Critical infrastructure protection and the role of emergency services

by Mike Rothery, Assistant Secretary,
Critical Infrastructure Protection Branch, Attorney-General's Department

Introduction

Since Al-Qaeda's attacks on the USA on 11 September 2001, protecting critical infrastructure from terrorist attack has become a high priority for the Australian Government. There are other factors, however, that need to be taken into consideration as they can seriously affect critical infrastructure.

As most of Australia's critical infrastructure is privately owned or operated it has been essential to build a partnership between business and government to ensure critical infrastructure is adequately protected, not just from terrorism, but from all hazards, be they flood, fire, or a tsunami such as the one that devastated our close neighbours so recently.

The Australian Government regards emergency services as essential government services that form part of Australia's critical infrastructure. Australia's emergency services, police, ambulance, fire, State Emergency Services, both volunteer and professional organisations, as well as non-government organisations such as the Red Cross are represented in the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).

The TISN is not an operational network, but is concerned with policy issues in a medium-to-long term timeframe. It plays a key role in protecting Australia's critical infrastructure by allowing members to share security-related information in a secure environment. Through its peak committee, the Critical Infrastructure Advisory Council, TISN members have a direct line of communication to the Attorney-General, and to the National Counter-Terrorism Committee.

As the Bali and Madrid bombings illustrated, terrorists also target large crowds, which is why the Australian Government treats the owners and operators of these types of events and venues in a similar way as the owners and operators of critical infrastructure.

Critical Infrastructure Protection has become a general label for a range of activities undertaken jointly by government and the operators of key locations, facilities and systems to ensure they are adequately managing risk. These initiatives cover three main categories:

- *critical infrastructure assets*—those assets or systems deemed more likely to be targeted because of the downstream impact of a successful attack, or where the consequences would be intolerably severe, or some combination of the two;
- *places of mass gathering*—those types of sites where large numbers of people congregate, such as those terrorists have previously targeted overseas; and
- *information infrastructure*—the possible exploitation of the inherent vulnerabilities in computer and communication systems so as to bring about failure in critical systems, or the loss or compromise of data.

The Emergency Services sector falls into the category of "critical infrastructure assets" because it is a key system providing an essential service.

Defining critical infrastructure

The term "critical infrastructure protection" has been around for some time. Originally it was used to describe mission critical IT systems in the Y2K context. Its usage has since grown to include other work such as "vital assets" and "lifelines". At the core of this work is some form of value judgement about importance or criticality, often measured in terms of the downstream effects of a particular incident.

From a national perspective, the Australian Government defines critical infrastructure as:

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

Some critical elements in these sectors are not strictly speaking infrastructure, but are in fact networks or supply chains that support the delivery of essential products or services. For example, bringing food from the paddock to the plate is dependent not only on particular key facilities, but also on a complex network of producers, processors, manufacturers, distributors and retailers. Where an incident involving these networks could have a significant impact, those networks are treated as critical infrastructure.

The Emergency Services sector is classed as critical infrastructure, not only in terms of specific assets such as control centres, but also in terms of its supporting communication networks, such as 000.

Some types of critical infrastructure depend on other forms of infrastructure being available, while some sectors are mutually dependent on each other. The degree and complexity of interdependencies is increasing as Australia becomes more dependent on shared information systems and convergent communication technologies, including the Internet.

Protecting such a wide range of critical infrastructure is an enormous task. In addition, up to 90 per cent of Australia's critical infrastructure is owned or operated by the private sector.

The Government believes that adequate and appropriate security is best achieved by building a strong partnership between it and the private sector and other levels of government, based on trust and a willingness to share information about security-related issues—not just problems, but solutions.

