From: Andrew KILEY
To: s. 22(1)(a)(ii)
Subject: FW: TISN for CI Resilience - request for info [DLM=For-Official-Use-Only]
Date: Tuesday, 18 February 2020 12:26:12 PM
Attachments: MS19-002869 - minister signed submission.pdf

For-Official-Use-Only

Andrew Kiley
Assistant Secretary | Assurance, Risk and Engagement Branch
Critical Infrastructure Security Division
Department of Home Affairs
P: 02 s. 22(1)(a)(ii) | M: s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @homeaffairs.gov.au

For-Official-Use-Only

From: Samuel GRUNHARD s. 22(1)(a)(ii) @homeaffairs.gov.au>
Sent: Tuesday, 18 February 2020 11:53 AM
To: Craig MACLACHLAN <s. 22(1)(a)(ii) @homeaffairs.gov.au>
Cc: s. 47E(d) @homeaffairs.gov.au>; s. 47E(d) @homeaffairs.gov.au>; Andrew KILEY s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 47E(d) s. 47E(d) @homeaffairs.gov.au>; s. 22(1)(a)(ii) s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>
Subject: RE: TISN for CI Resilience - request for info [DLM=For-Official-Use-Only]

For-Official-Use-Only

Hi Craig,

I understand you requested some information this morning about the TISN and the Resilience Strategy. Please find below and attached, and let us know if you need anything further for now.

- The Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) is the Australian Government's primary national engagement mechanism for business-government information sharing and resilience-building initiatives relating to critical infrastructure.
    - It is a trusted, non-competitive environment comprised of a significant number of highly engaged industry bodies from across the banking and finance, communications, energy, water services, health, transport and food and grocery sectors. Similar business-government mechanisms exist in Canada and the United States and form the basis of government-industry critical infrastructure resilience arrangements in those countries.
- The TISN is a mechanism through which government can and does engage with industry on a broad range of issues, including all-hazards resilience, but also including any issues government wishes to engage with critical infrastructure

owners and operators on.

- It is also the primary mechanism through which we engage with industry to deliver the Critical Infrastructure Resilience Strategy (CIRS), last updated in 2015 and due for refresh this year.
- Through TISN, industry and government regularly discuss security, business continuity and resilience measures, including industry preparation and response to events.
    - While not operational, TISN groups have supported the national response to the recent bushfire crisis, and are also assisting in delivering messages relating to the COVID-19 outbreak. Lessons learned through these (and past) events form the basis of ongoing resilience planning. As an example, the Water Services Sector Group are developing best practice advice for the water sector on recovery after a bushfire, with particular regard to drinking water quality.
- The Minister noted the approach to the revised CIRS in October 2019 (MS19-002869 refers and is attached). The department therefore commenced industry consultation regarding the revised CIRS in November 2019. The revised CIRS is due for release in 2020 and will provide the policy platform for the more effective delivery of resilience outcomes.
    - s. 47C(1) [redacted]
    - A strengthened and reinvigorated Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) will be used to re-energise government-industry partnerships, and enhance and integrate Government's existing industry education, communication and engagement activities, with an integrated view of security as part of the existing all-hazards approach.
    - Industry stakeholders are engaged and highly motivated, and have provided significant feedback on both the draft revised strategy, and how to best structure the TISN to maximise outcomes for industry.
    - s. 47C(1) [redacted]

Kind regards
Sam

Sam Grunhard
a/g First Assistant Secretary
Critical Infrastructure Security Division
Security and Resilience Group
Department of Home Affairs
P: 02 s. 22(1)(a)(ii) [redacted] | M: s. 22(1)(a)(ii) [redacted]
E: s. 22(1)(a)(ii) [redacted] @homeaffairs.gov.au

For-Official-Use-Only

From: s. 47E(d) @homeaffairs.gov.au>
Sent: Monday, 17 February 2020 3:03 PM
To: s. 22(1)(a)(ii) @homeaffairs.gov.au>
Cc: s. 47E(d) @homeaffairs.gov.au>; s. 47E(d) @homeaffairs.gov.au>
Subject: TISN for CI Resilience - request for info [DLM=For-Official-Use-Only]

For-Official-Use-Only

Hi s. 22(1)(a)(ii)

Minister Dutton's CoS has asked for some information on the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience.

Craig is happy to receive the info via email from Sam. Are you able to arrange some details to be sent to Craig by midday tomorrow?

Some basic details about the background and current status of the review would be ideal.

Kind Regards,
s. 22(1)(a)(ii)

s. 22(1)(a)(ii)
Senior Departmental Liaison Officer
Office of the Hon Peter Dutton MP
Minister for Home Affairs
Suite MG.46, Parliament House, Canberra
P: 02 s. 22(1)(a)(ii) | M: s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @homeaffairs.gov.au | s. 22(1) @homeaffairs.gov.au

For-Official-Use-Only

For-Official-Use-Only

Australian Government
Department of Home Affairs

Submission

For information
PDMS Ref. Number MS19-002869

To **Minister for Home Affairs**

Subject **Review of the Critical Infrastructure Resilience Strategy**

Timing At your convenience, noting upcoming industry engagements events in early November.

Recommendations

That you note the proposed approach to:

1. review the Critical Infrastructure Resilience Strategy, and — noted / please discuss
2. refresh the implementation mechanisms which underpin the Critical Infrastructure Resilience Strategy. — noted / please discuss

Minister for Home Affairs

Signature.....

Date...15.../...10.../2019

RECEIVED
30 SEP 2019
Minister for Home Affairs

Minister's Comments

Rejected	Timely	Relevance	Length	Quality
Yes/No	Yes/No	☐ Highly relevant ☐ Significantly relevant ☐ Not relevant	☐ Too long ☐ Right length ☐ Too brief	Poor 1.....2.....3.....4.....5 Excellent **Comments:**

Key Issues

1. The Critical Infrastructure Resilience Strategy (2015-2020) (the Strategy) was launched by the then Attorney-General in May 2015. The aim of the 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 to businesses, governments and the community.
2. Responsibility for the Strategy transferred from the Attorney-General to you as part of the Machinery of Government changes to establish the Home Affairs Portfolio.
3. The current Strategy comprises two publically available documents: a Policy Statement and a Plan (**Attachments A and B**).
4. The principles and content of the current Strategy are largely sound. However, the documents require updating for release in 2020, in line with the Strategy's five-year review cycle. This provides an opportunity to refresh content and refocus the Strategy to better address evolving national security risks such as foreign involvement.
5. The current implementation mechanism for the Strategy centres around the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN). The TISN provides a secure environment for critical infrastructure owners and operators across eight sector groups to regularly share information and cooperate within and across sectors to address resilience, security and business continuity challenges.
6. The TISN is overseen by the Department in conjunction with the Critical Infrastructure Advisory Council (CIAC), where Commonwealth, state and territory government representatives meet twice a year with sector chairs from industry.
7. On November 6 2019, CIAC will meet to discuss the Strategy revision. CIAC will be asked to shape the strategy and its implementation to ensure it meets the needs of Government and Industry. The Department will also meet with sector groups on 7-8 November at which the review of the Strategy will be a point of discussion.

8. The updated Strategy will provide an opportunity to update the strategy for today's threat environment, review the operation of the TISN, coordinate roles across Commonwealth agencies and State and Territory governments, and consider streamlining material into a single document.

9. The Department will aim to increase the effectiveness of the TISN by better utilising available resources, including by encouraging sector groups to operate on a more self-sufficient basis with Government providing stronger information sharing and policy support.

Next steps

10. Following engagement in November, the Department proposes to undertake more detailed consultation with relevant stakeholders in early 2020. Following this consultation we will seek your approval of the updated strategy. We will engage with your Office as necessary throughout this process.

11. The Department will also align the updated strategy and implementation to other work being progressed by the Department in relation to enhanced critical infrastructure compliance and the review of the Critical Infrastructure Centre, as well as the 2020 Cyber Security Strategy.

Consultation – internal/external

Internal consultation

12. Cyber Security Policy Division, Aviation and Maritime Security Division.

External consultation

13. The Department of Communications and the Arts, the Department of Environment and Energy, the Department of Health and the Department of Agriculture have been consulted in their capacity as secretariats for TISN sector groups.

14. The Resilience Expert Advisory Group, comprised of industry and academic members, is providing industry insights and support to the development of the Strategy and implementation mechanisms.

15. TISN members have provided their intial views on Strategy development and implementation mechanisms.

Consultation – Secretary

16. The Secretary was not consulted on the approach in the submission.

Client service implications

17. NIL.

Sensitivities

18. The information contained in this submission is classified and should not be publicly released without the authority of the Department of Home Affairs. In accordance with our long standing practices, should you wish for unclassified media lines to be prepared in relation to this issue please contact the Home Affairs Media Coordination team at media@homeaffairs.gov.au.

Financial/systems/legislation/deregulation/media implications

19. NIL.

Attachments

Attachment A Critical Infrastructure Resilience Strategy Policy Statement 2015

Attachment B Critical Infrastructure Resilience Strategy Plan 2015

Authorising Officer
Cleared by: Sam Grunhard A/g First Assistant Secretary Critical Infrastructure Security Division Date: 26 September 2019 Ph: 02 s. 22(1)(a)(ii)

Contact Officer Andrew Kiley, Assistant Secretary, Assurance, Risk and Engagement Branch, Ph: s. 22(1)(a)(ii)

Through Paul Grigson, Deputy Secretary, Security and Resilience

CC Secretary
Marc Ablong, Deputy Secretary, Policy

From: s. 47E(d)
To: s. 22(1)(a)(ii)
Cc: s. 47E(d) ; s. 22(1)(a)(ii)
Subject: For Action: Minute: Review of the Critical Infrastructure Resilience Strategy [DLM=For-Official-Use-Only]
Date: Monday, 19 August 2019 1:24:06 PM
Attachments: Minute- Review of Critical Infrastructure Resilience Strategy.pdf
Attachment A. CriticalInfrastructureResilienceStrategyPolicyStatement.PDF
Attachment B. CriticalInfrastructureResilienceStrategyPlan.PDF
Attachment C. Critical Infrastructure Resilience Strategy Handbook.DOCX

For-Official-Use-Only

Hi s. 22(1)(a)(ii)

Please see the attached Review of the Critical Infrastructure Resilience Strategy Minute signed by Sam and relevant attachments for Paul's consideration.
Please let me know if you would like the printed version with the attachments and I can bring it over to you.

