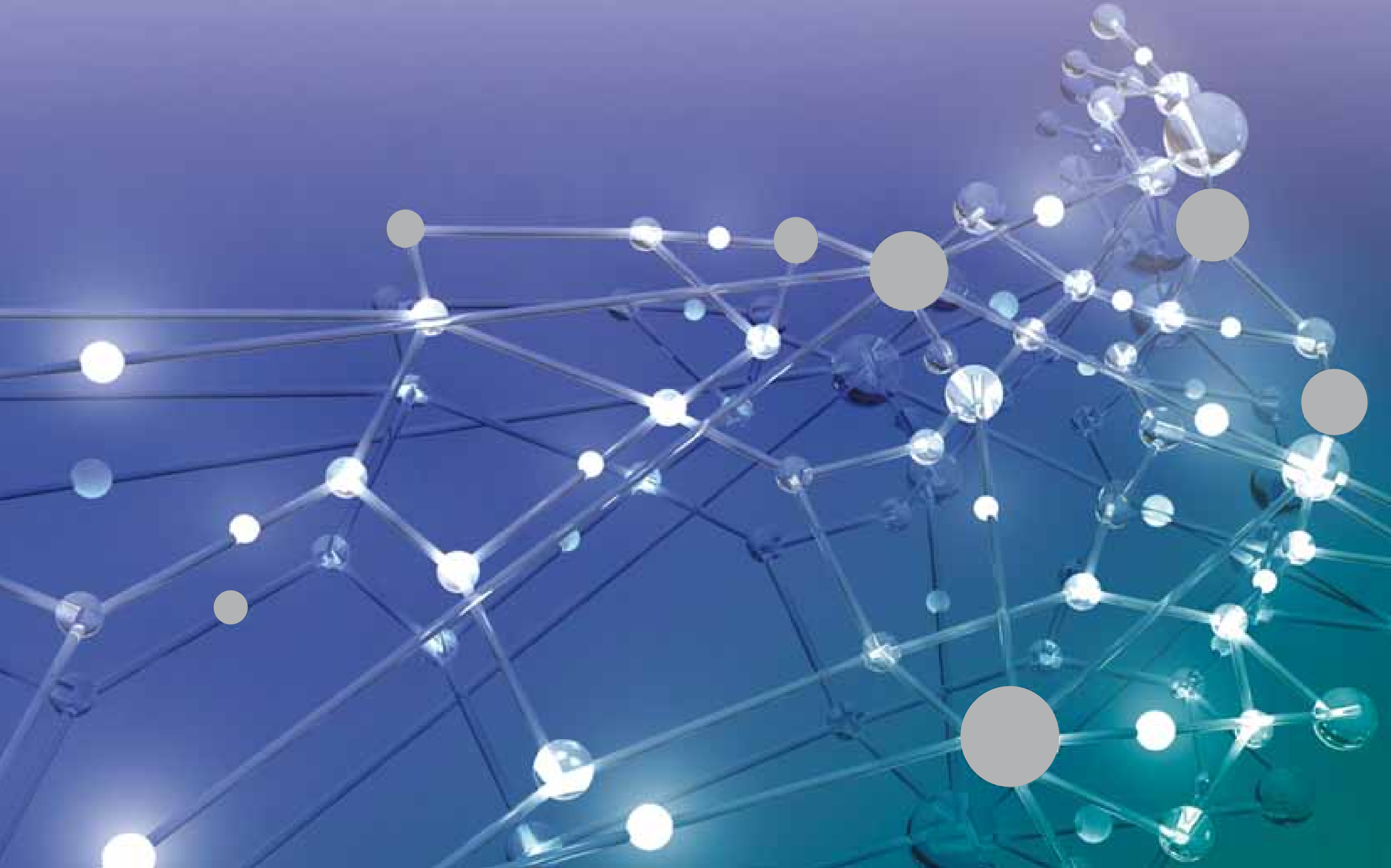
Australian Government

CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY SUPPLEMENT

An overview of activities to deliver the Strategy



ISBN: 978-1-921725-24-1

Introduction

THE AUSTRALIAN GOVERNMENT'S CRITICAL INFRASTRUCTURE RESILIENCE (CIR) STRATEGY IS IMPLEMENTED THROUGH SIX STRATEGIC IMPERATIVES. THERE ARE IMPORTANT INTER-RELATIONSHIPS BETWEEN THE SIX IMPERATIVES AND EACH ONE CONSISTS OF A NUMBER OF ACTIVITIES (DESCRIBED ON THE FOLLOWING PAGES) TO DELIVER THE AIM AND OBJECTIVES OF THE STRATEGY.

