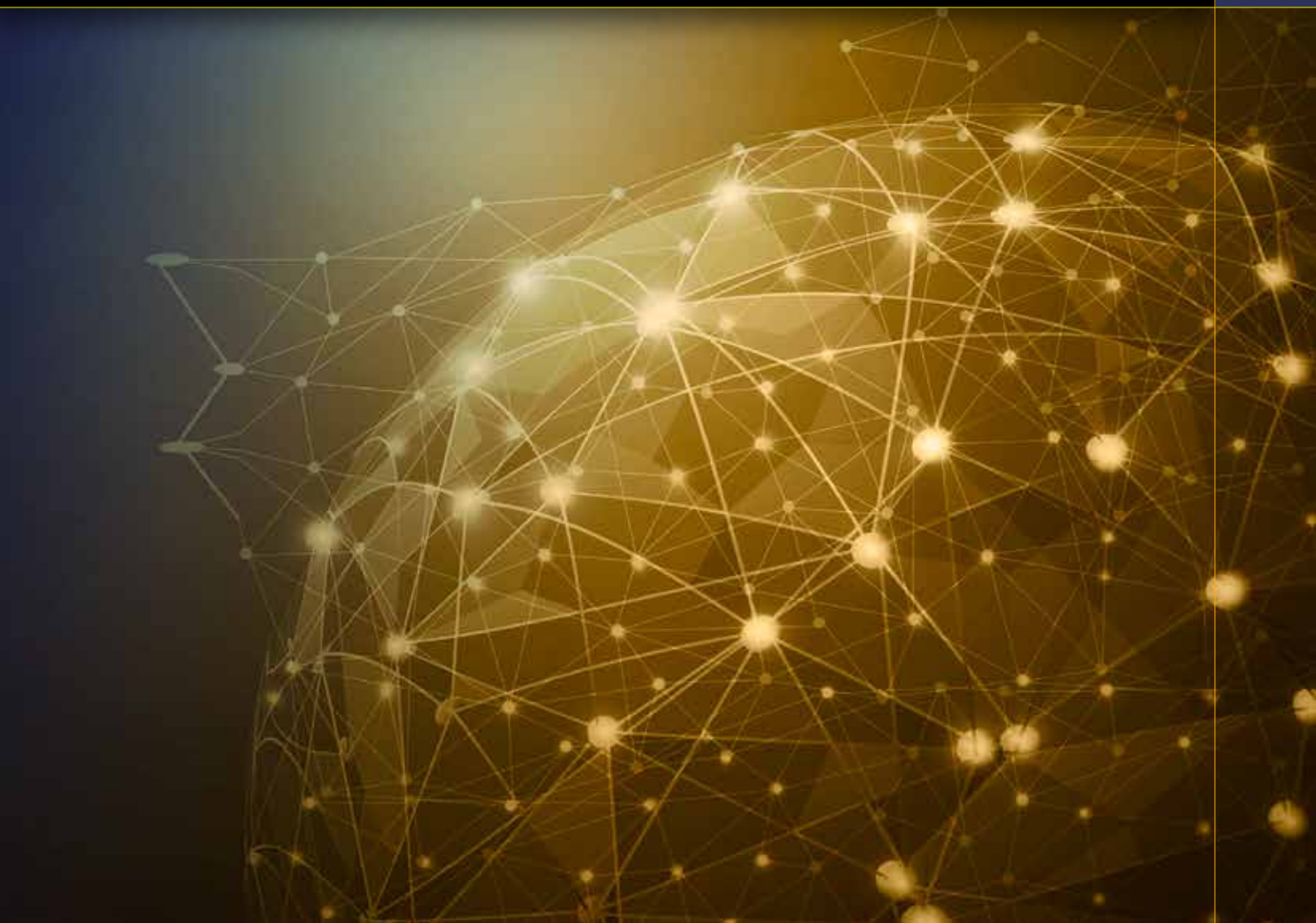
Australian Government

POLICY STATEMENT

# CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY: **POLICY STATEMENT**



# CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY: POLICY STATEMENT

ISBN: 978-1-925290-04-2 (Print)
ISBN: 978-1-925290-05-9 (Online)



**Contact us**
Enquiries regarding the licence and any use of this document are welcome at:

Commercial and Administrative Law Branch
Attorney-General's Department
3–5 National Cct
BARTON ACT 2600
Email: copyright@ag.gov.au

# A STRONG **FOUNDATION**

In the wake of the 11 September 2001 terrorist attacks in the United States and the 2002 Bali Bombings, the Australian Government established a national Critical Infrastructure Strategy for Australia. This 'all hazards' Strategy provided a strong foundation on which critical infrastructure owners and operators and governments could prepare for, and respond to, a range of significant disruptive events.