Regards

s. 22(1)(a)(ii)
A/g Executive Officer
A/g FAS Sam Grunhard | Critical Infrastructure Security
Security and Resilience Group
Department of Home Affairs
P: 02 s. 22(1)(a)(ii)

For-Official-Use-Only

Australian Government
Department of Home Affairs

For Official Use Only

Minute

To: **Deputy Secretary, Security and Resilience** s. 22(1)(a)(ii)

Through: A/g First Assistant Secretary, Critical Infrastructure Security Division

Date: 15 August 2019

Review of the Critical Infrastructure Resilience Strategy

Timing

None, however prompt consideration will enable earlier targeted consultation with stakeholders.

Purpose

To note the proposed approach to:

a. review the Critical Infrastructure Resilience Strategy, and
b. refresh the implementation mechanisms which underpin the strategy.

Background

1. The current Critical Infrastructure Resilience Strategy (2015-2020) comprises three documents; a Policy Statement, a Plan (both publicly available) and an internal Handbook (see Attachments A, B and C). The strategy takes an all hazards approach to critical infrastructure resilience. The 2015-20 strategy includes a prescriptive list of 29 work items that sector groups and the Commonwealth are required to drive. The implementation of the Strategy is overseen by the Critical Infrastructure Advisory Council (CIAC), where Commonwealth, state and territory government representatives meet twice a year with sector chairs from industry.
2. The principles and content of the current strategy are largely sound. However, the documents require updating for release in 2020. This provides a good opportunity to refresh content and refocus the strategy to better address evolving national security risks, alongside reconsidering how we can best drive outcomes.
3. The current implementation mechanism for the strategy centres around the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN). The TISN provides a secure environment for critical infrastructure owners and operators across eight sector groups to regularly share information and cooperate within and across sectors to address resilience, security and business continuity challenges. The TISN is supported by the use of GovTEAMS, a whole-of-government web platform which provides for secure information sharing across sectors.
4. The Department of Home Affairs (the Department) provides secretariat support for four sectors: the banking and finance and water sectors (CISD) and the transport sector and oil and gas security forum

(AMS). The Department also supports the Resilience Expert Advisory Group (REAG) which discusses, develops and promotes organisational resilience across private and public sector industries. The other sector groups are supported by other Commonwealth departments.

Issues

5. While the existing Strategy and TISN continue to provide a sound base for working with industry on resilience and security matters, there are some issues that need to be resolved:

   Funding – ongoing funding was provided to departments with responsibility for secretariat duties to fully fund these activities. These funds have since moved from an identified work stream into each department's base departmental allocation, resulting in a loss of visibility and making funds subject to the discretion of the respective agency heads,

   Sector maturity – due to the spread of secretariat responsibilities across a number of government agencies, and varying levels of industry participation, sectors have different levels of engagement, maturity and effectiveness, and

   Duplication of effort – recent feedback from TISN secretariats and members indicates that it is difficult to keep industry engaged in TISN activities including as a result of duplication of effort across Commonwealth and State/Territory government.

Opportunities

6. The updated strategy will provide an opportunity to:

   a. define the roles and responsibilities for Commonwealth, state and territory governments and industry
      i. this will include clarifying roles and responsibilities across Commonwealth agencies, including different areas of Home Affairs,
   b. set out government's expectations for how industry manages risk, for example, through a critical infrastructure security code of conduct,
   c. emphasise national security risk within the all hazards approach to critical infrastructure resilience,
   d. better align the strategy (and associated implementation) with existing (and future) Commonwealth and state and territory government strategies that relate to critical infrastructure,
   e. explore whether the document should be a *national* strategy endorsed by states and territories and considered by the Council of Australian Governments,
   f. develop a more responsive high-level principles approach to achieving resilience and security outcomes,
   g. streamline documentation by considering the need for a separate Policy Statement, Plan and Handbook,
   h. ideally incorporate a system for measuring the resilience and security posture of sectors, and
   i. review the structure and function of the TISN to:
      i. ensure the TISN is capturing all relevant parts of the CI community,
      ii. consider new ways of information sharing,
      iii. reduce duplication of effort, and
      iv. use Commonwealth resources more effectively.

Business Government Collaboration

7. The Department will aim to increase the effectiveness of the TISN by better utilising available resources, noting current resources are severely constrained (see 'Resourcing' below). There are several options for achieving this, including;

   a. a renewed focus on engaging on a threat vector rather than sector basis (for example, cyber threats, natural hazards, foreign involvement),

b. sectors operating on a more self-sufficient basis, providing their own secretariat support and functioning more independently from the Commonwealth government (similar to the United States' Information Sharing and Analysis Centres),

c. outsourcing the secretariat and logistics support currently provided to sector groups, as well as the responsibility for producing papers on relevant topics and co-ordinating major events,

d. abolishing the national TISN structure and bringing together the state and territory TISN equivalents once or twice per year in a 'CIAC-like' meeting,

e. Commonwealth Government support focusing more exclusively on information and contact sharing between industry and state and territory government (through the GovTEAMS platform) as well as higher value events and policy discussion, and

f. a combination of the above options.

Consultation

8. Consultation will be paramount in developing a strategy and implementation mechanisms that are accepted by both industry and government.

9. The REAG, comprised of industry and academic members, is providing industry insights and support to the development of the strategy and implementation mechanisms.

10. Subject to your consideration, we will begin to engage more formally with a select group of industry and state and territory government representatives to ensure we have the necessary buy-in and so that the strategy and implementation mechanisms align with expectations.

11. Our proposed consultation (late 2019) includes a roadshow to major capital cities to allow industry and state and territory governments to directly engage with this work. However, we are aware of the upcoming Cyber Strategy consultations and are working closely with our colleagues in the Cyber Security Policy Division (CSPD) to ensure that consultation does not overlap. CISD and CSPD agree that consultations on these two processes should not coincide and that the Cyber Strategy will likely need to proceed first, subject to decisions to be made by Government.

Timing

12. It is proposed that the completed strategy will be subject to Ministerial endorsement and released by June 2020. This is in line with the five-year review cycle.

Resourcing

13. Currently there are three FTE (one APS6, one EL1 and an EL2) administering the TISN alongside other duties. There are also some resources within other agencies who have secretariat responsibilities for sector groups.

14. The resourcing requirements to implement the options above have not been fully assessed, however current staffing and resourcing levels are likely insufficient to successfully deliver some of the options outlined above.

Consultation

15. The 2015 Strategy was released by the then Attorney-General, and the Minister for Home Affairs has not yet had visibility of this process. We propose to brief the Minister ahead of the proposed roadshow.

Recommendation

It is recommended that you:

16. note the proposed approach to:

    a. review the Critical Infrastructure Resilience Strategy, and
    b. refresh the implementation mechanisms for enabling the strategy.

s. 22(1)(a)(ii)

Noted ☐ Discuss ☐

Andrew Kiley

Assistant Secretary, Critical Infrastructure Security Division

(02) s. 22(1)(a)(ii)

16 August 2019

Paul Grigson

Deputy Secretary, Security and Resilience

August 2019

Contact Officer: s. 22(1)(a)(ii)

Division/branch: Critical Infrastructure Security Division

Phone: (02) s. 22(1)(a)(ii)

Attachments

Attachment A: Critical Infrastructure Resilience Strategy Policy Statement

Attachment B: Critical Infrastructure Resilience Strategy Plan

Attachment C: Critical Infrastructure Resilience Strategy Handbook

TISN
FOR CRITICAL INFRASTRUCTURE
RESILIENCE

Critical Infrastructure Resilience

Handbook

Contents

Introduction

The resilience of Australia's critical infrastructure is a shared responsibility between owners and operators of critical infrastructure and Australian, state and territory governments.

Australian, state and territory governments have complimentary critical infrastructure programs. These programs include activities and measures designed to ensure both the protection of critical infrastructure from terrorism, and its resilience against a wide range of threats and hazards. Australian, state and territory governments work together in this regard and collaborate with industry through a range of fora to maximise information sharing, increase the awareness of threats and hazards, and develop possible solutions to common security and resilience challenges.

State and territory governments bear primary responsibility for responding to critical infrastructure related incidents that occur within their jurisdictions. Likewise, each state and territory government has its own critical infrastructure program geared to its operating environment and local arrangements. For example, state and territory governments often operate critical infrastructure in their own right and need to coordinate their emergency response efforts with other (private sector) owners and operators of linked infrastructure.

The Victorian Government is the only government that has specific legislation and related regulations for critical infrastructure resilience. Other jurisdictions, including the Commonwealth, have opted to take a mostly non-regulatory approach to building the resilience of our critical infrastructure to all hazards.

Community expectations

The community expects that the Australian Government is engaged on issues that could, or do, significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.

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.

Critical Infrastructure Resilience Strategy

The Australian Government's approach to strengthening the resilience of our critical infrastructure is set out in the Critical Infrastructure Resilience (CIR) Strategy, which was released in May 2015. There are two key facets of the Strategy.

- Firstly, the Strategy adopts an all hazards approach. This ensures that critical infrastructure owners and operators are able to prepare, plan, respond and recover from a broad range of threats.

  These threats and hazards may include natural disasters, pandemics, negligence, accidents, criminal activity, terrorism, trusted insiders and cyber-attack.

- Secondly, the Strategy puts collaboration with critical infrastructure owners and operators at the centre of its delivery.

There are two objectives of the strategy:

- Critical infrastructure owners and operators are effective in managing foreseeable risks to the continuity of their operations through a mature risk-based approach, and
- Critical infrastructure owners and operators are effective in managing unforeseen risks to their operations through an organisational resilience approach.

The four key outcomes of the strategy are:

This Handbook outlines the key functions and roles, at the Commonwealth level, to deliver these outcomes and ensure the resilience of Australia's critical infrastructure in the face of all hazards.

What is Critical Infrastructure Resilience?

Protection vs Resilience Approach

In 2009 the Australian Government adopted a resilience approach to critical infrastructure to encompass the broad range of potential threats and hazards that are faced. At a national level critical infrastructure protection is used to describe the actions or measures undertaken to mitigate against the specific threat of terrorism, and is an important component of critical infrastructure resilience.