Aim

The aim of the 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.

Objectives

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; and

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.

Strategic Imperatives

1. Operate an effective business-government partnership with critical infrastructure owners and operators
2. Develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience
3. Assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies
4. Provide timely and high quality policy advice on issues relating to critical infrastructure resilience
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
6. Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate

1. Operate an effective business-government partnership with critical infrastructure owners and operators

Activity	Description
1.1 TISN related activity	The TISN, through sector specific and cross-sectoral activity, is a forum where competitors can collaborate on common issues and solutions to domestic security problems in a trusted environment which is sanctioned by business regulators. The Australian Government recognises that the TISN Sector Groups (formerly the Infrastructure Assurance Advisory Groups) have matured over the years and the differences between the Sector Groups in terms of composition of membership, sectoral operating environments, and the nature and extent of their relationship with the Australian Government, is very apparent. Accordingly, it is acknowledged that there are practical limitations in regarding the TISN as an homogenous collective. In fact, the TISN comprises seven unique Sector Groups each with their own culture, people and approach. In recognition of these differences, the Australian Government, through the CIR Strategy is taking a more tailored approach to each Sector Group. When describing the work of the TISN, the Australian Government is referring to the activities of the individual Sector Groups and the Expert Advisory Groups.
1.2 Core TISN activities	The core activities of the TISN-related part of the business-government partnership for CIR include: • seven critical infrastructure Sector Groups (Energy, Water, Communications, Banking and Finance, Health, Transport, Food). A key body of work for each Sector Group is the development and revision of a sector resilience strategy and annual work plan • two Expert Advisory Groups (Resilience[1], IT Security) • one Oil and Gas Security Forum (under the Energy Sector Group) • three Communities of Interest (Climate Change, Pandemic, SCADA) • two annual all-sector workshops (a 2 day conference on CIR in the first half of the year, and a 2 day workshop on cross-sectoral dependencies in the second half of the year), and • information sharing via electronic media including the upgraded TISN public and TISN secure websites.

[1] Due to the importance and ongoing nature of resilience work, the Resilience Community of Interest has been transitioned to be the Resilience Expert Advisory Group. AGD will provide secretariat support to the Resilience EAG and support its operation and work program. Given it is effectively a new group, it will need to develop terms of reference which capture membership, how it would operate, who would chair, reporting arrangements, resourcing and development of the work program.

Activity	Description
1.3 TISN governance arrangements	As lead Australian Government agency for CIR, the Attorney-General's Department (AGD) has put in place governance arrangements to facilitate the effective operation of the TISN. These include: • revised arrangements for the Critical Infrastructure Advisory Council (CIAC) to oversee the Sector and Expert Advisory Groups, and assist with implementing the CIR Strategy • desk officer support by AGD to assist agency secretariats to enhance Sector Groups' visibility of broader TISN activities that may be relevant, including assistance in managing issues that are effectively outside the scope of the TISN (see also Strategic Imperative 6) • management and coordination of the mechanisms that facilitate the free exchange of information within the TISN framework (including Deeds of Confidentiality, the Government Representative Confidentiality Acknowledgement, and access and security arrangements for the upgraded TISN public and TISN secure websites) • service principles and standards for Sector Group secretariats. The purpose of developing service principles and standards is to achieve more consistent levels of secretariat service across the TISN and encourage a culture of continuous improvement. Each service principle has one or more corresponding service standards that guide secretariats in their support of their Sector Group, and • as required, the review and clarification of the roles of Sector Groups or Expert Advisory Groups where questions or perceptions arise regarding the purpose or activities of a group (or groups), including perceptions of duplication, and to ensure sector coverage remains appropriate and meets the needs of existing and potential stakeholders.

