of other activities that occur outside the TISN that support an effective business-government partnership. For example, government's provision of *intelligence and other security related information,* such as terrorism threat assessments. Much of this work is conducted through the auspices of the National Counter-Terrorism Committee (NCTC). This work contributes to increased awareness of the terrorist threat, with a broad range of critical infrastructure owners and operators being briefed. The result is that owners and operators are able to make better risk management decisions and undertake effective risk mitigation measures, in response to the threat environment.

Research and Development

The Australian Government can also connect the *research and development* requirements of stakeholders with national research priorities and facilitate partnerships with related programs both in Australia and overseas. The Government recognises the importance of engaging with the research sector to ensure policies and approaches remain responsive to change and identify and mitigate knowledge gaps identified by critical infrastructure stakeholders. The Government will foster a stronger relationship between the owners and operators of critical infrastructure and the research community to ensure the research needs of critical infrastructure stakeholders on a range of security issues are being met.

A business-government partnership is the foundation of the Australian Government's approach to CIR, and underpins all other strategic imperatives. Without a strong and robust business-government partnership, the other strategic imperatives could not be effectively achieved.

The Australian Government's Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience



AGD	Attorney-General's Department
DAFF	Department of Agriculture, Fisheries and Forestry
DBCDE	Department of Broadband, Communications and the Digital Economy
DoHA	Department of Health and Ageing
DITRDLG	Department of Infrastructure, Transport, Regional Development and Local Government
DRET	Department of Resources, Energy and Tourism

Strategic Imperative 2: **Develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience**

It is in the interests of all businesses to be resilient. However, for many critical infrastructure owners and operators the imperatives are different, as they need to ensure the continuity of essential services to the community in the face of all hazards.

The Australian Government strongly supports the concept of organisational resilience for critical infrastructure, as this approach assists owners and operators to manage unforeseen or unexpected risks, i.e. those risks that might never have been experienced by an organisation before and are therefore not categorised as foreseeable but are still plausible and may happen. This approach not only builds on and complements traditional risk management and business continuity work (which will continue to be promoted under the CIR Strategy), but also represents the most significant advance to the previous CIP Program.

Many organisations are realising that traditional corporate strategies are not protecting them from an unexpected crisis. Organisations need to be resilient, they need to be able to absorb an event that necessitates change, to adapt and continue to maintain their competitive edge and profitability.

The viability and sustainability of organisations continues to be tested in a world that is constantly changing, predominantly through globalisation which is being driven by technological innovation, and with it comes a range of new threats and challenges. Critical infrastructure systems and networks are increasingly complex and operate in a global environment of growing complexity. A resilience approach recognises the need to more effectively manage this complexity.

Attributes of organisational resilience need to be better understood and integrated into an organisation's everyday life, philosophy and culture which will ultimately help ensure survivability in times of adversity. Organisational resilience means different things to different people and there is currently no common understanding of what it entails. This strategic imperative seeks to build a common understanding and the value proposition for business to adopt an organisational resilience approach through the introduction of a number of activities and initiatives, including a resilience training program, research and development, and real life case studies.

Strategic Imperative 3: **Assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies**

The identification and analysis of cross-sectoral dependencies assists the risk management decision making of critical infrastructure organisations and helps to inform Australian Government policy on CIR.

Critical infrastructure in Australia is highly interdependent, so that failure or disruption in one sector can lead to disruptions in other sectors. For instance, owners and operators of water infrastructure rely on electricity for pumping and telecommunications for monitoring operations. Similarly, the communications industry needs electricity to run their networks, and the electricity industry needs telemetry services to run their operations and participate in the electricity market.

A cross-sectoral analysis of dependencies will assist owners and operators of critical infrastructure and the Australian Government to understand system-wide risks that are beyond the purview of individual organisations or sectors. This increases the potential for a more effective sharing of risk to cope with certain incidents. The Critical Infrastructure Program for Modelling and Analysis (CIPMA) is a key initiative in the Australian Government's efforts to enhance the resilience of Australia's critical infrastructure (see Box 4.2).

The Critical Infrastructure Program for Modelling and Analysis (CIPMA)

CIPMA is a computer-based capability which uses a vast array of data and information from a range of sources (including the owners and operators of critical infrastructure) to model and simulate the behaviour and dependency relationships of critical infrastructure systems.