Concept of Resilience

The Australian community, the economy and the delivery of government services are all dependent on robust and resilient infrastructure. At its basic level resilience is the capacity of a system to deal with change and continue to develop. The complexity and interconnectedness of Australia's critical infrastructure systems is increasing, due to the proliferation of new technologies and globalisation of markets and supply chains. This has introduced new uncertainty, vulnerabilities and risks, where disruptions may cascade through multiple systems and sectors in a manner that is difficult to predict or plan for. Traditional risk management approaches, that identify and treat *foreseen* risks are limited in this environment. Owners and operators of CI, together with Australian, state and territory governments need to be agile in the face of *unforeseen* risks.

This is where resilience comes in. Resilience is where the approach to the management of risk is at a point that a system (for example an industry sector, a network or an organisation) has an almost organic capacity to respond to, and even capitalise on, change whenever it occurs. Resilient systems adapt to changes in their environment to maintain core characteristics or functionality, no matter what the cause of that change. For this reason the Australian Government maintains an all-hazards approach to resilience; seeking to increase the capability of organisations and communities to survive, recover, and adapt to all types of threats.

This is why the CIR Strategy focuses on two key objectives—to ensure that owners and operators are equipped to effectively manage reasonably foreseeable risks to the continuity of their operations, as well as an ability to effectively manage unforeseen risks through an organisational resilience approach.

Trusted Information Sharing Network (TISN) for Critical Infrastructure

Purpose:
Provide a secure, non-competitive environment in which owners and operators of critical infrastructure and Australian, state and territory governments have the opportunity to share information and work together to strengthen the resilience of critical infrastructure in the face of all hazards.

"Delivery of the Strategy is dependent on a productive business-government partnership."

Role of the TISN

The Australian Government takes a non-regulatory approach to critical infrastructure resilience, favouring a productive business-government partnership. To this end the 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 for critical infrastructure. The TISN provides a secure environment in which critical infrastructure owners and operators meet regularly to share information and cooperate within and across sectors to address security and business continuity challenges.

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 treatment strategies. In many cases though, neither business nor government in isolation have access to all the information they need to understand and treat risks; nor the ability to influence their operating environments to the extent required to ensure the continuity of essential services. This is a shared responsibility between owners and operators of CI, state and territory Governments and the Australian Government.

The primary focus of the business-government partnership, therefore, is the creation of an environment in which all parties can openly and securely share information, develop trust and collectively build solutions to increase the resilience of CI.

Structure and Membership

The TISN is made up of:

- eight Sector Groups
- Expert Advisory Groups
- an Oil and Gas Security Forum, which is a sub-group of the Energy Sector Group, and
- Cross-Sectoral Interest Groups, which assist in the temporary exploration of cross-cutting issues.

TISN Sector Groups

Sector Groups enable critical infrastructure owners and operators from the same sector to share information on threats and vulnerabilities, and collaborate on appropriate measures to treat risk and increase resilience.

The eight Sector Groups cover:

- Banking and finance
- Communications
- Commonwealth government
- Energy
- Food and grocery
- Health
- Transport
- Water services

Each Sector Group is supported by an Australian Government agency – usually the agency that has portfolio responsibility for that sector.

Structure and Membership

The structure and membership varies between sectors due to the variety that exists in the organisational make-up, regulatory environments and market competiveness across sectors. Sector Groups, therefore, have their own Terms of Reference outlining specific conditions, which are developed by the Group and endorsed by CIAC.

Membership of TISN Sector Groups is based on the principle of establishing trust by ensuring there is a common, non-competitive interest in sharing information on security threats, vulnerabilities and organisational and sector resilience. The Sector Groups are comprised of representatives of the owners and operators of critical infrastructure, rather than product vendors, academics or consultants.

OVERVIEW OF THE BANKING AND FINANCE SECTOR

What does the sector do?

The sector provides financial services, including banking, insurance, securities, superannuation and wealth-building products. The banking and finance sector plays a fundamental role in driving productive investment in the economy and provides the infrastructure necessary for the exchange of goods, services and financial assets. Individuals, communities, businesses and governments are all reliant on this infrastructure to continue to operate and thrive.

What does the market look like?

Banking is dominated by the so-called 'Big Four' banks – ANZ, CBA, NAB and Westpac, which together represent more than 80% of the market. There are also a number of other smaller ('tier 2') institutions, the largest of which include Suncorp and Bendigo Adelaide banks.

Australia's insurance industry is dominated by a 'Big Five' which includes the Big Four banks, along with AMP. Australian insurers generally do not provide insurance directly, but instead repackage overseas products.

Australia's (compulsory) superannuation sector represents the world's fourth largest funds pool.

What does the sector depend on?

The sector has identified 17 essential business functions that are critical to its continued provision of services to the community. Of these, the most crucial depend on a handful of communications-based systems including the Reserve Bank's Real-time Information Transfer System (RITS), the Community of Interest Network (COIN), the ASX's AustraClear system, the SWIFT network, and Continuous Linked Settlement (CLS).

In most cases, these systems are dependent on access to electricity, water and in particular, communications – including international submarine cables.

What are the key risks/threats/vulnerabilities to the sector?

Because of the unique business-model of the banking industry, the most significant risks to the sector are market-based, with public confidence in the soundness of institutions integral to their ongoing viability.

The sector's critical infrastructure, which is largely shared, faces similar risks to those of the communications sector. Disruptions can occur through cyber-attack or computer-based human error. Some infrastructure is reliant on international connectivity, making it vulnerable to submarine cable outages.

Other risks include pandemic outbreak, which could impact upon the sector's workforce; and natural disasters, which may have a localised impact on banking services. The sector has also, in the past, been targeted by extreme left wing protest due to its status as a symbol of capitalism and its funding of projects which damage the environment.

Both Sydney and Melbourne contain banking precincts (Martin Place and Docklands respectively) which provide a degree of concentration risk should there be a terrorist attack or downstream critical infrastructure outage.

What controls are in place to contribute to sector resilience?

The sector is overseen by a number of organisations, including the Australian Prudential Regulation Authority, which holds significant legislative powers aimed at managing risks to the sector. Regulation is strong and effective, although the focus of regulators has traditionally been on market-based risks.

The sector has a good understanding of its risk environment and a sophisticated capacity to manage its risks. Redundancy arrangements exist for everything of importance – although some redundancy arrangements have the same downstream dependencies. Business continuity, risk, and crisis managers within the industry have strong informal networks and information is shared across organisations.

OVERVIEW OF THE COMMUNICATIONS SECTOR

What does the sector do?

The communications sector provides essential transmission systems and services to the nation through the telecommunications, broadcast, international submarine cable and postal sub-sectors. The broadcasting sub-sector is particularly important in providing forecasts and regular updates to the Australian public during natural disasters. The sector more broadly also provides essential inputs for other Australian CI sectors, such as banking and finance (i.e. real-time data and data transmission), and *all* CI sectors rely on the communications sector in some form. For example, the transport sector depends on the communication sector for positioning and navigation data services. The postal sub-sector also remains important to the Government sector for transferring classified and other sensitive information.

What does the market look like?

The telecommunications sub-sector is a key focus of the sector, providing telephony, satellite and internet services to the public. This sub-sector currently comprises 250 licensed carriers and 1500 carriage service providers but is dominated by the three largest carriers (Telstra, Optus and Vodafone Hutchison Australia), who account for over 90 per cent of revenue in the telecommunications market.

Submarine cables are also another critical sub-sector, accounting for a high percentage of Australia's international connectivity.

What does the sector depend on?

The increasingly virtual nature of the communications sector means that it depends on robust cabling infrastructure, as well as satellites and phone towers, for the continued provision of services. This infrastructure in turn relies on access to power, equipment providers and hence, transport. Disruption in the telecommunications environment is a routine occurrence for a range of reasons however redundancy is built into most of the sector to manage these events (albeit for a short period of time).

On the other hand, until automated transport truly advances in Australia, the postal sub-sector will continue to depend on humans to provide postal and courier services to the community.

What are the key risks/threats/vulnerabilities to the sector?

With this sector being very market-based, its critical infrastructure faces many similar risks to those of the banking and finance sector. Network disruptions can occur through cyber-attack, operational failures and human error, natural disasters and other external factors. In addition, some infrastructure is reliant on international connectivity, making it vulnerable to submarine cable outages. The result of these disruptions can threaten organisations' reputations and ultimately customer trust.

The communications sector is also vulnerable to foreign involvement risks. As Australia does not produce or supply many critical inputs to telecommunications infrastructure, involvement by foreign owned companies in this sub-sector is unavoidable – and in fact, outsourcing and off-shoring business functions have been a hallmark of the telecommunications sub-sector since the reforms of the 1990s. Foreign investment in the broadcasting sub-sector is also significant, where commercial broadcasters are largely foreign owned.

What controls are in place to contribute to sector resilience?

A number of Australian Government regulatory and non-regulatory mechanisms exist to manage risks in the communications sector. In particular, the Telecommunications Act establishes a detailed regulatory regime for telecommunications providers. Additionally, the telecommunications and communications systems are subject to lower monetary thresholds for screening by the Foreign Investment Review Board, meaning that most foreign investment in the sub-sector will be detected through this process.

The sector has a good understanding of its risk environment, and the need to share information within the sector on emerging threats. However, *sector wide* resilience may not be as high as it could be as it is largely privately owned and operated and consists of a large number of diverse businesses that vary in redundancy arrangements, resources and the ability to engage in the sector as a whole.

OVERVIEW OF THE COMMONWEALTH GOVERNMENT SECTOR

What does the sector do?

The sector covers a wide variety of government activity and comprises Commonwealth owners and operators of critical infrastructure (CI) supporting the delivery of essential services to the nation, including but not limited to, legislation and policy; defence and border control (including visa provisions); medical and community health (including nuclear science and technology); welfare and benefits payments to individuals; international trade and consular assistance; and taxation to name a few.

What does the sector look like?

Unlike the other sector groups the Commonwealth Government sector is diverse covering a large range of agencies delivering a wide variety of essential services. These can be grouped into the following streams:

- Policy coordination and advice, governance
- Defence, national security, intelligence
- Criminal justice, law enforcement and border protection
- Human, health and social services
- International relations
- Industry engagement, oversight and regulation
- Research and trade

These are each broadly defined capabilities supported and delivered by multiple agencies.

What does the sector depend on?