Activity	Description
1.4 Other business-government partnership activity	Outside the TISN, Australian Government agencies also engage with owners and operators to identify and categorise critical infrastructure, share security and risk information across sectors and between business and government, and discuss and develop mitigation strategies and other security solutions. These activities are often (but not always) focused on the specific threat of terrorism and are conducted under the auspices of the National Counter-Terrorism Committee (NCTC). These core activities include: • ASIO's work in identifying and categorising critical infrastructure • the critical infrastructure threat assessment briefing programs in collaboration with the States and Territories • the Business Government Advisory Group on National Security (a mechanism for the Australian Government to discuss a broad range of national security issues and initiatives with CEOs and senior business leaders), and • the review of arrangements for the sharing of intelligence and other sensitive information with business being led by the Department of the Prime Minister and Cabinet (as recommended by the Homeland and Border Security Review (HBSR).
1.5 Facilitate a dialogue between owners and operators of critical infrastructure and the research community to identify and prioritise specific critical infrastructure related research and development projects	The Australian 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. Research is an important component of the Government's intelligence and information led, risk informed approach. This activity focuses on promoting CIR as a national research priority. It aims to 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 are being met on a range of security issues. The focus in previous years has been on reducing the vulnerabilities of critical infrastructure to the threats of terrorism and this will continue as a discrete body of work. However, research to improve our understanding of other issues including the trusted insider threat, climate change adaptation, and vulnerabilities of the submarine cables network will also be a focus (see also Strategic Imperative 2).

2. Develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience

Activity	Description
2.1 Develop guidance materials and tools	The Australian Government recognises that significant work has already been undertaken by a range of stakeholders on organisational resilience. The objective of this activity is to review the existing work, supplement this with additional work where required, and compile guidance material on organisational resilience to assist critical infrastructure owners and operators enhance their understanding of the resilience approach. The main deliverable, a 'Resilience Handbook', will be developed for resilience practitioners in business and government. The Resilience Handbook will contain practical information, tools, guides and references to other publications about resilience, and will be made available electronically and in hard copy. Specific guidance material will also be developed targeting senior business executives such as CEOs and Board Members. Sector Groups will be able to use the Resilience Handbook as an input into the development of their sector resilience strategies and work programs. It is important to note the Resilience Handbook is just one component of the broader body of knowledge on organisational resilience. Online tools such as the Resilience Benchmarking Tool can assist organisations to get a better understanding of resilience as it applies to their specific circumstances. The Australian Government will support further refinement and development of the current Resilience Benchmarking Tool, and will investigate the feasibility of developing other resilience tools.
2.2 Establish a resilience training program	Recent work by some leading resilience practitioners to trial a 'Resilience Master Class' has encouraged the Australian Government to support the development and implementation of an organisational resilience training program. The Resilience Expert Advisory Group will assist with this initiative in consultation with the Australian Emergency Management Institute and other interested business and government stakeholders. Critical infrastructure owners and operators will be a priority target group for delivery of the training program. Modules of the training program will range from an introduction to the concept of organisational resilience to a stand-alone 'Master Class on Organisational Resilience'. It would also be useful for the training program to include a module focussing on enhancing governments' understanding of business operating environments, and businesses' understanding of the machinery of government. This mutual understanding will contribute to a more effective business-government partnership. Over time, training in organisational resilience will be extended to other interested parties in business, government and the community.