Successive Strategies have encompassed over a decade of collaborative effort and achievement by businesses and all levels of government. The resilience of Australia's critical infrastructure has been enhanced by the collective work of the States and Territories, the Commonwealth Government and the owners and operators of critical infrastructure. The Trusted Information Sharing Network (TISN) continues to provide a secure, non-competitive environment in which all stakeholders have the opportunity to work together to ensure the continued operation of critical infrastructure.

The Critical Infrastructure Resilience Strategy (the Strategy), which consists of this *Policy Statement* and a *Plan* for practical implementation, builds on past successes, provides greater value to stakeholders, and continues to deliver significant outcomes for business and the economy, governments and the community.

# Critical Infrastructure **Protection**

*Terrorism remains an enduring threat to Australia's national security, and violent extremists continue to seek to target critical infrastructure sectors in Australia and abroad.*

*In early 2009, a review of national critical infrastructure protection arrangements was conducted by COAG Senior Officials. The review examined the appropriateness and effectiveness of national critical infrastructure protection (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. Therefore a resilience approach is more suitable for activities in response to all hazards.*

*At the national level, the term 'critical infrastructure protection' is used to describe actions or measures undertaken to mitigate against the specific threat of terrorism, whereas the term 'critical infrastructure resilience' encompasses the Government's all hazards approach, which includes terrorism. CIP is overseen by the Australian and New Zealand Counter-Terrorism Committee (ANZCTC). While the ANZCTC has high level oversight for CIP activities, critical infrastructure protection remains an important component of the Australian Government's all hazards Strategy.*

# AIM OF THE **STRATEGY**

*The Australian, State and Territory governments share the following definition of critical infrastructure:*

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

*In this context, 'significantly' 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.*

The aim of the Australian Government's Critical Infrastructure Resilience Strategy is the **continued operation of critical infrastructure** in the face of all hazards. More resilient critical infrastructure will also help to support the continued provision of essential services (provided by critical infrastructure) to businesses, governments and the community, as well as to other critical infrastructure sectors.

# UNDERPINNING **PRINCIPLES**

The Australian Government's policy approach to critical infrastructure recognises that:

- critical infrastructure is essential to Australia's economic and social prosperity;
- resilient critical infrastructure plays an essential role in supporting broader community and disaster resilience;
- businesses and governments have a shared responsibility for the resilience of our critical infrastructure, requiring strong partnerships; and
- all States and Territories have their own critical infrastructure programs that best fit the operating environments and arrangements in each jurisdiction.

## ECONOMIC AND SOCIAL PROSPERITY

Critical infrastructure underpins the functioning of Australia's society and economy. It enables the provision of essential services such as food, water, health services, electricity, communications, transportation and banking. Without these services, our social cohesion, economic prosperity and public safety are threatened. The resilience of Australia's critical infrastructure is integral to the prosperity of the nation.

Most critical infrastructure in Australia is either privately owned and operated, or run on a commercial basis by government. In many sectors, competitive markets determine the way in which critical services are provided to the Australian community. Businesses have a strong incentive to ensure the resilience of the critical infrastructure they own and operate, as the continuity of their services and their ability to manage disruptions directly affects their profitability and reputations.

The operation of critical infrastructure represents a significant proportion of economic activity in its own right. More importantly, it provides the foundation on which almost all economic activity in Australia is built. The commercial shipping industry, for example, handles 99 per cent of international trade volumes to and from Australia, making our ports and other maritime infrastructure and supply chains critical to every sector of the national economy.

Resilient infrastructure improves productivity and helps to drive the business activity that underpins economic growth. The availability of essential services (such as telecommunications and electricity) can be a key factor in determining where different types of economic activity will occur. Many high value industries require access to such services before they can be attracted to, and established in, a region. Critical infrastructure also connects regional and international markets by decreasing the operating costs and logistical challenges associated with distance.

The availability of reliable critical infrastructure promotes market confidence and economic stability, and increases the attractiveness of Australia as a place to invest. Owners and operators that effectively manage critical infrastructure during a crisis can outperform less-resilient competitors by maintaining the ability to conduct business and reap reputational rewards. Resilience during disasters can also have a positive flow-on effect for other industries, reducing the overall negative impact to economic prosperity.