CIPMA uses an all hazards approach to undertake computer modelling to determine the consequences of different disasters and threats (human and natural) to critical infrastructure. Owners and operators of critical infrastructure can use this information to prevent, prepare for, respond to or recover from a natural or human-caused hazard. CIPMA also helps government shape policies on national security and critical infrastructure resilience.

CIPMA is an important capability to support the business-government partnership, and relies on strong support from stakeholders such as owners and operators of critical infrastructure, State and Territory governments, and Australian Government agencies for its ongoing development. Importantly, CIPMA can show the relationships and dependencies between critical infrastructure systems, and the cascade impacts from a failure in one sector on the operations of critical infrastructure in other sectors.

AGD manages CIPMA and works with Geoscience Australia and other technical service providers to further develop and deliver this whole-of-government capability.

Box 4.2

Strategic Imperative 4: Provide timely and high quality policy advice on issues relating to critical infrastructure resilience

Australian Government agencies provide policy advice to relevant Ministers on a range of critical infrastructure related issues. It is now an accepted doctrine of the Australian Government that policy advice needs to be constructed through a 'whole-of-Australian Government' approach and reflect the relationship with other Government policies.

In addition, by looking over the horizon to the challenges and opportunities of the coming years, the Australian Government will be well positioned to support the business-government partnership for CIR.

Participation in the business-government partnership enables Australian Government agencies to provide better policy advice on critical infrastructure related issues. Through raising the awareness of critical infrastructure issues, including potential impediments to achieving CIR, Australian Government agencies directly involved in CIR are able to better represent stakeholder interests in the various machineries of government that are used to develop and implement Government policy and act as critical infrastructure advocates in the broader policy debate.

Accordingly, Australian Government agencies that have a role in implementing the CIR Strategy are able to influence or shape government policy initiatives that impact on critical infrastructure organisations and their ability to achieve CIR.

Strategic Imperative 5: Implement the Australian Government's Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators

Cyber security is one of Australia's top national security priorities. Australia's information and communications technologies (ICT) underpin every aspect of our modern lives, including the operation of critical infrastructure. As a result, cyber security and the resilience of our critical infrastructure are inherently linked.

The global community continues to experience an increase in the scale, sophistication and successful perpetration of cyber crime. Given the reliance of critical infrastructure organisations on ICT and the increasingly hostile cyber environment, it is essential that the implementation of the Australian Government's Cyber Security Strategy is incorporated into the CIR Strategy.

In late 2009, the Australian Government launched its inaugural Cyber Security Strategy, with the explicit aim of maintaining a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy (see Box 4.3). Integral to the Cyber Security Strategy are two mutually supporting organisations: CERT Australia and the Cyber Security Operations Centre (CSOC). CERT Australia is the Australian Government's primary mechanism for engagement with the private sector on cyber security issues.

Objectives and Priorities of the Australian Government's Cyber Security Strategy

- All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online
- Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers, and
- The Australian Government ensures its information and communications technologies are secure and resilient.

To achieve these objectives the Australian Government applies the following strategic priorities to its programs:

- Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest
- Educate and empower all Australians with the information, confidence and practical tools to protect themselves online
- Partner with business to promote security and resilience in infrastructure, networks, and services
- Model best practice in the protection of government ICT systems, including the systems of those transacting with government online
- Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests
- Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber crime, and
- Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.

Box 4.3

Strategic Imperative 6: **Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate**

Tailored Engagement

All Australian governments have an interest in protecting and ensuring the continued operation of critical infrastructure, and all have programs in their jurisdictions to support and assist the owners and operators of critical infrastructure. These programs are based on an assessment of the most relevant threats, and the capabilities and resources within each government. Given the shared responsibility for CIR, it is important each jurisdiction (including the Australian Government) has a common understanding of the others' programs. This is because parts of Australia's critical infrastructure span jurisdictional borders and there are often critical infrastructure interdependencies that spread across a number of jurisdictions. Further, many owners and operators of critical infrastructure conduct their business nationally and have an expectation that there will be a level of consistency and coordination between the critical infrastructure policy settings and activities of all governments. Therefore, there is a strong policy imperative that Australian governments collaborate and coordinate on critical infrastructure activities.

It is important to emphasise that consistency for critical infrastructure does not mean uniformity. Each jurisdiction operates within unique parameters, particularly regarding the prevailing threat environment, but also in terms of population size, market maturity, and the form and focus of business-government engagement. The Australian Government recognises the various approaches to critical infrastructure across jurisdictions and will take a tailored approach when engaging with the States and Territories. This approach is consistent with the findings of the recent review of national critical infrastructure arrangements under the auspices of COAG Senior Officers. This tailored engagement will be informed through the Australian Government's involvement in the National Critical Infrastructure Resilience Committee (NCIRC, see Box 4.4).