The sector is currently undertaking an assessment of its essential business functions an on agency basis. This work, while ongoing, has already identified the criticality of information technology and communications-based systems for each agency. In most cases, these systems are dependent on access to electricity, water and in particular, communications – including the Intra Government Communications Network (ICON) as well as satellite based services.

For many agencies ICT will be their key infrastructure investment. It is worth noting however that there will be some services (i.e. defence, national security and border protection) that are marked by a distinct and heavy investment in capital infrastructure (i.e. aircraft, ocean vessels, port and air-base assets).

It is important to note that government agencies are more often reliant on commercially owned infrastructure rather than being owners/operators in their own right.

What are the key risks/threats/vulnerabilities to the sector?

There are multiple business-models involved in all of the different streams of government activity identified above. At this stage, the most significant risks common to the various streams comprising the government sector are related to the continuity of ICT capabilities and how this impacts on public confidence in the reliability of government services and trust in its institutions.

Much of the sector's critical infrastructure, which is largely based in ICT capability, faces similar risks to those of the communications sector. Disruptions can occur through cyber-attack or computer-based human error. Some infrastructure is reliant on international connectivity, making it vulnerable to satellite service or submarine cable outages.

What controls are in place to contribute to sector resilience?

The government sector operates under the *Public Governance, Performance and Accountability Act 2013* which links to standards set out in the *Protective Security Policy Framework* and the *Information Security Manual* aimed at managing protective and information security risks to the individual agencies. In broader terms the national *Critical Infrastructure Resilience Strategy* applies to government agencies but this is a non-regulatory approach which prioritises business –government partnership, coordination and information sharing.

The sector has a good understanding of its risk environment and a sophisticated capacity to manage its risks. Redundancy arrangements exist—although some redundancy arrangements have the same downstream dependencies (i.e. ICT, energy, water). Business continuity, risk, and crisis managers within the government sector have strong coordination and information sharing networks.

OVERVIEW OF THE ENERGY SECTOR

What does the sector do?

The energy sector sustains the society and the economy through the generation, transmission and distribution of electricity; production and delivery of natural gas and liquid fuels. Other CI sectors are dependent on the sector for energy. The energy sector is a key enabler for all elements of society.

What does the market look like?

The sector is made up of three sub-sectors – electricity, natural gas and liquid fuels – these are detailed below. A sub-group of the energy sector group is the Oil and Gas Security Forum.

Electricity

Electricity generation (including renewables) is the process of generating electric power from other sources of primary energy. Australia's electricity generation sector is undergoing transformative change from its historic reliance on coal and, to a lesser extent hydroelectricity, to a more diverse mix using coal, gas and renewable energy sources.

Electricity transmission networks allow the bulk transport of electricity at high voltages from a range of generators to major demand centres. The transmission network consists of towers and the wires that run between them, underground cables, transformers, switching equipment, reactive power devices, and monitoring and telecommunications equipment.

Electricity distribution networks transport electricity from transmission networks to end-use customers. The high voltage electricity that is used for transmission from the generator is converted into lower voltages by substation transformers. It is then carried in wires over poles - or in densely populated areas, in wires buried underground - to businesses and homes.

The production of electricity underpins Australia's society and economy.

Natural Gas

Natural gas produced for domestic consumption is transported (or 'shipped') by high pressure **transmission pipelines** from the production facility to the entry point of the distribution network (known as the city gate) or to large users that are connected to the transmission pipeline. Pipeline operators sell transport services, limited by their pipeline capacity, to gas 'shippers'. Many large gas buyers act as their own shipper. Gas storage facilities can inject gas into the transmission system at short notice to manage peak demand or emergencies. They are typically owned by energy retailers.

Gas distribution networks transport natural gas from transmission pipelines to end users. They typically consist of a backbone of high and medium pressure pipelines running between the 'city gate' (the point of connection to the transmission pipeline) and major demand centres. This network feeds low pressure pipelines, which deliver the gas to businesses and homes.

Energy retailers are the distribution networks' main customers. They buy natural gas in large volumes and on-sell it to consumers. Retailers arrange with gas distribution network operators for the supply of gas to end users via the distribution network.

Liquid Fuels

Australia has been a petroleum producer for many decades. Our liquid fuels markets have always been linked to the global market through the open movement of crude oil and petroleum products. The supply chain, which delivers petroleum products to customers, is a dynamic, complex, and global web of interlinking facilities and operations that has developed over decades.

Australia consumes around 55,000 megalitres (ML) of liquid fuels per year. This product demand is met by a mix of domestically refined crude oil and other feedstock and finished product imports.

The number of oil refineries in Australia has declined from seven to four in recent years as the result of competitive pressures from larger scale refineries in the Asia Pacific region which have lower unit costs of production. The closure of refineries, combined with increasing demand for petroleum products, is resulting in increasing reliance on imported product to satisfy growth in market demand, although there are widely different growth profiles between fuel types.

The market is a mix of large and small enterprises as well as government.

What are the key risks/threats/vulnerabilities to the sector?

Societal, environmental and technology changes are forcing transformative change in the energy sector. These changes are creating new uncertainty and risks. Cyber threats pose ongoing and new risks, particularly for the operation of electricity networks and the shift to remote monitoring and operation.

Physical terrorism, while a threat to the sector, is of low risk as the global trend in terrorism is toward low capability attacks aimed at people and symbolic targets, not infrastructure. See BLU 047/2014 of 23 September 2014, *Australia's electricity systems sector*.

From a TISN perspective the major vulnerability for resilience is a poor understanding of cross-sector dependencies low organisational resilience and adaptability and financial pressures.

What controls are in place to contribute to sector resilience?

There is a strong regulatory environment for the energy sector. The Office of Energy Security in the Department of Industry, Innovation and Science is responsible for policy development and implementation of energy security matters. Other organisations with key responsibilities for oversight, regulation and operation of the sector include:

- The COAG Energy Council
- The Australian Energy Market Commission
- The Australian Energy Market Operator
- The Australian Energy Regulator

What does the sector depend on?

The sector is highly dependent on water and communications to maintain services. Prolonged outages in these sectors would have significant impacts on the ability for the energy sector to continue to operate.

OVERVIEW OF THE FOOD AND GROCERY SECTOR

What does the sector do?

The Australian food and grocery sector sustains the society by ensuring people have access to food. It encompasses food for consumption in and outside of the home. The sector relies heavily on supply chains including physical and information systems, and processes used to deliver a product or service from one location to another – mostly supplier to consumer. For some food items, there is importation of fresh products and ingredients, as well as packaging, but for others, the supply is wholly domestic.

What does the market look like?

The Australian food and grocery sector incorporates a diverse range of production areas, processors, manufacturers and retailers – many thousands of participants ranging from highly sophisticated international companies to local sole traders as well as more than 20 million consumers. The bigger retailers like Woolworths (Woolworths Ltd) and Coles (Wesfarmers) dominate the retail component of the market, with secondary competition from IGA (Metcash) and Aldi.

A broad overview of the food and grocery sector market:

> Food production → Food processing and/or packaging → food distribution → grocery retailers and/or food outlets → food consumers

What does the sector depend on?

Like any physical supply chain, food supply depends on a range of infrastructure for continuity of production, processing, distribution and retail—power, water, financial services, communications and transport. This infrastructure allows manufacturers to undertake energy-intensive processing, supports retailers to store chilled food and process transactions, and transport to take products from place to place.

What are the key risks/threats/vulnerabilities to the sector?

The complexity of distribution systems has grown – the information needed to manage food distribution has become more sophisticated and requires complex systems and record keeping. This has increased the vulnerability to the sector for cyber-attack, computer viruses and industrial espionage by cyber means and other types of system breakdowns.

The Australian food supply chain is also vulnerable to large-scale events such as human or animal pandemic, national fuel shortage and combinations of events that affect multiple links of the food supply chain at the same time – like a widespread electricity outage combined with floods or fires. Concurrent loss of a number of transport links to and between major areas is also a key vulnerability.

What controls are in place to contribute to sector resilience?

The overarching competitive environment of the food and grocery sector promotes the building of resilience at an organisational level whereas the competitive regulatory framework makes it difficult to measure resilience at a sector level.

The sector is mainly privately owned and operated and consists of a large number of diverse individual business that vary in sophistication, resources and the ability to engage in the sector as a whole, meaning *sector wide* resilience is

low. Leading food companies recognise that a resilient supply chain can be a competitive advantage - by allowing them to cohesively react to adverse events faster than their competition to take market share and outperform.

OVERVIEW OF THE HEALTH SECTOR

What does the sector do?

Australia's health system is a multifaceted network of public and private providers, settings, participants and supporting mechanisms that maintains the health and wellbeing of the Australian community.

Services provided include private hospitals, general practitioner services, insurance, medicines, blood products, ambulance and medical goods supply. Other sectors are reliant on this sector for the health and wellbeing of employees and the community.

What does the market look like?

The Australian health system involves multiple layers of responsibility and funding provided by governments, individuals, health providers and private health insurers. The sector broadly comprises three sub-sectors: health services, health products, and health protection. These sub-sectors are interconnected and each is critical to supporting the whole health system.

Health services

Health care in Australia is provided through a range of acute, primary, secondary and aged care services and involves supporting infrastructure such as public and private hospitals, private practices, residential facilities, laboratories and pharmacies. The provision of health service is critical to ensure that Australian's receive appropriate and timely healthcare.

The private health services network ranges from small individual practices to larger multination companies. The private hospital network is owned by a range of companies and not-for-profit providers.

Health products

A wide array of health products and equipment, including vaccinations, pharmaceuticals, blood products and medical devices (such as specialised diagnostic and treatment equipment) support the provision of health care in Australia.

The majority of health products rely on global supply chains, as domestic manufacturing is mostly in packaging and distribution.

Health protection

Health protection is critical for Australia to be able to prevent, prepare and respond to emergencies such as natural disasters, disease outbreaks and mass casualty events, including chemical, biological, radiological and nuclear (CBRN) events.

The Government plays a key role in health protection and manages enabling groups, items and facilities to maintain Australia's emergency response capability. The Government works with state and territory governments and relevant experts to respond to health issues of national significance.

What does the sector depend on?

The health sector provides a vast array of goods and services and is geographically diverse. The sector is dependent on access to electricity, water and transport (for the delivery of medicines and medical equipment from suppliers

around the world). The sector is also reliant on global supply chains for the majority of medical products and the infrastructure that supports this.

