The Australian Government's Critical Infrastructure Resilience Strategy: Plan

INTRODUCTION

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[1]'.*

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 achieve the continued provision of essential services (provided by critical infrastructure) to businesses, governments and the community, as well as to other critical infrastructure sectors.

Implementation of the Strategy is through a broadly non-regulatory business-government partnership. There are two core policy objectives under the Strategy. The first objective is for critical infrastructure owners and operators to be effective in managing reasonably foreseeable risks to the continuity of their operations, through a mature, risk-based approach. The second objective is for critical infrastructure owners and operators to be effective in managing unforeseen risks to the continuity of their operations through an organisational resilience approach.

The key outcomes that the Strategy seeks to achieve are:

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.

This *Plan* outlines the core activities that will be undertaken at a national level in pursuit of these outcomes. **It is a 'living' document and will be updated as required.** The *Plan* is to be read in conjunction with the *Policy Statement*, which provides the high-level policy direction underpinning the Australian Government's approach to critical infrastructure resilience.

The *Statement* and *Plan* both aim to complement existing industry business continuity plans of owners and operators, and state and territory government plans and arrangements.

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.

[1] 2010 Australian Government Critical Infrastructure Resilience Strategy. 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.

ENGAGEMENT WITH INDUSTRY

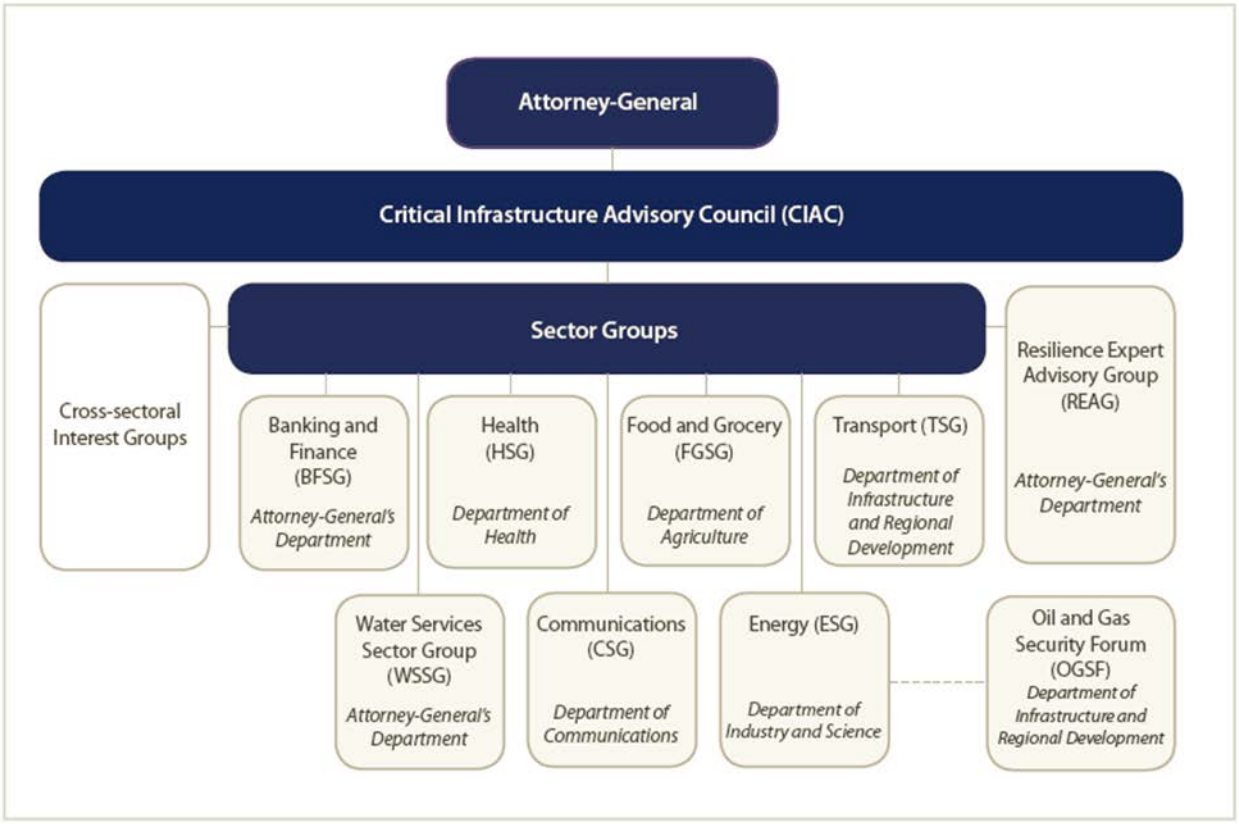
Delivery of the Critical Infrastructure Resilience Strategy is dependent on a productive business-government partnership. In practice, there are a range of forums which contribute to the aim of ensuring the continued operation of critical infrastructure.