The National Counter-Terrorism Committee and the role of the States and Territories

The National Counter-Terrorism Committee (NCTC) is the primary body for developing Australia's national counter-terrorism arrangements. The committee includes the deputy commissioners from each State and Territory Police service and senior representatives from premiers' and chief ministers' departments. It is chaired by the Department of the Prime Minister and Cabinet and includes senior representatives from the Department of the Prime Minister and Cabinet, the Attorney-General's Department, Emergency Management Australia, the Department of Defence, Australian Federal Police, Australian Security Intelligence Organisation, the Department of Transport and Regional Services and other relevant agencies.

The NCTC has recently developed *National Guidelines for Protecting Critical Infrastructure from Terrorism*[1]. These guidelines provide a nationally consistent approach for Australian governments to provide advice to the owners and operators of critical infrastructure on the protection of their assets from terrorism. They provide suggested actions to be considered in response to the security environment and address topics such as risk assessments, public information and media management, prevention and preparedness and response and recovery.

The guidelines set out the roles and responsibilities of the Australian, State and Territory and local governments, police, and owners and operators of critical infrastructure in protecting from terrorism.

State and Territory governments are responsible for distributing the guidelines, as they have identified which infrastructure is critical within their jurisdiction. Similarly, they are primarily responsible for the prevention of, and response to, incidents threatening the security of businesses within their jurisdiction. They are currently developing and implementing frameworks, in co-operation with the business community, to apply the guidelines within their jurisdictions. It is through these relationships that the essential counter-terrorism message will be delivered to business.

The National Committee on Critical Infrastructure Protection (NCCIP) is the dedicated standing committee that co-ordinates critical infrastructure protection policy development across all levels of government. The committee comprises Australian and State/Territory government representatives as well as a representative from the Australian Local Government Association. This mechanism ensures greater awareness within and between governments of CIP initiatives.

Business–Government Task Force on critical infrastructure protection

The terrorist attacks on the USA on 11 September 2001 brought the Australian Government's policy on critical infrastructure protection sharply into focus. In November 2001 the Prime Minister announced the formation of the Business-Government Task Force on Critical Infrastructure. The Task Force was given the mission of examining what needed to be done to ensure Australia's critical infrastructure was adequately protected.

The Task Force meeting in Sydney on 21–22 March 2002 brought together senior executives from some of Australia's major corporations, representatives from various utilities, State and Territory governments and a range of interested Commonwealth agencies[2].

That meeting produced a list of six recommendations provided in the accompanying box. These recommendations were accepted by the Government in November 2002.

[1] The National Counter-Terrorism Committee's *National Guidelines for Protecting Critical Infrastructure from Terrorism* is not a public document. A fact sheet on the Guidelines is available at http://www.tisn.gov.au or from the Attorney-General's Department Critical Infrastructure Branch (ph: 02 6272 7100 or email cip@ag.gov.au).

[2] The Task Force's report and other background documents are available from http://www.tisn.gov.au or from the Attorney-General's Department Critical Infrastructure Protection Branch (ph: 02 6272 7100 or email cip@ag.gov.au).

Task force 2002 recommendations

1. The Commonwealth and the States and Territories, in consultation with the private sector, should develop a strategic overview of risks to critical infrastructure and, as a first step, commit to prioritisation of tasks building on the work that has already been done to assess vulnerabilities in the telecommunications, transport and public utilities sectors, by 30 September 2002.
2. The Commonwealth, in co-operation with the private sector and the States and Territories, should build on existing mechanisms, such as the Standing Advisory Committee on Commonwealth-State Cooperation for Protection Against Violence (SAC-PAV) and arrangements for emergency management, to ensure systems and procedures are in place to adequately protect the critical infrastructure.
3. The Commonwealth should build a learning network among the key public and private sector organisations to improve systematic, strategic responses to the security of the National Information Infrastructure—separate from, but linked to, physical critical infrastructure protection and SAC-PAV.
   - The network should have a clear brand, clear responsibilities, protocols, priorities and a central point of contact for authoritative statements, but should also have redundancy and linkages to key international resources.
   - A public/private sector partnership to enhance national information infrastructure assurance should be developed out of this Business-Government Task Force for periodic consultation and advice to the network.
   - AusCERT should be strengthened as a central component of a national system for early warning and advice on immediate response and risk management. Issues to be discussed include funding and whether their advice would continue to be available for a fee only to member organisations, as at present.
   - The Commonwealth, in consultation with the private sector, should examine major threats and interdependencies in telecommunications and banking as an example of specific, targeted consideration between the relevant agencies and organisations.
4. The Commonwealth, States and Territories should review their legislative frameworks for sharing information so as to facilitate the supply of information by business, ensure its confidentiality and exclude liabilities.
5. The Commonwealth should develop models of good critical infrastructure assurance, taking into account relevant standards, in consultation with the private sector and the States and Territories.
6. The Commonwealth, States and Territories should examine ways to encourage investment in the security and resilience of critical infrastructure.