What are the key risks/threats/vulnerabilities to the sector?

The primary risk to the sector is a major health emergency, such as a pandemic outbreak of a disease with high mortality rate, which would overwhelm the sector's ability to respond.

The sector is highly reliant on a large number of global supply chains for things like medicines and medical equipment. While none of these would jeopardise the operation of the entire sector, there are a number of products with only one supplier whose loss could result in a large number of deaths or serious illness.

Individual health care sites, such as GP clinics and hospitals are reliant on energy, communications and water. While a disruption to these services on a local level would not impact the entire sector it could still have significant consequences.

From a TISN perspective, the membership is dominated by industry associations rather than practitioners and the industry membership is incredibly diverse.

What controls are in place to contribute to sector resilience?

The health services and products sub-sectors are regulated to ensure continuity of supply and patient safety, including through state and territory licensing of private hospitals, health professionals and pharmacies and Commonwealth regulation of the safety and availability of health products and the private health insurance industry. There is also strong government ownership, control and regulation of the health protection sub-sector.

Redundancy arrangements exist for much of the infrastructure in the sector, such as hospitals but there are a number of key medicines for which there is no redundancy.

OVERVIEW OF THE TRANSPORT SECTOR

What does the sector do?

The transport sector sustains the society and the economy through the movement of people and essential goods. Other CI sectors are dependent on the sector for the importation and movement of their essential products. The transport sector is also a key enabler of growth in mining, agriculture and tourism.

What does the market look like?

The movement of people and essential goods is provided through three sub-sectors —aviation, maritime and surface—which are detailed below. These sub-sectors are managed by a mix of large and small enterprises, as well as government.

Aviation

The aviation sector facilitates both travel and trade and connects Australia's cities and towns with each other and internationally. As our population centres are dispersed over a large geographical area there are limited alternatives for convenient/fast travel. Regional and remote communities also rely heavily on its infrastructure as it facilitates access to health care, education, legal and financial services. It is also a big driver of economic growth for regional businesses as it connects them to domestic and international markets.

Maritime Sector

The maritime sector supplies a major mode of transport for food, oil & gas, medical supplies and many other essential commodities, including building and construction materials required for the provision of other critical infrastructure sectors. Included in this sector are all major ports in Australia, their processes, supply chains and the systems and operations that allow the ports to operate. There is an extensive network of commercial ports ranging from resource export terminals to multi-cargo ports. Some are also key import hubs servicing communities and industries. As an island nation, Australia has a heavy reliance on maritime infrastructure and there are limited alternatives. It is critical for the export of agriculture and mineral commodities and for the import of household goods, manufacturing products, vehicles, machinery and fuel.

Surface

Roads and rail form the land transport network in Australia and it is made up of a complex series of nodes and links. Both provide essential transport services for passengers and freight within cities and between areas of economic production and consumption.

What are the key risks/threats/vulnerabilities to the sector?

Terrorism is still a key threat to the sector, with terrorist attacks typically being directed against publicly accessible areas of transport systems as they confine large numbers of people within an area at predictable times. This is likely to remain an attractive target.

Technology changes and the way that transport is coordinated are also bringing new risks to the sector. Cyber security is posing new risks, particularly for the operation of ports and supply chains.

From a resilience perspective the sector is generally collaborative and responds well to incidents and supports resilience development. The major vulnerability for resilience is a poor understanding of cross-sector dependencies.

What controls are in place to contribute to sector resilience?

There is a strong regulatory environment for the transport sector, specifically for aviation and maritime. The Office of Transport Security in the Department of Infrastructure and Regional Development monitors and maintains policies, procedures, guidelines and regulations to ensure the safe transport of people and products.

What does the sector depend on?

The sector is highly dependent on energy and communications to maintain services. Prolonged outages in these sectors would have significant impacts on the ability for the transport sector to continue to facilitate the movement of people and essential products (particularly health products and fuel).

OVERVIEW OF THE WATER SERVICES SECTOR

What does the sector do?

The sector provides safe drinking and raw water, and the collection and treatment of waste water and storm water. The collection and distribution of water for a variety of uses contributes to our economic, social and environmental wellbeing, while supporting a healthy population. Other sectors are reliant on the water sector for the safe operation of their buildings and equipment and the health of employees. The Energy Sector is also reliant on the water sector for the production of energy.

What does the market look like?

The vast majority of Australians are served by a limited number of major water companies to the standards specified in the Australian Drinking Water Guidelines. The balance of the population is serviced by other operators, which may include local councils or smaller water companies.

Each state and territory has its own water industry approach to water management. For example, while one water company manages most of Western Australia, many local council-based water companies operate in Queensland.

Due to the size of Australia and the remoteness of many communities, a number of different types of water supply systems have been constructed, with a range of source waters.

The east coast uses dams and reservoirs to capture source water. The drier central and western parts of Australia have strategies for ground water extraction. Many States have developed desalination plants to supplement existing water supply schemes.

Australian water organisations generally fall into one or more of the following categories:

- catchment management authority
- rural water authority (irrigation)
- regional urban authority
- wholesaler (bulk water distribution)
- retail water company.

What does the sector depend on?

The sector has identified 4 essential business functions that are critical to its continued provision of services to the community. In most cases, these functions are dependent on access to: power and fuel, chemicals, telecommunications, monitoring systems and access to laboratories for water quality testing and other services.

What are the key risks/threats/vulnerabilities to the sector?

The most significant risks to the sector are natural disasters, contamination events or human action (either error or deliberate).

Other risks include pandemic outbreak, which could impact upon the sector's workforce; and communications outages which may have a localised impact on infrastructure, such as water storages and water treatment plants. The sector has also, in the past, been targeted by protest due to the symbology of its major infrastructure (water towers and dams).

What controls are in place to contribute to sector resilience?

The sector has no national oversight but is overseen by one or more regulatory agencies at the state and territory level. Regulation is strong and effective, although the focus of regulators has traditionally been on ensuring a high level of water quality and minimising environmental impacts of water sector activities.

The sector has a good understanding of its risk environment and a sophisticated capacity to manage its risks, such as the Australian Water Sector Mutual Aid Guidelines. Due to the linear nature of much of the sectors assets redundancy arrangements may not exist for everything of importance. Business continuity, risk, and crisis managers within the industry have strong informal and formal networks and information is shared across organisations.

Cross Sector Interest Groups

Space

Purpose:
The Space CSIG will provide input, advice, support and guidance to the TISN on current, emerging and future (medium to long term) issues and trends relating to the operation, integration and use of space-based systems, technologies and information by Australian critical infrastructure.

Role of the Space CSIG

The Space CSIG forms part of the TISN.

The Space CSIG supports the CIR Strategy key outcomes through research and the development of concepts, tools and other initiatives, consistent with its work plan, to assist the owners and operators of critical infrastructure to enhance their resilience.

The Space CSIG will develop and implement a forward work plan that is consistent with the key activities of the CIR Strategy. The work plan will be developed in consultation with Australian Government agencies and sector and expert advisory groups of the TISN.

The Space CSIG may develop recommendations for CIAC's consideration of mechanisms to enhance the ongoing provision of space expertise to the owners and operators of Australia's critical infrastructure.

Membership and structure

The Space CSIG will comprise space experts drawn from academia, industry, peak bodies; relevant TISN sector group representatives; and government representatives. Members will be selected for their individual expertise rather than as representatives of their organisations. Ideally, TISN sector group representatives will have expert knowledge of their own sector as well as how their sector utilises space assets and information.

The Space CSIG will report directly to the CIAC, which may provide direction for its operations or refer specific issues for its consideration. The Space CSIG strategy and annual work plan will be developed for noting and discussion by CIAC, as appropriate.

Infrastructure Information in the Public Domain

Purpose:
The Information in the Public Domain Cross Sector Interest Group has been formed to develop; a better understanding of what is 'sensitive information', determine how best to provide guidance and resources, identify existing obligations that may require the publication of potentially sensitive information, implement support mechanisms to help organisations identify stakeholders and effectively consult and to engage with and promote these activities through TISN.

Role of IIPD CSIG

The IIPD CSIG forms part of the TISN. Following an initial review of the *Infrastructure Information in the Public Domain guidelines 2006*, it was determined a number of broader issues needed appropriate consideration.

The IIPD CSIG has been formed to:

- develop a better understanding of what is 'sensitive information' in the contemporary environment
- determine how best to provide guidance for government, business, regulatory bodies and other organisations to assist in determining what is 'sensitive information'
- identify the accessibility and appropriateness of available resources that currently provide users guidance on 'sensitive information'
- identify existing government, regulatory and industry obligations, that may require the publication of potentially sensitive information
- determine how best to support organisations to better determine stakeholders and consultation mechanisms when considering the publication of data
- if necessary, develop updated or new guidance material and supporting resources, and
- engage with the TISN and other interested parties to promote and support the use of any new guidance and supporting resources.

Membership and structure

The IIPD CSIG may comprise representatives from TISN sector groups, academic specialists, representatives from peak bodies and associations, representatives of relevant government agencies, and consultants who are selected for their individual subject matter expertise or interest rather than as representatives of their organisations.

The IIPD CSIG will report directly to the CIAC, which may provide direction for its operations or refer specific issues for its consideration. The IIPD CSIG principles and work plan will be developed for noting and discussion by CIAC, as appropriate.

Expert Advisory Groups

Resilience Expert Advisory Group

Purpose:
To provide input, especially strategic thinking and the practical dimension into the development of the concept of organisational resilience. This includes guidance and advice on tools and other initiatives to assist the owners and operators of critical infrastructure to adopt a resilience approach. The REAG will also provide support and guidance to the TISN on emerging and future (medium to long term) resilience trends and issues.

Role of REAG

The Resilience Expert Advisory Group (REAG) forms part of the TISN and has been formed to facilitate the consideration of issues in relation to critical infrastructure resilience. The discussions may include (but are not limited to) the following:

- Assisting the owners and operators of critical infrastructure to adopt an organisational resilience approach to their business
- Providing input and advice on the development of tools, guidance material, education and outreach programs and other initiatives to assist owners and operators of critical infrastructure to adopt and maintain a resilience approach
- Developing case studies on organisational resilience
- Providing input and advice on the development of initiatives to build capacity in organisations for resilience, including for incident preparedness
- Identifying emerging resilience-related policy issues

Membership and Structure

REAG includes selected members from academia, business, peak bodies, and government representatives that participate in their capacity as experts rather than as representatives of their organisations. Where the work plan requires specific skills or strategic alignment, the REAG can adjust their membership to harness the necessary expertise. New members are selected by incumbent REAG members through an expression of interest process. REAG members vote on suitable candidates and CIAC endorses the selections.