The Trusted Information Sharing Network (TISN) was established by the Australian Government in 2003, and remains Australia's primary national engagement mechanism for business-government information sharing and resilience-building initiatives. The TISN provides a secure environment in which critical infrastructure owners and operators across seven sector groups meet regularly to share information and cooperate within and across sectors to address security and business continuity challenges.

The sector groups of the TISN include banking and finance, communications, energy, food and grocery, health, transport and water. In addition, there are specialist forums (Cross-Sectoral Interest Groups) which assist in the temporary exploration of cross-cutting issues, and a Resilience Expert Advisory Group which has a strong focus on organisational resilience.

Coordination and strategic guidance for the TISN is provided by the Critical Infrastructure Advisory Council (CIAC). CIAC consists of the Chairs of each of the TISN Groups, senior Australian Government representatives from relevant agencies, and senior state and territory government representatives.

Figure 1 shows the governance structure for the TISN.



The work of the TISN is complemented by a range of other business-government engagement mechanisms on broader national security policy issues. The Australian Security Intelligence Organisation's Business Liaison Unit (BLU)

provides an interface between Australian business and the Australian intelligence community. The BLU aims to ensure that owners and operators of critical infrastructure and other relevant members of the Australian business community can access timely information on matters affecting the security of the assets and staff for which they are responsible.

The Industry Consultation on National Security (ICONS) is the Australian Government's primary business-government engagement mechanism at the CEO level on national security matters. ICONS provides an opportunity for business leaders to engage directly with the Attorney-General on national security issues, shape broad solutions to mitigate national security risks, and advance the deregulation agenda as it relates to national security. ICONS membership includes participants from many of Australia's critical infrastructure sectors.

ENGAGEMENT WITH GOVERNMENT

Critical infrastructure protection and resilience is of paramount interest to governments. There is a strong expectation within the Australian community that governments will take all necessary action to safeguard our critical infrastructure and assure its continued operation. The Australian and state and territory governments all own and operate some critical infrastructure.

Australia's federated system means that different governments have different direct responsibilities for critical infrastructure depending upon its type, or upon the nature of the threat. Intergovernmental work on critical infrastructure occurs on a cooperative basis.

State and territory governments

State and territory governments are responsible for managing threats to life and property within their jurisdictions. They prepare for and respond to emergencies, and ensure law and order. They also often deliver essential services such as healthcare and the supply of water. All Australian state and territory governments have their own critical infrastructure programs according to the operating environment and arrangements for each jurisdiction. The Australian Government's Critical Infrastructure Resilience Strategy aims to complement these programs and support their objectives wherever possible.

State and territory governments are also key participants in the TISN. All TISN sector groups benefit from state and territory government participation, with jurisdictional representatives sharing valuable information and providing points-of-contact for industry members on jurisdictional and local arrangements. It is essential that critical infrastructure owners and operators know and understand the jurisdictional response arrangements and have good working relationships with the appropriate state and territory agencies.

As partners in promoting national critical infrastructure protection and resilience, it is important that the value provided to state and territory governments through this Strategy is maximised wherever possible. The interests of critical infrastructure owners and operators, the Australian Government and state and territory governments are advanced through a cooperative approach.