National Coordination

NCIRC, comprising relevant Australian Government and State and Territory officials, has been established to provide coordination of the national approach to CIR. It is a forum for high-level dialogue, collaboration and visibility of government activities relating to CIR. Outside of NCIRC, where there are issues of a bilateral nature, specific engagement between the relevant governments will take place.

All Australian governments have agreed to the *Principles and Protocols for Government Engagement with the Owners and Operators of Critical Infrastructure* (see Box 4.5). In addition, in discussions with the States and Territories on national arrangements for critical infrastructure it was noted that in the work of the TISN, issues that relate primarily to the responsibility of the States and Territories can arise. In these cases, the Australian Government has agreed that all groups in the TISN will be encouraged to refer such matters to NCIRC for consideration and response, where appropriate. Where issues arise that relate to a particular jurisdiction (including the Australian Government), Sector Group secretariats will propose that the matter be taken up directly with the relevant jurisdiction. The Australian Government will co-chair NCIRC, and AGD will provide secretariat support.

The National Critical Infrastructure Resilience Committee (NCIRC)

Purpose

The NCIRC will co-ordinate national critical infrastructure resilience activity, which includes protection activities. A key function of the NCIRC will be to provide a level of visibility and co-ordination to the critical infrastructure activities of each government.

Scope

The scope of the NCIRC would be to cover issues that require national co-ordination, such as:

a) those related to critical infrastructure assets, supply chains or networks which, if disrupted, would result in significant social or economic impacts nationally or across jurisdictions, and

b) issues of common interest which would benefit from national collaboration.

The NCIRC's mandate will be the resilience of critical infrastructure against a range of threats and hazards, including terrorism, natural disasters, pandemics, industrial incidents and supply chain interruptions. The scope of this body of work is very broad, and many extant bodies have primary responsibility for specific types of critical infrastructure incidents or issues. Accordingly, the NCIRC would not assume responsibility for all critical infrastructure issues, but rather should foster strong working relationships with such bodies.

NCIRC Functions

The NCIRC should fulfil the following functions:

- operate as a forum for national dialogue and collaboration on critical infrastructure resilience
- identify, develop, propose and promote initiatives that contribute to the resilience of critical infrastructure in Australia
- facilitate information sharing between relevant agencies to contribute to resilient critical infrastructure in Australia
- facilitate co-ordination of work on critical infrastructure resilience being undertaken through the NCTC, NEMC and other relevant bodies and agencies, and
- identify research needs and facilitate research activity to improve the resilience of critical infrastructure in Australia.

The National Critical Infrastructure Resilience Committee (NCIRC) (continued)

Accountability and Reporting Structures

In order to ensure that there is an appropriate level of accountability to Commonwealth, State and Territory Ministers, the NCIRC will report to COAG SOM annually about is major achievements, work progressed and direction for the following year. It will also provide support to, or be tasked by, the following COAG Senior Officials Committees:

- NCTC: for issues relating to terrorism. The NCIRC will integrate terrorism specific national critical infrastructure protection activity, oversighted by the NCTC
- NEMC: for issues relating to national disasters, and
- Other COAG Senior Officials Committees: for specific issues other than terrorism and natural disasters/emergency management.

Relationship with CIAC

The NCIRC would have an informal relationship with the CIAC. The CIAC may refer issues to the NCIRC where a nationally consistent approach is required. The NCIRC may also identify issues that require a cross sectoral business perspective and seek advice from the CIAC.

Representation

The NCIRC should be made up of senior officials from the Commonwealth, States and Territories, usually including a First Ministers representative.

Box 4.4

Principles and Protocols for Government Engagement with Critical Infrastructure Owners and Operators

Key principles

1. Effective critical infrastructure programs are based on a partnership approach between the owners and operators of critical infrastructure, and all levels of government.

2. Within an all hazards approach, the engagement of Australian governments on critical infrastructure is focussed on assisting owners and operators of critical infrastructure to increase their resilience and protect their assets. The protection of critical infrastructure from acts of terrorism is an area of special focus.