The REAG reports directly to the CIAC, which may provide directions for its operations or refer specific issues for its consideration. The REAG's work plan will be developed in consultation with Australian Government agencies and sector and expert advisory groups of the TISN. The REAG will seek CIAC endorsement of its work plan.

For further information, refer to the *Resilience Expert Advisory Group (REAG).*

Governance and Key Roles

Critical Infrastructure Resilience Section (AGD)

Purpose:
Contribute to a secure and prosperous nation through the continued operation of critical infrastructure in the face of all hazards.

This will be realised through strong collaboration with critical infrastructure owners and operators, governments, communities and international partners to deliver resilience building initiatives and provide the highest quality advice to government and industry.

Role of the Critical Infrastructure Resilience Section

The Critical Infrastructure Resilience Section in the Attorney-General's Department (AGD) is the lead for critical infrastructure resilience policy for the Australian Government. This includes driving the policy agenda for the TISN and providing policy advice to government on critical infrastructure resilience issues. The primary document that drives the work of the section is the Critical Infrastructure Resilience (CIR) Strategy. This document is updated every five years to reflect the changing environment. The Strategy consists of a Policy Statement that outlines the Government's high-level policy approach to critical infrastructure resilience and a Plan that outlines the activities to be undertaken to implement the policy. Through the implementation and ongoing review of the strategy the section works towards its core objective to ensure the continued operation of critical infrastructure in the face of all hazards.

Functions to support the delivery of the Strategy include:

- Driving the policy agenda of:
  - The Critical Infrastructure Advisory Council (CIAC)
  - The Industry Consultation on National Security (ICONS)
- Provide strategic oversight for the implementation of the strategy and the work of the TISN
- TISN Secretariat for:
  - The Banking and Finance Sector Group (BFSG)
  - Water Services Sector Group (WSSG)
  - Commonwealth Government Sector Group (CGSG)
  - The Resilience Expert Advisory Group (REAG)
- TISN Desk Officer for:
  - Energy Sector Group
  - Communications Sector Group
  - Transport Sector Group
  - Food and Grocery Sector Group
  - Health Sector Group
- Facilitate an increased understanding and awareness of strategic issues and trends and their impact on the operating environment through the CIR Forum and cross-sectoral activities.

Critical Infrastructure Advisory Council

Purpose:
Provide leadership and strategic guidance for the TISN and advise the Attorney-General on matters of critical infrastructure resilience. This includes overseeing the implementation of the Critical Infrastructure Resilience Strategy and Plan and monitoring the work of the Sector Groups, Expert Advisory Groups and Cross-Sectoral Interest Groups within the TISN.

Role of the Critical Infrastructure Advisory Council

The Critical Infrastructure Advisory Council (CIAC) is a joint government and industry advisory body that provides strategic direction and priorities for the Trusted Information Sharing Network (TISN). To drive the implementation of the Critical Infrastructure Resilience Strategy and Plan, CIAC oversees the work of each of the seven sector groups (banking and finance, communications, energy, food, health, transport and water services). It also advises the Attorney-General on critical infrastructure resilience.

The functions of the CIAC include[1]:

- Assist the Australian Government with the implementation of the Critical Infrastructure Resilience Strategy
- Provide strategic oversight and direction to the TISN Sector Groups, Expert Advisory Groups and Cross-sectoral Interest Groups
- Undertake activities to achieve an enhanced understanding of cross-sectoral dependencies between TISN Sector Groups
- Maintain good governance of the TISN, including overseeing the work of the Sector Groups, Expert Advisory Groups and Cross-sectoral Interest Groups
- With the agreement of the Attorney-General's Department, create new groups and communities as appropriate
- As appropriate, refer matters that require a multi-jurisdictional approach or are the responsibility of other bodies (such as the Australia-New Zealand Counter-Terrorism Committee (ANZCTC), Australia-New Zealand Emergency Management Committee (ANZEMC) or other Ministerial Councils) to the appropriate body,
- As appropriate, advise the Attorney-General on matters of critical infrastructure resilience.

Structure and membership

CIAC is chaired by the Attorney-General's Department (either Deputy Secretary or First Assistant Secretary depending on availability). Its membership consists of the chairs of each TISN sector group, senior Australian Government representatives from relevant agencies, and senior State and Territory government representatives.

[1] Critical Infrastructure Advisory Council Terms of Reference

TISN Sector Chair

Purpose:
Champion critical infrastructure resilience initiatives and represent the interests of owners and operators of critical infrastructure to government.

Role of the TISN Sector Chair

The operation of TISN Sector Groups is reliant on a strong partnership between industry and government representatives. For that reason the Chair is drawn from the sector, usually through an election process, and the TISN Secretariat function is provided by a government department. The TISN Sector Chair provides their expertise and knowledge of the sector to help drive the priorities for TISN Sector Group and build the resilience of Australia's critical infrastructure.

The TISN Sector Chair needs to:

- chair meetings of Sector Group
- build a strong partnership with the TISN Secretariat
- set the policy agenda for the sector, in partnership with the TISN Secretariat
- develop and drive the work plan for the sector, in partnership with the TISN Secretariat
- act as the primary conduit of information between the TISN Sector Group and government
- represent the TISN Sector Group at the Critical Infrastructure Advisory Council meetings and provide update reports on the work of the sector
- as a member of CIAC, assist in driving the strategic direction of the TISN through setting objectives and priorities and advising the Attorney-General on matters of critical infrastructure resilience, and
- create cross-sectoral linkages and drive cross-sectoral activities in partnership with the TISN Secretariat.

TISN Secretariat

Purpose:
Build and sustain a strong business-government partnership with the sector and drive resilience building initiatives to achieve the outcomes of the CIR Strategy and Plan.

"A strong and effective business-government partnership ensures arrangements are in place for information sharing and collaboration on risk and resilience initiatives".

Role of the Secretariat

Sector Groups and Expert Advisory Groups are each supported by a secretariat, which provides policy guidance and administrative assistance to build a strong business-government partnership in the sector. The TISN Secretariat is the front of house for government engagement with industry through the TISN. The TISN Secretariat should build a detailed knowledge of the sector and work closely with CI owners and operators to gain a shared understanding of the security and business continuity issues within the sector. With this information the Secretariat will proactively work with the sector to improve the overall resilience of the critical infrastructure that underpins the provision of essential services to the Australian community.

To achieve this outcome the TISN Secretariat needs to:

- build a strong partnership with the TISN Sector Chair
- build strong relationships with stakeholders in industry and Australian, state and territory government agencies
- work with industry and relevant government agencies to build the resilience of the relevant sector
- understand the security and resilience issues facing the sector, including through working with relevant national security agencies,
- develop a basic level understanding of resilience fundamentals
- drive the policy agenda of the sector, in partnership with the TISN Sector Chair
- lead and/or contribute to a range of resilience building initiatives, including the development of high-quality reports, guidelines and standards; and the conduct of exercises and workshops
- ensure the Sector Group is professionally administered and membership effectively managed
- collaborate with other TISN Secretariats to pursue best practice and understand cross-sectoral dependencies
- provide specialist portfolio policy advice on critical infrastructure, and
- facilitate the sharing of information, including threat and risk information, within and across sectors, in consultation with security agencies, industry and other government departments.

Government Departments with this role:

Attorney-General's Department – Banking and Finance Sector Group, Water Services Sector Group, Commonwealth Government Sector Group

Department of Health – Health Sector Group

Department of Agriculture and Water Resources – Food and Grocery Sector Group

Department of Industry, Innovation and Science – Energy Sector Group

Department of Infrastructure and Regional Development – Transport Sector Group

Department of Communications and the Arts – Communication Sector Group

TISN Desk Officer

Purpose:
Provide support and advice to the TISN Secretariat to ensure that they are equipped with the information and resources required for their sector to effectively achieve the outcomes of the CIR Strategy and Plan.

Role of the TISN Desk Officer:

As lead agency for the Critical Infrastructure Resilience Strategy, AGD has an understanding of, and access to, information across the TISN. Through its desk officers, AGD is able to bring a cross sectoral understanding to discussion and connect sector groups to resources across the TISN (information and people) that may assist in achieving the outcomes of the CIR Strategy.

The desk officer brings knowledge of broader CI activities being undertaken across government and the TISN, provides visibility of issues being progressed in other forums, forges cross-sectoral connections, and ensures broad policy consistency across sectoral activities.

To achieve this outcome the TISN Desk Officer needs to:

- build strong relationships with members of the TISN Secretariat and TISN Sector Group
- understand the security and resilience issues facing the sector
- provide advice to the TISN Secretariat and TISN Sector Group on the CIR Strategy and Plan
- monitor policy developments and ensure consistency in policy application and delivery of messages across the TISN
- assist with the development of the sector work plan to ensure it meets the objectives of the CIR Strategy and Plan
- share cross-sectoral issues (including vulnerabilities and opportunities) with other desk officers
- participate in regular sector meetings as the AGD representative and update members on AGD projects and the work being undertaken by other sectors
- coordinate and engage with other TISN Secretariats and TISN Sector Groups on a regular basis to understand linkages and opportunities
- monitor the health of the TISN Sector Group and brief executive as required
- monitor media and intelligence (horizon scanning/issues management) to be better across sector group issues, vulnerabilities and opportunities.

From: Andrew KILEY
To: bfsg s. @communications.gov.au; Esg Secretariat; OGSF Secretariat; s. 47E(d) @awe.gov.au; s. 47E(d) ; s. @industry.gov.au; s. 47E(d) ; wssg; s. 47F(1) ; s. 47F(1) ; s. 47F(1) ; s. 47F(1) ; s. 47F(1) ; s. 47F(1) ; s. 47F(1) ; s. 47F(1) ; s. 47F(1) ; s. 22(1)(a)(ii) @awe.gov.au
Cc: s. 22(1)(a)(ii) ; s. 22(1)(a)(ii) @communications.gov.au; s. 22(1)(a)(ii) @environment.gov.au; s. 22(1)(a)(ii) @environment.gov.au; Leanne LOAN; s. 22(1)(a)(ii) @health.gov.au; s. 22(1)(a)(ii) @awe.gov.au; s. 22(1)(a)(ii) @space.gov.au; s. 47E(d) s. 22(1)(a)(ii) CI Centre; s. 22(1)(a)(ii)
Subject: TISN and Resilience Strategy update [DLM=For-Official-Use-Only]
Date: Wednesday, 19 February 2020 2:48:26 PM

For-Official-Use-Only

To TISN colleagues,

Happy new year to all. I hope you and your families were able to have an enjoyable, and most importantly safe, break.