Critical infrastructure protection has grown to include vital assets including building structures and lifeline utilities

Trusted Information Sharing Network for Critical Infrastructure Protection

The Attorney-General's Department hosted a summit on critical infrastructure protection in Melbourne in April 2003. The summit brought together representatives from industry, State and Territory governments and Australian Government agencies. The Australian Local Government Association also attended, representing its members. The role of emergency services in critical infrastructure protection was acknowledged by the attendance of a number of representatives from emergency services organisations.

It was at this summit that the then Attorney-General, Daryl Williams, launched the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), which was formed as a direct result of the Task Force's recommendations.

Following is a brief overview of the different areas of the TISN, their structure, roles and responsibilities.

Infrastructure Assurance Advisory Groups

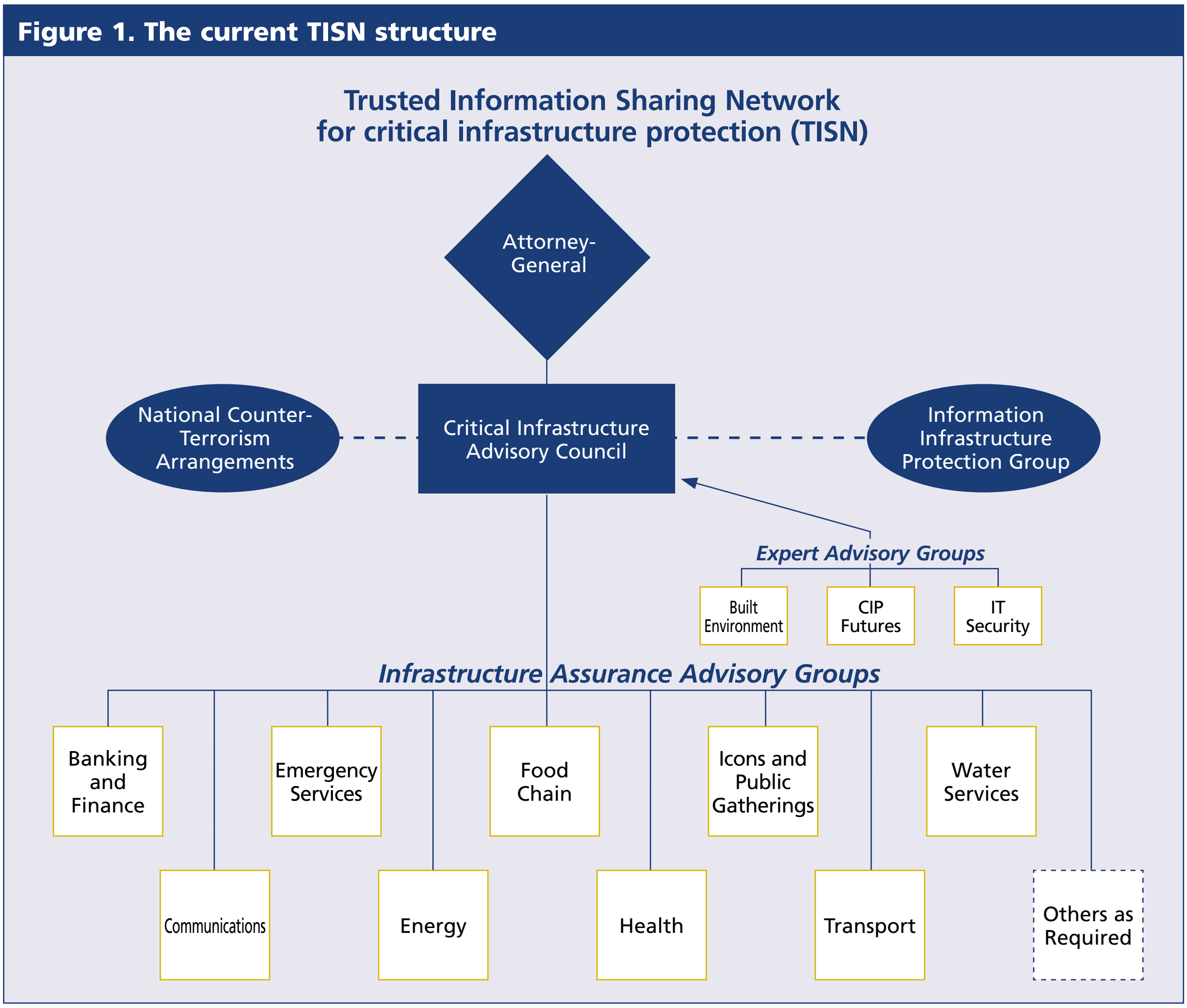
The Infrastructure Assurance Advisory Groups (IAAGs) have been created to allow the owners and operators of critical infrastructure to share information on threats and vulnerabilities and appropriate measures and strategies to mitigate risk. By having agencies from both the Australian Government and the States and Territories participating or involved, industry can be briefed on government activity. To date groups have been established for the banking and finance, communications, emergency services, energy, food chain, health, icons and public gatherings, transport and water services sectors. The structure is, however, flexible to allow new groups to join as and when necessary.