Protocol of engagement

3. Australian governments will, in engaging with the owners and operators of critical infrastructure:

    a. take into account the interdependencies, and where relevant, the cross-jurisdictional nature of critical infrastructure

    b. take into account that agencies from various levels of governments have specific roles guiding their interactions with owners and operators

    c. seek to coordinate their activities with other arms of government who are engaging the same owners and operators

    d. provide information to owners and operators regarding the purpose of their intended interaction, and the role of the agency involved

    e. minimise duplication and inconsistency in the exchange of information and provision of advice to owners and operators

    f. be cognisant of the need to match expectations to capability both from governments to owners and operators, and from owners and operators to governments, and

    g. inform relevant governments either simultaneously, or at the earliest possible opportunity, of urgent threat information being conveyed to owners and operators of critical infrastructure noting that these arrangements are detailed in the NCTC Guidelines.

4. In order to ensure effective coordination, Australian governments undertake to:

    a. work in a consistent, cooperative and transparent manner, including through NCIRC, and

    b. use NCIRC as a forum to raise cross-jurisdictional issues, or issues where there is common interest that would benefit from national collaboration.

5. The Australian Government recognises that in industry engagement through the TISN, issues that relate primarily to the responsibilities of State and Territory governments can arise. AGD will inform NCIRC when such instances occur.

Box 4.5

5. SUCCESS CRITERIA AND REVIEW OF THIS STRATEGY

The aim of the Australian Government's CIR Strategy is the continued operation of critical infrastructure in the face of all hazards, as this critical infrastructure supports Australia's national defence and national security, and underpins our economic prosperity and social wellbeing. More resilient critical infrastructure will also help to achieve the continued provision of essential services to the community.

CIR is an ongoing process and occasional review and fine tuning of the activities under each strategic imperative will be required as the Strategy is implemented.

Success will be measured by:

- effective engagement between governments and industry, both within and outside the TISN, for the exchange of information and intelligence, and the development of solutions to relevant security issues, on a sectoral and cross-sectoral basis
- Sector Groups being well supported by government and responsive to changes in the environment, individually and collectively
- businesses and governments collaborating to develop and promote best practice in CIR and resilience capabilities being integrated into everyday business activities
- the need for investment in resilient, robust infrastructure being considered in market regulation decisions
- businesses and governments collaborating to identify key cross-sectoral dependencies and vulnerabilities with respect to both cyber and physical infrastructure
- businesses and governments collaborating to progress national research and development in CIR
- a positive and robust relationship between the different levels of government on CIR, and a level of national consistency and coordination while also supporting the different approaches of governments
- CIR issues and implications for owners and operators of critical infrastructure being considered in Australian Government policy development processes

- lessons from exercise activities and real life events being propagated to all Sector Groups to enhance organisations' understanding of resilience and improve planning arrangements

- owners and operators being integrated into the implementation of the Cyber Security Strategy and having useful engagement with CERT Australia, and

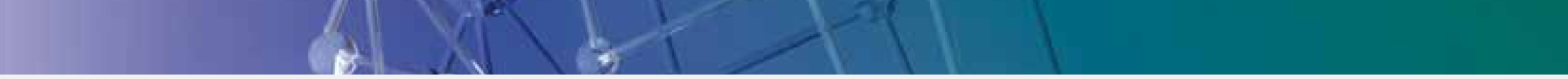
- Australian Government international engagement being coordinated with updates being provided to NCIRC as required.

To ensure the Australian Government's policy settings remain appropriate, the CIR Strategy will undergo a comprehensive review in 2015, after five years of operation.

6. CONCLUSION

Effective CIR is reliant on a strong, collaborative partnership between governments and critical infrastructure owners and operators to deliver the Australian Government's policy aim of the continued operation of critical infrastructure in the face of all hazards.

A separate implementation plan will be developed which will describe, in detail, how the Australian Government plans to execute the CIR Strategy. Development of the implementation plan will be coordinated by AGD, in consultation with business and government stakeholders as appropriate.