## SUPPORTING COMMUNITY AND DISASTER RESILIENCE

There are strong links between the resilience of Australia's critical infrastructure and the resilience of the broader Australian community to disasters. Critical infrastructure owners and operators provide resources, expertise and the essential services on which the community depends during and after disasters. Resilient critical infrastructure enables the community to recover faster from adversity and helps key social institutions, such as volunteer organisations, continue to function.

The National Strategy for Disaster Resilience (NSDR) provides high-level guidance on disaster management to governments, business, community leaders and the not-for-profit sector. The NSDR recognises that the responsibility for disaster resilience is shared between individuals, households, businesses, communities and governments, and specifically identifies critical infrastructure as an important component of disaster resilience.

The NSDR identifies seven priority areas for building disaster resilient communities across Australia. A number of these priority areas involve active engagement with, and participation by, critical infrastructure owners and operators.

The Australian Government's Critical Infrastructure Resilience Strategy will continue to complement new and ongoing initiatives, and the all-hazards approach, under the NSDR.

## SHARING RESPONSIBILITY FOR CRITICAL INFRASTRUCTURE RESILIENCE

The Australian Government takes a non-regulatory approach to critical infrastructure resilience, favouring a productive business-government partnership. This approach recognises that owners and operators of critical infrastructure are usually best placed to assess the risks to their operations and determine the most appropriate mitigation strategies. The complex and dynamic nature of risk to critical infrastructure sectors means that applying uniform compliance standards may not only be difficult but also inhibit the flexibility and innovation that is central to enhancing the resilience of critical infrastructure organisations. Where industry sectors are subject to existing regulatory arrangements, regulatory agencies remain key participants in the business-government partnership.

With most critical infrastructure in private hands or run by governments on a commercial basis, it is crucial that businesses work with one another, and with government, to ensure the continuity of operations and the provision of essential services to the Australian economy and community. The responsibility for achieving this aim is shared between owners and operators of critical infrastructure, State and Territory governments and the Australian Government.

In many cases, neither business nor government in isolation have access to all the information they need to understand and mitigate risks; nor the ability to influence their operating environments to the extent required to ensure the continuity of essential services. The primary focus of an effective business-government partnership must be the creation of an environment in which all parties can openly and securely share information, develop trust and build solutions to increase the resilience of critical infrastructure.

The TISN continues to provide a secure environment for information sharing and resilience-building initiatives related to critical infrastructure, and remains a valuable part of the Strategy. The TISN's governance body, the Critical Infrastructure Advisory Council (CIAC), provides strategic direction and priorities for the TISN. Ongoing opportunities to strengthen the business-government partnership will be captured to generate greater value for stakeholders.

## COMPLEMENTING STATE AND TERRITORY PROGRAMS

The Australian Government and private-sector owners and operators value the active involvement of State and Territory governments in the Strategy, which aims to complement State and Territory programs wherever possible.

State and Territory governments have primary responsibility for responding to incidents that occur within their jurisdictions, and often maintain specialist capabilities for managing specific threats such as terrorism. Each State and Territory government has its own critical infrastructure program according to the local operating environment and arrangements. It is essential that critical infrastructure owners and operators have a strong understanding of jurisdictional arrangements and develop productive working relationships with local authorities. States and Territories also own and operate critical infrastructure, making them integral to our collective efforts to increase the resilience of critical infrastructure.

Critical infrastructure often spans across state and territory borders (and in some cases, international borders), with some States and Territories highly dependent on critical infrastructure that is located in other jurisdictions. In these cases, it is crucial that industry and governments work together to ensure that resilience-building efforts are targeted, coordinated and complement one another.

# POLICY **OBJECTIVES**

The resilience of critical infrastructure depends on the capacity of owners and operators to effectively manage the risks to their operations. This includes having in place mature risk management procedures, based on best practice, to effectively prepare for, prevent, respond to and recover from foreseeable risks; and developing capabilities that empower and enable organisations to manage unforeseen risks. Both of these approaches are integral to effective risk management and complement each other. In this regard, the Strategy has two key objectives.

1. **Critical infrastructure owners and operators are effective in managing foreseeable risks to the continuity of their operations through a mature risk-based approach.**

Owners and operators of critical infrastructure are usually best placed to determine, assess and mitigate risks to their operations and have responsibility for these decisions and outcomes. A mature risk-based approach enables owners and operators to maximise their understanding of reasonably foreseeable risks and develop appropriate mitigation strategies.