Australian Government

The Australian Government is responsible for national defence and security, and for assisting states and territories to respond to large-scale emergencies when requested to do so. The Australian Government also has direct regulatory oversight over a number of critical infrastructure sectors, such as aviation, communications, offshore oil and gas and banking. In a number of cases, these regulatory agencies participate in the TISN (in a non-regulatory capacity) with the aim of contributing to the resilience of the relevant sector. In this way the TISN provides an important informal link between industry sectors and the agencies that supervise their activities.
A range of other Australian Government agencies have policy responsibilities that are relevant to critical infrastructure sectors. An overview of these responsibilities is provided at **Appendix A**.

KEY OUTCOMES

Outlined below are the four key outcomes that will be delivered through the Critical Infrastructure Resilience Strategy. These outcomes will be used to assess the success of the Strategy when it is reviewed in 2020. A number of high-level activities are listed that will contribute toward each outcome, and in turn underpin the aim and objectives of the Critical Infrastructure Resilience Strategy.

Figure 2 shows how the four outcomes work together to build overall critical infrastructure resilience.

It is not intended for all activities to occur in all sector groups at the same time. CIAC will set and review strategic priorities to guide the activities of the TISN, based on input from sector groups, government, and the outcomes of sectoral and cross-sectoral activities. This approach aims to ensure that an appropriate balance is struck between the provision of strategic direction and priority setting by CIAC, and the targeting of activities according to the specific needs of each sector. More detailed implementation plans including timeframes and responsibilities will be developed for each CIAC priority, and as part of the work plans developed by each TISN group.

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.

Activities

1.1 ***Effective forums and arrangements exist that facilitate information exchange between businesses and governments.***

1.1A - Maintain and enhance sectoral information sharing initiatives, such as sector group meetings, threat briefings, exercises and teleconferences on issues of concern to TISN members; and the trusted environment of the TISN in

which these activities occur, by ensuring the currency of governance arrangements and establishing clear protocols for participation (including virtual participation).

1.1B - Increase engagement with senior business leaders on critical infrastructure issues, including through the Industry Consultation on National Security (ICONS).

1.2 ***Effective leadership of the TISN through enhanced strategic guidance and priority setting by CIAC.***

1.2.A - Ensure arrangements are in place for CIAC to set and review strategic priorities to guide the activities of the TISN (including the need for additional groups as appropriate), based on input from sector groups, government, and the outcomes of sectoral and cross sectoral activities.

1.2B - Implement annual work plans and related reporting by TISN groups to CIAC and Government outlining key resilience achievements of the past year and priorities for the year ahead, aligned to the key outcomes of the Critical Infrastructure Resilience Strategy.

1.2C - Provide greater opportunities for TISN groups and governments to present current and emerging issues to CIAC for consideration.

1.3 - ***A flexible participation model for the Strategy that delivers value to participants, including through enhanced information sharing.***

1.3A - Implement a more flexible participation model whereby critical infrastructure organisations and state and territory government agencies are encouraged to take a whole-of-organisation point-of-contact approach to "membership" of the TISN. This will enable key people within organisations to participate in TISN activities of greatest relevance and value to them.

1.3B - Utilise available technologies such as video and teleconferencing facilities for meetings and activities, to complement face-to-face engagement.

1.3C - Improve the functionality of the TISN public and members' websites to ensure their value to critical infrastructure stakeholders, including through:

- a 'knowledge hub' of useful information, articles, case studies and reports,
- greater access to cross-sectoral information,
- the establishment of a regular Critical Infrastructure Resilience e Newsletter, covering both sector specific and cross sectoral/strategic issues, and
- enabling virtual collaboration both within and across sectors, and internationally.

1.4 - ***Effective linkages and collaboration between critical infrastructure stakeholders.***

1.4A **-** Identify relevant industry associations, forums and non-member owners and operators that can be engaged to promote the work of the TISN, and to collaborate on issues of mutual interest/concern. Where appropriate, relevant information on critical infrastructure issues will be provided to these organisations for broader dissemination.

1.4B - Increase engagement and collaboration with the critical infrastructure programs of key international partners; promote international participation in TISN events, particularly through virtual collaboration; participate in international exercises; and identify and promote world's best practice.