GLOSSARY

AEMC – Australian Emergency Management Committee

AGD – Attorney-General's Department

AIC – Australian Intelligence Community

APRA – Australian Prudential Regulation Authority

ASIO – Australian Security Intelligence Organisation

BFSG – Banking and Finance Sector Group

BGAG – Business-Government Advisory Group on National Security

CERT Australia – Computer Emergency Response Team

CIAC – Critical Infrastructure Advisory Council

CIP – Critical Infrastructure Protection

CIPMA – Critical Infrastructure Program for Modelling and Analysis

CIR – Critical Infrastructure Resilience

COAG – Council of Australian Governments

COAG-SOM – Council of Australian Governments Senior Officials Meeting

CSG – Communications Sector Group

CSOC – Cyber Security Operations Centre

CT – Counter-Terrorism

DAFF – Department of Agriculture, Fisheries and Forestry

DBCDE – Department of Broadband, Communications and the Digital Economy

DCCEE – Department of Climate Change and Energy Efficiency

DoHA – Department of Health and Ageing

DRET – Department of Resources, Energy and Tourism

EMA – Emergency Management Australia

ESG – Energy Sector Group

FCSG – Food Chain Sector Group

HBSR – Homeland and Border Security Review

Infrastructure – Department of Infrastructure, Transport, Regional Development and Local Government

ISG – Infrastructure Sector Group

ITSEAG – IT Security Expert Advisory Group

MCPEM-EM – Ministerial Council for Police and Emergency Management – Emergency Management

NCCIP – National Committee on Critical Infrastructure Protection

NCIRC – National Critical Infrastructure Resilience Committee

NCIRR – National Critical Infrastructure Risk Register

NCTC – National Counter-Terrorism Committee

NEMC – National Emergency Management Committee

NSRPD – National Security Resilience Policy Division

OGSF – Oil and Gas Security Forum

OTS – Office of Transport Security

PM&C – Department of the Prime Minister and Cabinet

SCADA – Supervisory Control and Data Acquisition

TSG – Transport Sector Group

TISN – Trusted Information Sharing Network

WSSG – Water Services Sector Group

APPENDIX A:
SUPPORT FOR THE SHIFT TO RESILIENCE FROM PAST POLICY REVIEWS

Several key pieces of work have recommended a shift to resilience. A comprehensive review of the Australian Government's Critical Infrastructure Protection Program was undertaken in 2007 (the 2007 CIP Review). A key finding of the review was that the term 'critical infrastructure protection' did not adequately reflect the Program's all hazards approach, instead implying a protective security focus. It was recommended that the Program be shifted to resilience to more accurately reflect its work and objectives.

In 2008, Ric Smith AO undertook a review of Australia's homeland and border security arrangements. The Homeland and Border Security Review (HBSR) recognised that 'resilience is an underlying element of the CIP arrangements and should be promoted'. It also went on to propose that the term 'resilience' be incorporated into the title of relevant committees.

In early 2009, a review of national critical infrastructure protection arrangements was initiated under the auspices of COAG Senior Officials. The review examined the appropriateness and effectiveness of national CIP arrangements, the accountability to governments and the related mechanisms for engagement between governments and industry.

The review found that while it is possible to plan for some incidents that may affect critical infrastructure, given the broad range of potential threats and hazards, including natural disasters, pandemics, negligence, accidents, criminal activity, or computer network attack, it is not possible to foresee, mitigate or prevent all of these events. In particular, protective security measures alone cannot mitigate supply chain disruption, nor ensure the rapid restoration of services. Owners and operators of critical infrastructure often have limited capacity to continue operations indefinitely if the essential goods and services they require are interrupted.

CIR is therefore a more suitable approach, and organising principle, for activities in response to all hazards. The review also recommended that with regard to the specific threat of terrorism, the protection of critical infrastructure should remain a discrete body of work oversighted by the National Counter-Terrorism Committee (NCTC). At the national level, the term 'critical infrastructure protection' will only be used to describe actions or measures undertaken to mitigate the specific threat of terrorism.

While the NCTC has high-level oversight for CIP (i.e. terrorism specific) activities at the national level, the threat of terrorism is part of the all hazards approach to critical infrastructure encapsulated in the CIR paradigm.

APPENDIX B:
ROLES OF AUSTRALIAN GOVERNMENT AGENCIES

A range of Australian Government agencies make a significant contribution to the implementation of the Australian Government's CIR Strategy. Recognising that all Australian Government agencies have a role to play in ensuring the security and resilience of Australia's critical infrastructure, the following agencies have clear responsibility for the delivery of the Australian Government's CIR Strategy.

The **Attorney-General's Department** (AGD) provides essential support to the Government in the maintenance and improvement of Australia's system of law and justice and its national security and emergency management systems. Under the CIR Strategy, AGD is responsible for:

- the provision of strategic leadership and coordination in the development of a consistent Australian Government approach to CIR
- the development of policy and advice to Government on CIR
- management of the Trusted Information Sharing Network (TISN)
- the provision of secretariat support to the Banking and Finance and Water Services Sector Groups, and the Resilience Expert Advisory Group
- the provision of support to the Business-Government Advisory Group on National Security (BGAG), the National Critical Infrastructure Resilience Committee (NCIRC) and the Critical Infrastructure Advisory Council (CIAC)
- management of information-sharing mechanisms including the TISN websites, the TISN calendar and the TISN deeds and register, and
- coordination of the critical infrastructure threat assessment briefing programs.