A mature risk-based approach enables clear differentiation between security environments and the appropriateness of different measures and responses. For example, a national telecommunications provider would develop different risk mitigation strategies for assets in cyclone-prone North Queensland than for high-risk bushfire areas of western Victoria. Likewise, the mitigation strategies to address supply chain vulnerabilities would be different to measures to mitigate risks in linear assets.

This approach allows resources to be targeted where they are needed most. The complex and dynamic nature of the operating environment and threats in that environment provide the general context for the analysis of risk. Multifaceted social, economic, technological and environmental changes across the globe mean that owners and operators of critical infrastructure face an evolving and changing set of risks. However, the challenge is that critical infrastructure is often designed and built for decades of service.

The Strategy helps owners and operators to determine, assess and mitigate reasonably foreseeable risks to their operations. This includes a better understanding of cross-sector dependencies, key sectoral vulnerabilities and resilience gaps; and working with international partners to ensure Australia's critical infrastructure sectors have access to world's best-practice approaches.

## 2. Critical infrastructure owners and operators are effective in managing unforeseen risks to the continuity of their operations through an organisational resilience approach.

While a mature risk-based approach is useful when risks are well understood, critical infrastructure owners and operators often face situations in which risk information is either unavailable, insufficient, or too complex to interpret. Risk bias can also affect an organisation's perception of what constitutes reasonably foreseeable risk and some threats to critical infrastructure are entirely unexpected.

Globalisation, new technologies and a range of social, demographic and environmental trends continue to increase the complexity of the operating environment for critical infrastructure. It is no longer possible for owners and operators to understand all the risks they face, which include vulnerabilities in other sectors and disruption to distant supply chains.

Organisations must build an inherent capacity to respond to unforeseen or unexpected risks and events. In the face of adversity, organisations with a strong resilience culture and capability will maintain operational continuity for longer, and return to normal business more quickly. Such organisations will enhance their reputations and reap economic benefits by maintaining the confidence of their customers and of the market. An organisation with a strong resilience culture is more likely to share information with others, learn from crises, have flexible approaches to problem solving and have collaborative relationships with government and the industry sectors.

An organisational resilience approach does not preclude the use of traditional risk management practices. Highly resilient organisations are able to adapt and utilise risk-based methods and tools more flexibly and across a range of circumstances. In addition to planning for reasonably foreseeable risks, resilient organisations prepare for uncertainty and ensure their arrangements are adaptable and scalable to disruptions of all kinds.

The Resilience Expert Advisory Group will continue researching the benefits and indicators of organisational resilience to assist critical infrastructure owners and operators to build a mature organisational resilience approach. It will also promote and develop tools and advice, and share real life case studies demonstrating the practical advantages of organisational resilience. The Australian Government will also assist critical infrastructure owners and operators to better understand and manage strategic risks to their operations, such as low-frequency, high-impact events.

# KEY **OUTCOMES**

Four key outcomes will be delivered through the Critical Infrastructure Resilience Strategy. These outcomes work together to build overall critical infrastructure resilience.