1.4C - Strengthen both formal and informal engagement between relevant Commonwealth government agencies to increase the effectiveness of both government-led resilience initiatives and the support provided to TISN groups, including through the creation of a Commonwealth Government Cross-sectoral Interest Group to increase the resilience of Commonwealth Government owned and operated critical infrastructure.

1.4D - Establish a new Commonwealth/State and Territory inter-governmental consultation forum to facilitate greater collaboration and cooperation on issues of mutual interest, and enhance the value of TISN initiatives for state-based agencies.

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.

Activities

2.1 - ***A clearer understanding of the systems, networks and assets that are most critical at a national level; and of the resilience of our critical infrastructure sectors***.

2.1A - Develop sector-level understanding of nationally vital and significant critical infrastructure assets or networks, by:

- developing sector/systems-level guidance for undertaking criticality and dependency assessments; and
- implementing a sectoral approach to determining national criticality, utilising TISN Sector Groups with support from the Attorney General's Department and relevant government agencies.

2.1B - Develop guidance for indicative measures of resilience at the sectoral level; undertake an initial sector level resilience benchmarking exercise to determine indicative resilience levels of critical infrastructure sectors in Australia; and identify and agree opportunities for improvement.

2.2 - ***Well-developed understanding and awareness of cross sector dependencies; supported through effective collaboration and networks across sectors.***

2.2A - Establish a program of targeted, more frequent, smaller-scale, cross sectoral workshops and exercises on specific issues of interest to two or more sectors (prioritised by CIAC), including following-up on the outcomes of

these events. This will include holding events in a broader range of jurisdictions to provide the opportunity to tailor events around particular geographic issues.

2.2B - Further enhance the effectiveness of services provided by the Critical Infrastructure Program for Modelling and Analysis (CIPMA) to critical infrastructure organisations and governments, to gain a clearer understanding of cross-sector dependencies and impacts.

2.2C - Facilitate greater cross-sectoral information sharing between TISN sector groups, including through:

- the establishment of temporary Cross-sectoral Interest Groups, as required;
- joint sector group meetings; and
- sharing sector newsletters, reports and other information via the TISN members' site.

2.2D - Explore opportunities for a peer exchange program between critical infrastructure organisations, and other opportunities such as 'organisation open days', to promote understanding and deeper cross-sectoral relationships.

2.3 - ***An increased capability to explore and understand cyber cross sector dependencies.***

2.3A - Increase the exploration of cyber cross-sectoral dependencies through more cyber-focused TISN activities, including in conjunction with CERT Australia and CIPMA.

2.3B - Explore opportunities for greater international collaboration on cyber security issues as they relate to critical infrastructure.

2.3C - Implement the outcomes of the Australian Government's cyber security review as they relate to critical infrastructure.

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.

Activities

3.1 - ***High quality policy advice and advocacy on issues relating to critical infrastructure resilience is provided to the Australian Government.***

3.1A - Provide high-quality advice on critical infrastructure resilience issues to the Australian Government; and provide opportunities through the TISN, and other forums such as ICONS, for critical infrastructure organisations to contribute to policy development and implementation.

3.2 - ***An increased understanding and awareness of strategic issues and trends; and their impact on the operating environment of critical infrastructure.***

3.2A - Ensure there are appropriate forums (such as the Critical Infrastructure Resilience Conference, Cross-sectoral Interest Groups, workshops and exercises) for examining strategic issues and trends and promoting resilience best practice.

3.2B - As part of the TISN website enhancements, incorporate mechanisms to support information sharing on significant trends and strategic issues, including existing or new research and forecasts; and enable virtual discussions and collaboration on key strategic issues.

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.

Activities

4.1 - ***An increased capacity for critical infrastructure owners and operators to manage unforeseen or strategic risks to their operations, through the implementation of an organisational resilience approach.***

4.1A - The Resilience Expert Advisory Group (REAG) to continue to develop the organisational resilience body of knowledge and further review and refine the resilience indicators.