I would like to provide you with an update on the progress of the critical infrastructure resilience strategy review. As you are aware, last year we commenced a review of the critical infrastructure resilience strategy for release in 2020. In conjunction with the strategy review, the Trusted Information Sharing Network (TISN) structure and functions are also being reviewed to ensure we have the most effective engagement mechanisms underpinning our work. We greatly appreciate the engagement of all members of the TISN to date and the insights that have been shared. Your feedback has been collated and is being used to shape the next draft of the strategy and how we engage across the CI community.

We had been hoping to come back out to the TISN early this year, however a number of recent and ongoing events are impacting this timeline. This includes our need to consider the summer's bushfires, the proposed Bushfire Royal Commission, the COVID-19 outbreak and Government's recent consultation on the 2020 Cyber Security Strategy.

We hope to soon be able to provide you with greater certainty on upcoming strategy consultations and an updated timeline for the strategy review. In the meantime, we look forward to working with all sectors in the coming months to work through the impacts of COVID-19 and the bushfires on your sectors, particularly in relation to how you engage with or rely on other sectors or parts of the economy (e.g. supply chains). We are hopeful that the lessons from these events will ultimately result in a strengthened strategy and more effective TISN.

Thanks again for your ongoing support of this project. Please feel free to contact me if you have any questions.

Thanks,

Andrew

Andrew Kiley
Assistant Secretary | Assurance, Risk and Engagement Branch

Critical Infrastructure Security Division
Department of Home Affairs
P: 02 s. 22(1)(a)(ii) | M: s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @homeaffairs.gov.au

For-Official-Use-Only

Using a Theme to Focus TISN Activities
12 Month Cycle

1
- CIAC meeting 1 (e.g. November meeting)
  - Members agree on theme for next 12 months.

2
- TISN sector groups focus activities on theme
- Commonwealth to run introductory events early in the year, based on the theme, to inform specific sector group activities
- States/territories to consider how they could incoporate theme into their work program

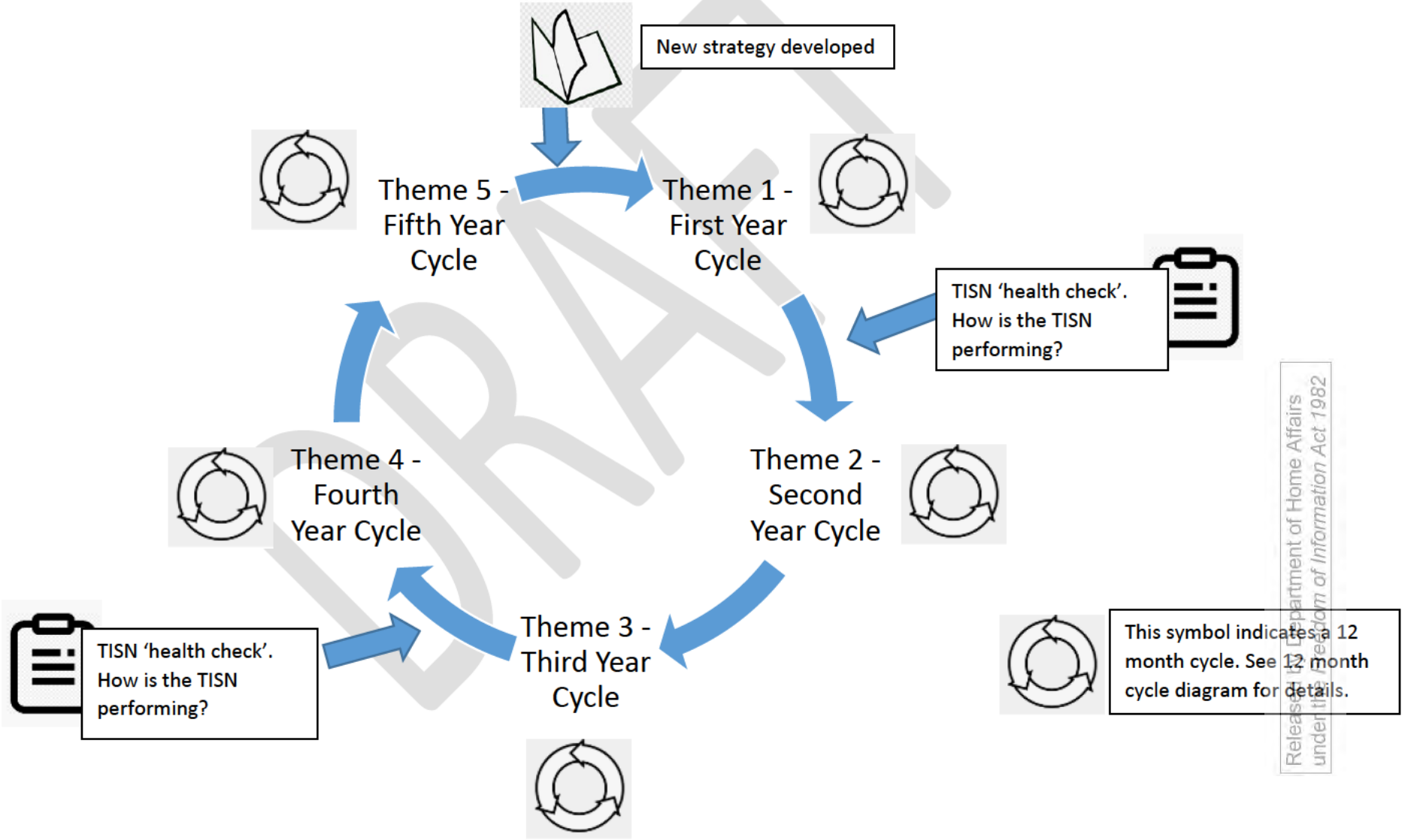
3
- Further events occur throughout the year, based on the themed work program
  - Includes specific Commonwealth-held events as well as information sharing on state/territory and industry events
- Use of GovTEAMS for information sharing on events and reports relevant to the theme

4
- CIAC meeting 2 (e.g. June meeting)
  - Sectors and jurisdictions present on progress towards objectives
  - Feedback on events and types of information provided received

5
- Continuing events and activities, including tailoring based on feedback from CIAC meeting 2

6
- CIAC meeting 3 (e.g. November meeting)
  - Sectors and jurisdictions report on previous years' activities
  - New theme for next 12 month cycle agreed
- Reports from jurisdictions and sectors incorporated into a document by the CIC for presentation to the Minister

Using a Theme to Focus TISN Activities
5 Year Cycle



Roles and Responsibilities

Group	Roles and responsibilities
CIAC	• Decide on theme for 12 month cycle • Provide leadership on the continuing role of the TISN (e.g. through TISN review and strategy development) • Discuss effectiveness of using theme to focus TISN activities • Oversee and drive the TISN and attend TISN events • Support to Commonwealth in policy development, as necessary
Sector groups	• Create work plan based on theme • Produce annual sector report outlining work undertaken for the past 12 months (particularly in relation to the annual theme), for submission to CIAC • Meet to discuss issues specific to group • Organise and attend TISN events
Commonwealth	• Organise TISN events based on theme • Develop policy in consultation with TISN, as appropriate (E.g. TISN refresh, strategy update) • Provide linkages for industry to approach specific parts of government (e.g. cyber) • Use jurisdictional and sector CIAC updates to produce a yearly report to be presented to Cth and S/T ministers
States and territories	• Attend CIAC • Produce jurisdictional report outlining work undertaken for the past 12 months, for submission to CIAC • Attend TISN events • Involvement in sector groups as appropriate • Support greater cross-jurisdictional engagement and information sharing

Option 1 – Full Home Affairs Representation, Full REAG Representation, All states and territories

	ACT		NSW		WA		SA		NT		QLD		VIC		TAS		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps																	
SES/EL2																	
To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	1200	250	900	250	1200	300	350	250	500	250	1000	250	
Assistant Director																	
To maintain visibility of discussions and provide back up for the rewrite.			300	188	1000	156	700	143	900	220	250	148	500	164	900	147	
Project Lead																	
The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	1000	156	700	143	900	220	250	148	500	164	900	147	
Logistical lead																	
To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence.			300	188	1000	156	700	143	900	220	250	148	500	164	900	147	
Estimated Travel costs for HA	**0**	**0**	**1300**	**814**	**4200**	**718**	**3000**	**679**	**3900**	**960**	**1100**	**694**	**2000**	**742**	**3700**	**691**	**$24,498.00**
REAG Reps to travel	**5**		**3**		**4**		**4**		**5**		**5**		**5**		**4**		
SYD	350	150	0	0	1000	156	700	143	900		250	148	500	164	900	147	
SYD	350	150	0	0	1000	156	700	143	900		250	148	500	164	900	147	
Perth	1000	150	700	188	0	0	700	143	900	220	1000	148	900	164	1000	147	
SA	700	150	600	188	600	156	0	0	900		700	148	700	164	600	147	
TAS	900	150	900	188	1000	156	700	143	1200		600	148	300	164	0	0	
Estimated Travel costs for REAG	**3300**	**750**	**2200**	**564**	**3600**	**624**	**2800**	**572**	**4800**	**220**	**2800**	**740**	**2900**	**820**	**3400**	**588**	$30,678.00

Additional Resources (extimates based on 30 attendees)								
- catering	1200	1200	1200	1200	1200	1200	1200	1200
- venue hire	2000	0	0	0	0	0	0	0
- incidentals	200	200	200	200	200	200	200	200
Estimated additional costs	**3400**	**1400**	**1400**	**1400**	**1400**	**1400**	**1400**	**1400**	$13,200.00

Projected total expenditure	$68,376.00

Option 2 – Partial Home Affairs Representation, Partial REAG Representation, All states and territories