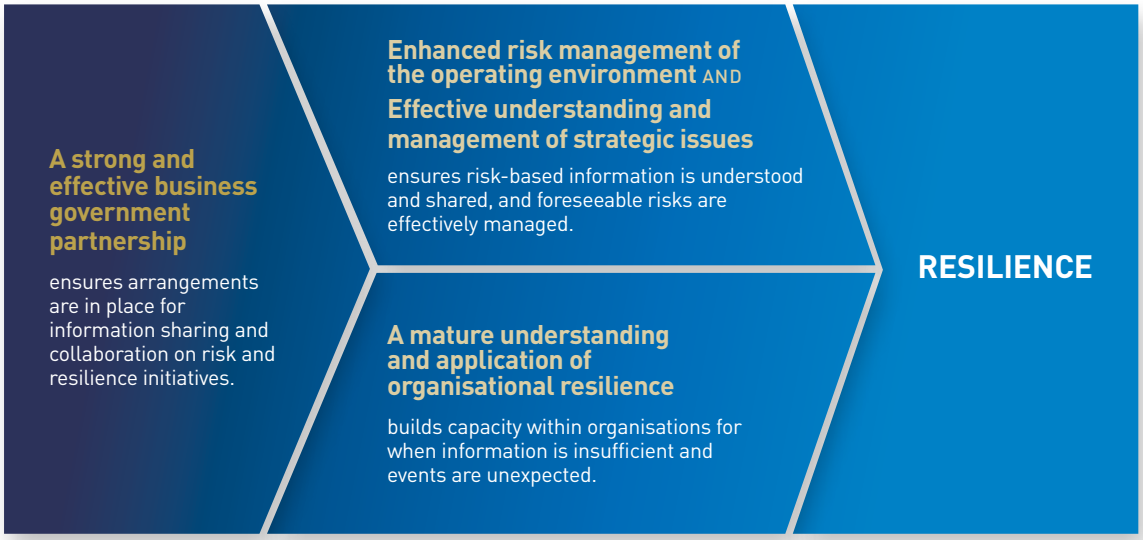



**Figure 1**: The four key outcomes that contribute to overall resilience

These key outcomes are summarised below, with core activities to achieve these outcomes detailed in the *Critical Infrastructure Resilience Plan*.

## OUTCOME 1: A STRONG AND EFFECTIVE BUSINESS-GOVERNMENT PARTNERSHIP

The business-government partnership, primarily embodied by the TISN, remains a highly-effective forum for information exchange and the facilitation of resilience-building initiatives. However, there are a number of opportunities to strengthen the business-government partnership in the face of contemporary challenges. These challenges include increasing demands on owners and operators arising from growing complexity within the operating environment, and ongoing resource constraints in both the private and public sectors.

The Australian Government will provide the greatest possible value to all stakeholders by harnessing opportunities to implement the Strategy more effectively, such as: more effective information sharing, particularly with regard to cross-sectoral information; stronger strategic guidance from the CIAC; more comprehensive reporting on sectoral achievements, lessons learnt and priorities; and greater flexibility in the way in which activities are delivered.

## OUTCOME 2: ENHANCED RISK MANAGEMENT OF THE OPERATING ENVIRONMENT

Critical infrastructure systems, networks and supply chains are increasingly complex and interconnected, particularly given the rapid proliferation of new technologies, and the globalisation of markets and the production process. Disruptions in one sector can quickly affect other sectors, and have the potential to cause serious cascading failures. Australia is also highly dependent upon particular types of goods and services that originate overseas. An improved understanding of interdependencies between critical infrastructure sectors, and regions, is essential to strengthening resilience.

It is crucial that critical infrastructure owners and operators understand, and are able to respond to, the vulnerabilities and dependencies in their own sector, and in other sectors. While this has always been a focus of the Australian Government's Critical Infrastructure Strategies, it is one of the most significant challenges to the continued operation of critical infrastructure during crises.

Identifying key elements of Australia's critical infrastructure that are 'most' important, as well as key dependencies, can assist owners and operators prioritise measures to address vulnerabilities and focus mitigation efforts where the need, and return, may be greatest. This is particularly important in an environment of both increasing threat complexity and ongoing resource constraints. Critical infrastructure owners and operators will benefit from a clearer national (and, where relevant, international) understanding of the systems, networks, assets and dependencies that are most critical at the organisational and sectoral levels.

The determination of what is most critical will be complemented by an indicative measurement of the resilience of critical infrastructure. This will enable the outcomes of resilience-building initiatives to be compared across time and environments, and further assist in the prioritisation and targeting of mitigation strategies.

The Australian Government will work closely with relevant stakeholders in a staged approach to develop and implement sector-led activities to map key dependencies, identify nationally critical systems, networks and assets, and indicatively measure resilience levels.

A more flexible approach will be implemented to delivering cross-sectoral engagement and information sharing. Specifically, the Australian Government will facilitate a program of targeted, more frequent and smaller-scale cross-sectoral events with more effective follow-up on outcomes; enhance cross-sectoral information sharing mechanisms and opportunities; and increase capabilities for critical infrastructure organisations to understand cross-sectoral dependencies, including cyber-security vulnerabilities.