Activity	Description
2.3 Promote the concept and practice of organisational resilience	While the concept and practice of organisational resilience will be promoted through the development of guidance materials, tools and training programs, a range of other initiatives will be developed and implemented to further promote organisational resilience. For example, the Australian Government will work with business to develop and promote case studies that illustrate real life examples of the 'value proposition' of organisational resilience. A study will be undertaken on the feasibility of implementing a mentoring program, where a senior executive with expertise in resilience could be loaned to another organisation to mentor management in organisational resilience. Another study will be undertaken on the feasibility of implementing a business awards program which would recognise and celebrate excellence in organisational resilience. One option may be to leverage off established and well regarded business awards programs to create a new category relating to excellence in organisational resilience.
2.4 Undertake specific research on organisational resilience	An important element of the CIR Strategy will involve deepening the understanding of organisational resilience as it specifically relates to the owners and operators of critical infrastructure. This will be reflected in the Strategy's research priorities. An initial point of focus will be the value proposition for resilience, including its direct relevance to business excellence and the long term prosperity of organisations. For example, further research and analysis could be undertaken to explain the relationships between good business practice, business sustainability, corporate social responsibility, quality management, business excellence and organisational resilience. Longitudinal studies could also help establish and validate the evidence base for organisational resilience. The Resilience Expert Advisory Group, in consultation with interested business and government stakeholders, will assist with the development of a research program on organisational resilience.

3. Assist owners and operators of critical infrastructure to identify, analyse and manage cross-sectoral dependencies

Activity	Description
3.1 The Critical Infrastructure Program for Modelling and Analysis (CIPMA)	CIPMA can examine the relationships and dependencies between critical infrastructure systems, and demonstrate how a failure in one sector can greatly affect the operation of critical infrastructure in other sectors. This 'virtual insight' assists owners and operators to enhance their mitigation strategies, and hence the resilience of their critical infrastructure, and provides the Australian Government with useful inputs to the development and direction of government policy on national security and CIR. In response to a recommendation from the HBSR, an independent review of CIPMA is currently being undertaken. The Australian Government will consider the findings and recommendations of the review, and announce the way forward for this important initiative.
3.2 Capacity building for incident preparedness	While the TISN is not an operational forum and has no formal role to play in incident response, it is important for critical infrastructure organisations to be prepared for incidents that have actual or potential cross-sectoral impacts that could disrupt critical infrastructure. To strengthen the preparedness of critical infrastructure organisations to manage cross-sectoral impacts, the Australian Government will develop and implement capacity building initiatives in consultation with business and government stakeholders. Further, the Australian Government will assist owners and operators of critical infrastructure to share lessons learnt from real and exercised incidents within their sector and across other Sector Groups. Participating in exercises can assist in building capacity in organisations. As such, exercises complement other capacity building initiatives.

Activity	Description
3.3 Annual desktop exercise on cross-sectoral dependencies and follow-up workshop.	Exercises have an important role to play in improving our preparedness for incidents, our understanding of cross-sectoral dependencies and tipping points that could trigger a decline in the resilience of our critical infrastructure. Exercises enable participants to think about and become more familiar with the current plans, procedures and the types of scenarios that will have significant implications for the operation of critical infrastructure – not only in their sector but across other sectors. Exercises can also help to promote cooperation and information exchange across sectors. To these ends, the Australian Government will support an annual 2 day desktop exercise and follow-up workshop on cross-sectoral dependencies in consultation with key business and government stakeholders. It is envisaged the exercise will be conducted in the second half of the year. The desktop exercise will take up the first day, and the second day will be dedicated to a follow-up workshop where key findings and lessons learnt will be identified and discussed. Exercises present an opportunity to not only understand interdependencies, but also to build communication, coordination and collaboration. To further facilitate cross-sectoral discussion, networking sessions will be included as part of these events.