The **Australian Security Intelligence Organisation's** (ASIO) responsibilities are defined by the *Australian Security Intelligence Organisation Act 1979,* and include identifying and investigating threats to security, wherever they arise, and providing advice to protect Australia, its people and its interests. As agreed by the National Counter-Terrorism Committee, ASIO's responsibilities in relation to the CIR Strategy include:

- the identification and prioritisation of national critical infrastructure, including maintaining a database of national critical infrastructure
- the preparation of vital and sectoral critical infrastructure threat assessments
- the briefing of owners and operators on vital and sectoral critical infrastructure threat assessments, and
- protective security risk reviews for specified critical infrastructure.

The **Department of Agriculture, Fisheries and Forestry** (DAFF) develops and implements policies and programs that ensure Australia's agricultural, fisheries, food and forestry industries remain competitive, profitable and sustainable. DAFF helps to ensure the safety and security of Australia’s food chains, aids in the management of pest and disease risks, protects the health and safety of plant and animal industries and supports sustainable natural resource use and management in a changing environment. Under the CIR Strategy, its responsibilities include:

- the provision of portfolio specific policy advice on critical infrastructure related issues
- the provision of secretariat support to the Food Chain Sector Group, and
- drafting risk context statements and contributing to briefings under the threat assessment briefing process.

The **Department of Broadband, Communications and the Digital Economy** (DBCDE) is responsible for policy development, advice and program delivery across a range of activities including the National Broadband Network rollout, Australia’s digital television switchover, initiatives that support development of the digital economy, telecommunications policy, media policy, cyber security and cyber safety, managing the radio frequency spectrum and postal policy. Under the CIR Strategy, its responsibilities include:

- the provision of portfolio specific policy advice on critical infrastructure related issues
- the provision of secretariat support to the Communications Sector Group and the IT Security Expert Advisory Group, and
- drafting risk context statements and contributing to briefings under the threat assessment briefing process.

The **Department of Health and Ageing** (DoHA) provides policy advice, programs and regulation across a wide range of areas including population health, medicines and medical services, aged care, primary care, rural health, Indigenous health, hearing services, biosecurity and health response, and health and medical research. DoHA also leads a whole-of-government approach to strengthening the health sector’s readiness for disease threats, national emergencies and other large-scale health incidents. Under the CIR Strategy, its responsibilities include:

- the provision of portfolio specific policy advice on critical infrastructure related issues
- the provision of secretariat support to the Health Sector Group, and
- drafting risk context statements and contributing to briefings under the threat assessment briefing process.

The **Department of Infrastructure, Transport, Regional Development and Local Government** (Infrastructure) is responsible for ensuring a transport system that is more secure against the threat of terrorism and acts of unlawful interference.

Through the Office of Transport Security (OTS), Infrastructure regulates the preventive security measures of industry participants in the aviation, maritime (including offshore oil and gas) and air cargo sectors. Infrastructure also works with State and Territory governments to develop a consistent and coordinated approach to securing the surface transport sector.

Infrastructure, through OTS, coordinates national transport security policy, provides security risk advice to industry participants in its regulated sectors, including critical infrastructure operators, and has specific responsibilities during an aviation or maritime transport security incident.

OTS also has responsibility for the provision of secretariat support to the Transport Sector Group and Oil and Gas Security Forum, and drafting risk context statements and contributing to briefings under the threat assessment briefing process which further contribute to the CIR Strategy.

The **Department of Resources, Energy and Tourism** (DRET) provides advice and policy support to the Australian Government regarding Australia's resources, energy and tourism sectors. DRET develops and delivers policies to increase Australia's international competitiveness, consistent with the principles of environmental responsibility and sustainable development. DRET is responsible for developing and maintaining government policies and programs to ensure resilient and secure energy systems. Under the CIR Strategy, its responsibilities include:

- the provision of portfolio specific policy advice on critical infrastructure related issues
- the provision of secretariat support to the Energy Sector Group, and
- drafting risk context statements and contributing to briefings under the threat assessment briefing process.