	ACT		NSW		WA		SA		NT		QLD		VIC		TAS		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps																	
SES/EL2																	
To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	1200	250	900	250	1200	300	350	250	500	250	1000	250	
Assistant Director																	
Only attend the busiest meetings to assist in leading discussions and capturing information.			300	188									500	164			
Project Lead																	
The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	1000	156	700	143	900	220	250	148	500	164	900	147	
Logistical lead																	
To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence.			300	188	1000	156	700	143	900	220	250	148	500	164	900	147	
Estimated Travel costs for HA	**0**	**0**	**1300**	**814**	**3200**	**562**	**2300**	**536**	**3000**	**740**	**850**	**546**	**2000**	**742**	**2800**	**544**	**$19,934.00**
REAG Reps to travel	**5**		**3**		**4**		**4**		**5**		**5**		**5**		**4**		
SYD	350	150	0	0													
SYD			0	0							250	148					
Perth					0	0			900	220							
SA							0	0	900	220							
TAS													300	164	0	0	
Estimated Travel costs for REAG	**350**	**150**	**0**	**0**	**0**	**0**	**0**	**0**	**1800**	**440**	**250**	**148**	**300**	**164**	**0**	**0**	$3,602.00
Additional Resources (extimates based on 30 attendees)																	
- catering	1200		1200		1200		1200		1200		1200		1200		1200		
- venue hire	2000		0		0		0		0		0		0		0		
- incidentals	200		200		200		200		200		200		200		200		
Estimated additional costs	**3400**		**1400**		**1400**		**1400**		**1400**		**1400**		**1400**		**1400**		$13,200.00

Projected total expenditure	**$36,736.00**

Option 3 – Partial Home Affairs Representation, Full REAG Representation, Selected States and territories

	ACT		NSW		WA		VIC		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps									
SES/EL2 To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	1200	250	500	250	
Assistant Director Only attend the busiest meetings to assist in leading discussions and capturing information.			300	188			500	164	
Project Lead The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	1000	156	500	164	
Logistical lead To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence. Only assist in the busiest meetings.			300	188			500	164	
Estimated Travel costs for HA	**0**	**0**	**1300**	**814**	**2200**	**406**	**2000**	**742**	**$7,462.00**
REAG Reps to travel	**5**		**3**		**4**		**5**		
SYD	350	150	0	0	1000	156	500	164	
SYD	350	150	0	0	1000	156	500	164	
Perth	1000	150	700	188	0	0	900	164	
SA	700	150	600	188	600	156	700	164	
TAS	900	150	900	188	1000	156	300	164	
Estimated Travel costs for REAG	**3300**	**750**	**2200**	**564**	**3600**	**624**	**2900**	**820**	**$14,758.00**

Additional Resources (extimates based on 30 attendees)					
- catering	1200	1200	1200	1200	
- venue hire	2000	0	0	0	
- incidentals	200	200	200	200	
Estimated additional costs	**3400**	**1400**	**1400**	**1400**	**$7,600.00**

Projected total expenditure	**$29,820.00**

Option 4 – Partial Home Affairs and REAG Representation, Selected states and territories

	ACT		NSW		WA		VIC		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps									
SES/EL2									
To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	1200	250	500	250	
Assistant Director									
Only attend the busiest meetings to assist in leading discussions and capturing information.			300	188			500	164	
Project Lead									
The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	1000	156	500	164	
Logistical lead									
To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence. Only assist in the busiest meetings.			300	188			500	164	
Estimated Travel costs for HA	**0**	**0**	**1300**	**814**	**2200**	**406**	**2000**	**742**	**$7,462.00**
REAG Reps to travel	**5**		**3**		**4**		**5**		
SYD	350	150	0	0					
SYD	350	150	0	0					
Perth			700	188	0	0			
SA					600	156	700	164	
TAS							300	164	
Estimated Travel costs for REAG	**700**	**300**	**700**	**188**	**600**	**156**	**1000**	**328**	**$3,972.00**
Additional Resources (extimates based on 30 attendees)									
- catering	1200		1200		1200		1200		
- venue hire	2000		0		0		0		
- incidentals	200		200		200		200		
Estimated additional costs	**3400**		**1400**		**1400**		**1400**		**$7,600.00**

Projected total expenditure	**$19,034.00**

Option 5 – Minimal Home Affairs and REAG Representation, Selected states and territories

	ACT		NSW		WA		VIC		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps									
SES/EL2 To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	1200	250	500	250	
Assistant Director Only attend the busiest meetings to assist in leading discussions and capturing information.			300	188					
Project Lead The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	1000	156	500	164	
Logistical lead - Role to be undertaken by Project lead To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence. Only assist in the busiest meetings.									
Estimated Travel costs for HA	**0**	**0**	**1000**	**626**	**2200**	**406**	**1000**	**414**	**$5,646.00**
REAG Reps to travel	**5**		**3**		**4**		**5**		
SYD	350	150	0	0					
SYD	350	150	0	0					
Perth			700	188	0	0			
SA					600	156	700	164	
TAS							300	164	
Estimated Travel costs for REAG	**700**	**300**	**700**	**188**	**600**	**156**	**1000**	**328**	**$3,972.00**

Additional Resources (extimates based on 30 attendees)					
- catering	1200	1200	1200	1200	
- venue hire	2000	0	0	0	
- incidentals	200	200	200	200	
Estimated additional costs	**3400**	**1400**	**1400**	**1400**	**$7,600.00**

Projected total expenditure	**$17,218.00**

Option 6 – Minimal Home Affairs and REAG Representation, All States and territories

	ACT		NSW		WA		SA		NT		QLD		VIC		TAS		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps																	
SES/EL2																	
To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	1200	250	900	250	1200	300	350	250	500	250	1000	250	
Assistant Director																	
Only attend the busiest meetings to assist in leading discussions and capturing information.			300	188									500	164			
Project Lead																	
The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	1000	156	700	143	900	220	250	148	500	164	900	147	
Logistical lead - Role to be undertaken by Project lead																	
To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence. Only assist in the busiest meetings.																	
Estimated Travel costs for HA	**0**	**0**	**1000**	**626**	**2200**	**406**	**1600**	**393**	**2100**	**520**	**600**	**398**	**1500**	**578**	**1900**	**397**	**$14,218.00**
REAG Reps to travel	**5**		**3**		**4**		**4**		**5**		**5**		**5**		**4**		
SYD	350	150	0	0													
SYD			0	0							250	148					
Perth					0	0			900	220							
SA							0	0	900	220							
TAS													300	164	0	0	
Estimated Travel costs for REAG	**350**	**150**	**0**	**0**	**0**	**0**	**0**	**0**	**1800**	**440**	**250**	**148**	**300**	**164**	**0**	**0**	$3,602.00
Additional Resources (estimates based on 30 attendees)																	
- catering	1200		1200		1200		1200		1200		1200		1200		1200		
- venue hire	2000		0		0		0		0		0		0		0		
- incidentals	200		200		200		200		200		200		200		200		
Estimated additional costs	**3400**		**1400**		**1400**		**1400**		**1400**		**1400**		**1400**		**1400**		$15,200.00

Projected total expenditure	$31,020.00

Option 7 – Minimal Home Affairs and Single REAG Representation, All States and territories

	ACT		NSW		WA		SA		NT		QLD		VIC		TAS		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps																	
SES/EL2																	
To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	1200	250	900	250	1200	300	350	250	500	250	1000	250	
Assistant Director																	
Only attend the busiest meetings to assist in leading discussions and capturing information.			300	188									500	164			
Project Lead																	
The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	1000	156	700	143	900	220	250	148	500	164	900	147	
Logistical lead - Role to be undertaken by Project lead																	
To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence. Only assist in the busiest meetings.																	
Estimated Travel costs for HA	**0**	**0**	**1000**	**626**	**2200**	**406**	**1600**	**393**	**2100**	**520**	**600**	**398**	**1500**	**578**	**1900**	**397**	**$14,218.00**
REAG Reps to travel	**5**		**3**		**4**		**4**		**5**		**5**		**5**		**4**		
SYD	350	150	0	0													
SYD			0	0							250	148					
Perth					0	0			900	220							
SA							0	0									
TAS													300	164	0	0	
Estimated Travel costs for REAG	**350**	**150**	**0**	**0**	**0**	**0**	**0**	**0**	**900**	**220**	**250**	**148**	**300**	**164**	**0**	**0**	$2,482.00
Additional Resources (estimates based on 30 attendees)																	
- catering	1200		1200		1200		1200		1200		1200		1200		1200		
- venue hire	2000		0		0		0		0		0		0		0		
- incidentals	200		200		200		200		200		200		200		200		
Estimated additional costs	**3400**		**1400**		**1400**		**1400**		**1400**		**1400**		**1400**		**1400**		$13,200.00

Projected total expenditure	$29,900.00

Option 8 – Minimal Home Affairs and Single REAG Representation, Selected States and territories

	ACT		NSW		QLD		VIC		
	Flights	Accom	Flights	Accom	Flights	Accom	Flights	Accom	
Home Affairs Reps									
SES/EL2 To lead discussions and show attendees that this is a priority for Home Affairs.			400	250	350	250	500	250	
Assistant Director Only attend the busiest meetings to assist in leading discussions and capturing information.			300	188			500	164	
Project Lead The primary strategy writer and project lead. This will allow full visibility of the process, participation in discussions and ensure all input is captured.			300	188	250	148	500	164	
Logistical lead - Role to be undertaken by Project lead To coordinate the administrative and logistical needs for the roadshow. This will include set up of room, attendee tracking, catering, minute taking, correspondence. Only assist in the busiest meetings.									
Estimated Travel costs for HA	**0**	**0**	**1000**	**626**	**600**	**398**	**1500**	**578**	**$4,702.00**
REAG Reps to travel	**5**		**3**		**5**		**5**		
SYD	350	150	0	0					
SYD			0	0	250	148			
Perth									
SA									
TAS							300	164	
Estimated Travel costs for REAG	**350**	**150**	**0**	**0**	**250**	**148**	**300**	**164**	**$1,362.00**

Additional Resources (extimates based on 30 attendees)					
- catering	1200	1200	1200	1200	
- venue hire	2000	0	0	0	
- incidentals	200	200	200	200	
Estimated additional costs	**3400**	**1400**	**1400**	**1400**	**$7,600.00**

Projected total expenditure	**$13,664.00**