4. Provide timely and high quality policy advice on issues relating to critical infrastructure resilience

Activity	Description
4.1 Coordination and advocacy of Australian Government's CIR policy	While whole-of-Australian Government policy coordination mechanisms are well established for the specific threat of terrorism and for some discrete policy issues, there may be a need to refine and enhance existing policy coordination mechanisms to ensure the effective implementation of the Australian Government's CIR Strategy. AGD will work with other Australian Government agencies on this matter. Relevant Australian Government agencies engaged in critical infrastructure act as an advocate for critical infrastructure within various machineries of government (e.g. Cabinet and Budget processes) where there are policy proposals or reforms which may impact on critical infrastructure. These agencies bring the knowledge and insight gained through the business-government partnership to represent critical infrastructure interests. Issues raised by Sector Groups and the Resilience Expert Advisory Group will inform and contribute to the development of Australian Government policy. Likewise, the Australian Government will ensure feedback mechanisms are in place so Sector Groups are aware of shifts in policy or new policy developments that may affect them. In addition, and given the important contribution that business can make to national security, CIAC has been asked to assist with the implementation of the Australian Government's CIR Strategy (see Strategic Imperative 1).
4.2 Horizon scanning to identify emerging issues	The provision of timely and high quality policy advice relies in part on the early identification of key emerging issues to allow maximum time for governments to understand the nature of the problem, develop options, and identify and socialise the preferred solutions. The establishment of the Resilience Expert Advisory Group is one way for the Australian Government to tap into the leading thinkers on resilience to assist in identifying emerging resilience-related policy issues.

Activity	Description
4.3 Coordination of international engagement on critical infrastructure-related issues	International engagement and research should continue to keep abreast of emerging issues and trends relevant to resilience, such as climate change adaptation and the trusted insider threat. Specific activities in international engagement on CIR include: • coordinating liaison with overseas governments • the initiation and management of productive bilateral and multilateral relationships with key countries and international organisations at the government to government level • developing and managing bilateral agreements and memoranda of understanding (MOU) • managing involvement by the Australian Government within key multilateral policy forums • identifying best practice, sharing lessons and identifying vulnerabilities in international supply chains • consultation with owners and operators of critical infrastructure on issues of international engagement, including providing feedback following engagement, where appropriate, and • developing policy advice for the Government on international critical infrastructure policy.

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

Activity	Description
5.1 Ensure critical infrastructure owners and operators are integrated into the implementation of the Cyber Security Strategy, including engagement with CERT Australia (Australia's national computer emergency response team)	CERT Australia commenced operations in January 2010. Run by AGD, it is the Australian Government's primary mechanism for engagement with the private sector on cyber security issues and works with, and provides advice to, the owners and operators of systems of national interest, including critical infrastructure. CERT Australia promotes greater shared understanding between government and business of the nature and scale of cyber threats and vulnerabilities within Australia's private sector networks and how these can be mitigated, including through a program of trusted cyber security information exchanges. It also provides targeted advice and assistance to enable the owners and operators of critical infrastructure and other systems of national interest to defend their systems from sophisticated electronic cyber attacks. In doing so, CERT Australia works in close collaboration with intelligence and law enforcement agencies via the Cyber Security Operations Centre (CSOC). The CSOC provides the Australian Government with all-source cyber security awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance. The CSOC will identify and analyse sophisticated cyber attacks and assist in responses to cyber events across government and critical private sector systems and infrastructure. The IT Security Expert Advisory Group (ITSEAG) supports the work of, and develops its work plan in consultation with, CERT Australia.

6. Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate

Activity	Description
6.1 More tailored engagement with States and Territories as appropriate	While most State and Territory critical infrastructure programs are based around resilience to all hazards, the Australian Government appreciates and respects the different emphases and approaches inherent in these programs and the complementary nature of critical infrastructure programs delivered by all governments in Australia. Accordingly, the Australian Government will undertake a more tailored approach to supporting State and Territory programs, and will progress this undertaking through a dialogue with jurisdictional colleagues at the National Critical Infrastructure Committee (NCIRC).
6.2 NCIRC to provide national coordination	NCIRC provides a forum for high level dialogue, collaboration and visibility of government activities relating to CIR. Where there are issues of a bilateral nature, specific engagement between the relevant governments will take place. The Australian Government (through AGD) is providing the secretariat support to NCIRC. This will include facilitating strong working relationships with relevant ministerial councils and committees, and undertaking further work on the roles and responsibilities of governments in relation to CIR.
6.3 Increased visibility of TISN activities	While the Australian Government encourages and welcomes State and Territory attendance and participation at TISN forums and activities, there is no expectation on the part of the Australian Government that this will occur on a consistent basis given the large number of TISN activities and the resource, priority and other constraints on all jurisdictions. In recognition of the growing maturity of the business-government partnership, and to ensure the States and Territories have greater visibility of the activities of the TISN, the Australian Government has agreed that all jurisdictions will have greater access to the TISN secure website, and that secretariats will post and update all relevant information to the website in a timely and comprehensive manner. States and Territories are also encouraged to use TISN mechanisms (e.g. the website or Sector Group meetings) to communicate with critical infrastructure owners and operators about activities and programs in their jurisdiction.