# Cyber **security**

*All critical infrastructure sectors in Australia rely on internet-connected computer systems. In some sectors, these systems are crucial to service delivery. For example, the supply of electricity is controlled by specialised, networked supervisory control and data acquisition systems that can, in some cases, be operated remotely via an internet connection.*

*All internet-connected computer systems are vulnerable to cyber-security threats, including from organised criminals, unscrupulous competitors, issue-motivated groups or foreign state actors. Therefore, it is crucial that owners and operators of critical infrastructure have the ability to rapidly respond to and recover from such threats.*

*CERT Australia is the Australian Government's national computer emergency response team and is the primary point of contact within the Australian Cyber Security Centre (ACSC) for cyber security issues affecting major Australian businesses. The ACSC brings together the Government's operational cyber security capabilities to create a hub for greater collaboration and information sharing with the private sector, State and Territory governments and international partners to combat the full breadth of cyber threats. Other agencies co-located within the ACSC are the Australian Security Intelligence Organisation, the Australian Federal Police, the Australian Signals Directorate, the Defence Intelligence Organisation and the Australian Crime Commission.*

*Through the CERT, the Government provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.*

*Cyber security and, in particular, acquiring a better understanding of cyber cross-sectoral dependencies, is an area of increasing priority for critical infrastructure owners and operators. In this regard, the Government will utilise existing mechanisms (such as CERT Australia and the Critical Infrastructure Program for Modelling and Analysis) to assist critical infrastructure organisations to better understand and manage risks in this area.*

*The Australian Government's Critical Infrastructure Resilience Strategy will complement the Government's cyber security strategy, and will create further opportunities for cooperation and information sharing between industry and government on cyber-security matters.*

## OUTCOME 3: EFFECTIVE UNDERSTANDING AND MANAGEMENT OF STRATEGIC ISSUES

Rapid and extensive technological, social, economic and environmental change will continue to impact on the resilience of Australia's critical infrastructure. The impact of such change is becoming increasingly complex and unpredictable over time. As critical infrastructure that is built today might remain in service for half a century, it is of paramount importance that owners and operators consider and account for trends that may impact their ability to deliver services far into the future.

However, strong demands on both time and resources mean that current operational imperatives are often prioritised over longer-term strategic challenges. Of particular concern are low-frequency, high-impact events which, due to their rarity, may not be treated with a high priority until they occur. The Australian Government has a strong interest in promoting an understanding of, and preparation for, severe, national-scale crises, given its unique role in responding to such events.

The Australian Government will continue to work closely with TISN groups, international partners, government agencies and academia to examine strategic issues and trends affecting critical infrastructure, and will facilitate cross-sectoral collaboration and information sharing on these issues, including through exercises and workshops.

The Attorney-General's Department, as lead Australian Government agency for critical infrastructure resilience, will continue to engage with business and government stakeholders on key policy issues and advocate critical infrastructure resilience issues across Government.

## OUTCOME 4: A MATURE UNDERSTANDING AND APPLICATION OF ORGANISATIONAL RESILIENCE

A growing number of Australian critical infrastructure owners and operators are utilising an organisational resilience approach to ensure the continuity of their operations and enhance their competitiveness.

Australia is a world leader in developing and promoting the organisational resilience approach. With organisational resilience now generally understood and its value largely accepted, the focus of work will shift to deepening our understanding of its dimensions and maturing resilience practice.

This will include continuing to build on the range of practical tools and guidance available to critical infrastructure organisations; capturing real life case studies; promoting the benefits of an organisational resilience approach; and further researching the benefits and indicators of organisational resilience.

# CONCLUSION

The continued operation of Australia's critical infrastructure underpins our social and economic wellbeing and enables the conduct of national defence and national security. Owners and operators, and governments at all levels will benefit by working in partnership to enhance and maintain the resilience of Australia's critical infrastructure.

A non-regulatory business-government partnership, involving a mature approach to risk management, effective information sharing and the building of organisational resilience will assist all critical infrastructure sectors face the challenges of an increasingly complex and dynamic array of operational risks. This approach benefits the community through increased safety and security and enhances the prosperity of Australian businesses and the Australian economy.

The Strategy will build on past experience, international best practice and adapt to challenges by delivering four key outcomes:

**1. A strong and effective business-government partnership;**

**2. Enhanced risk management of the operating environment;**

**3. Effective understanding and management of strategic issues; and**

**4. A mature understanding and application of organisational resilience.**

Detailed information on how the Critical Infrastructure Resilience Strategy will address these areas can be found in the *Critical Infrastructure Resilience Plan*.

To ensure the Australian Government's policy settings remain appropriate, the Strategy will undergo a comprehensive review in 2020, after five years of operation. Success will be measured by the degree to which the four key outcomes, through the activities detailed in the *Critical Infrastructure Resilience Plan*, are achieved.

Australian Government