4.1B - Partner with relevant organisations (including the Australian Emergency Management Institute and other academic institutions) on:

- the development and delivery of workshops and programs on organisational resilience, and
- research on organisational resilience, its benefits and the underpinning resilience indicators.

4.1C - Continue to develop relevant, practical and user-friendly tools and guidance material to assist businesses to implement an organisational resilience approach. This includes maintaining, improving and promoting the Organisational Resilience website and establishing it as the primary authoritative source of information on organisational resilience.

4.1D - Undertake work to explore and establish the links between critical infrastructure, community and disaster resilience; and complement activities under the National Strategy for Disaster Resilience.

4.1E - Explore opportunities to directly promote organisational resilience to critical infrastructure owners and operators. This could include, for example, the creation of resilience champions and mentors.

APPENDIX A: AUSTRALIAN GOVERNMENT ROLES AND RESPONSIBILITIES[2]

The Attorney-General's Department is responsible for:

- leading and developing whole-of-Australian-Government policy on critical infrastructure,
- providing policy advice to the Australian Government on critical infrastructure issues,
- supporting and substantially contributing to the policy agenda of:
    - the Industry Consultation on National Security (ICONS),
    - the Critical Infrastructure Advisory Council (CIAC),
    - the Banking and Finance Sector Group (BFSG),
    - the Water Services Sector Group (WSSG), and
    - the Resilience Expert Advisory Group (REAG).
- facilitating the sharing of threat and risk information in consultation with security agencies.
- providing CIPMA, a specialist modelling and analysis capability focussed on strengthening critical infrastructure resilience.
- providing, through CERT Australia, the key point of contact in the Australian Government for cyber security issues affecting Australian critical infrastructure and systems of national interest.

The Australian Security Intelligence Organisation is responsible for:

- providing timely advice to owners and operators on security threats to critical infrastructure as appropriate,
- preparing and briefing owners and operators on critical infrastructure threat assessments for each sector, and for individual assets as appropriate,
- conducting protective security risk reviews for specified critical infrastructure as appropriate.

The Department of Agriculture is responsible for:

- providing specialist portfolio policy advice on critical infrastructure,
- supporting and substantially contributing to the policy agenda of the Food and Grocery Sector Group, and
- facilitating the sharing of threat and risk information for the food and grocery sector, in consultation with security agencies.

The Department of Communications is responsible for:

- providing specialist portfolio policy advice on critical infrastructure,
- supporting and substantially contributing to the policy agenda of the Communications Sector Group, and
- facilitating the sharing of threat and risk information for the communications sector, in consultation with security agencies.

The Department of Health is responsible for:

- providing specialist portfolio policy advice on critical infrastructure,
- supporting and substantially contributing to the policy agenda of the Health Sector Group, and
- facilitating the sharing of threat and risk information for the health sector, in consultation with security agencies.

The Department of Infrastructure and Regional Development is responsible for:

[2] A range of other agencies, such as the Australian Federal Police and the Australian Border Force, also contribute to the resilience of Australia's critical infrastructure through operational and investigative responsibilities. Only those with policy responsibility for critical infrastructure resilience are included here.

- regulating preventive security planning in the aviation and maritime transport, air cargo supply chain and offshore oil and gas sectors,
- providing specialist portfolio policy advice on critical infrastructure,
- supporting and substantially contributing to the policy agenda of the Transport Sector Group and the Oil and Gas Security Forum,
- working with all jurisdictions to coordinate the dissemination of 'best practice' information on security measures in relation to surface transport security, and
- communicating a common picture of threat and risk to the transport and offshore oil and gas sectors and government stakeholders.

The Department of Industry and Science is responsible for:

- providing specialist portfolio policy advice on critical infrastructure,
- supporting and substantially contributing to the policy agenda of the Energy Sector Group and the Space Community of Interest, and
- facilitating the sharing of threat and risk information for the energy sector, in consultation with security agencies.

The Department of Prime Minister and Cabinet is responsible for:

- leading Australian Government policy on cyber security, and
  providing advice to the Prime Minister and whole of-Australian Government coordination on national security matters.