Activity	Description
6.4 Promote adherence to the COAG Principles and Protocols for Government Engagement with Critical Infrastructure Owners and Operators	In considering the review of national critical infrastructure arrangements, COAG agreed to a nationally consistent approach to engaging with critical infrastructure owners and operators. This approach assists in reducing overlap or conflict between the activities of Australian Government, and State and Territory critical infrastructure programs. The agreed principles and protocols include a provision that in the work of the TISN, all groups (including forums, workshops, CoI etc) will be encouraged to refer matters that relate primarily to State and Territory responsibility to NCIRC for coordination and response where appropriate. AGD desk officers will assist secretariats in this regard. If issues or concerns are raised in the TISN that relate to a particular State or Territory government, the secretariats, supported by the AGD desk officer, will propose that the matter be taken up with the relevant jurisdiction.

The Interconnectedness of the Strategic Imperatives of the CIR Strategy

The six strategic imperatives of the CIR Strategy identify the key work streams to deliver the Australian Government's policy aim and objectives with regard to CIR. Each strategic imperative supports and feeds into the others.

1. Operate an effective business-government partnership with critical infrastructure owners and operators

- A successful business-government partnership is an important element in building resilience. Sharing of information (for example, research and government prepared threat assessments) helps owners and operators better understand and mitigate their risks.
- This partnership helps owners and operators identify cross-sectoral dependencies, thus informing risk assessments and mitigation strategies.

2. Develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience

- Given the unique role played by organisations that operate critical infrastructure, building and promoting the organisational resilience body of knowledge is pivotal to the success of the CIR Strategy.
- The activities planned under this imperative will support a successful business-government partnership through, for example, the development of the Resilience Handbook and resilience training programs for public and private sector owners and operators.

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 risk assessments and consequently, mitigation policies.
- Greater insight to cross-sectoral dependencies contributes to the Australian Government's understanding of industry-wide security issues, thereby supporting the provision of high quality policy advice to Ministers.

4. Provide timely and high quality policy advice on issues relating to critical infrastructure resilience

- The ability of Australian Government agencies to provide high quality policy advice on a range of critical infrastructure related issues will be enhanced through achieving the other five strategic imperatives.
- A thorough understanding of cross-sectoral dependencies; a collaborative and complementary approach to the delivery of State and Territory government resilience programs; and the development of the resilience body of knowledge, all enable the provision of timely and high quality policy advice to the Australian Government.
- The business-government partnership informs the relevant Australian Government agency so they are better able to represent critical infrastructure interests and act as advocates within various Australian Government discussions where reforms and new policy proposals are being considered (e.g. climate change and the National Broadband Network).

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

- Maintaining a secure cyber environment is vital to Australia's continued economic and social wellbeing. Cyber security is an issue for all industry and government sectors and the effective delivery of the Cyber Security Strategy contributes to building resilience.
- If business is well informed of its operating environment, potential threats and cross-sectoral dependencies, this will contribute to identifying its cyber risks and better inform security and risk mitigation strategies.
- The facilitation of research on cyber security issues of importance to owners and operators of critical infrastructure will be informed by horizon scanning activities and emerging issues identified through international and domestic engagement.

6. Support the critical infrastructure resilience programs delivered by Australian States and Territories, as agreed and as appropriate

- All Australian governments have active and targeted critical infrastructure programs. Many owners and operators of critical infrastructure are engaged with all three levels of government. It is in the interests of the Australian Government to support all programs that contribute to building the resilience of organisations, including those delivered by State and Territory governments.
- Support for and understanding of State and Territory government resilience programs helps the Australian Government work more effectively with owners and operators, thus achieving a stronger business-government partnership. It also avoids potential duplication.