Critical Infrastructure Advisory Council

The Critical Infrastructure Advisory Council (CIAC) oversees the IAAGs and advises the Attorney-General on the national approach to critical infrastructure protection. It reports directly to the Attorney-General.

Members are drawn from each sector group, each of the States and Territories, relevant Australian Government agencies and the National Counter-Terrorism Committee. The committee is chaired by the Attorney-General's

Figure 1. The current TISN structure


Trusted Information Sharing Network
for critical infrastructure protection (TISN)
Attorney-General
National Counter-Terrorism Arrangements
Critical Infrastructure Advisory Council
Information Infrastructure Protection Group
Expert Advisory Groups
Built Environment
CIP Futures
IT Security
Infrastructure Assurance Advisory Groups
Banking and Finance
Emergency Services
Food Chain
Icons and Public Gatherings
Water Services
Communications
Energy
Health
Transport
Others as Required

Department. The current chair is Miles Jordana, Deputy Secretary, National Security and Criminal Justice Group. This committee provides the crucial link between the TISN and the counter-terrorism community.

TISN's focus

TISN does not have an operational focus and does not replace existing response and operational emergency services mechanisms. It is primarily a consultative and co-ordination body for policy issues surrounding critical infrastructure protection. The TISN brings a national focus to the subject area. Much of Australia's critical infrastructure, such as electricity and communications cables, and food and health supply chains, cross jurisdictional boundaries. It is therefore important that the operators of these infrastructure assets have a forum in which to discuss a national approach to these issues.

Responsibilities of owners and operators

Owners and operators of critical infrastructure are responsible for:

- providing adequate security of their assets;
- actively applying risk management techniques to their planning processes;
- conducting regular reviews of risk management assessments and plans;
- reporting any incidents or suspicious activity to State or Territory police;
- developing and regularly reviewing business continuity plans; and
- testing their plans by participating in any exercises conducted by government authorities.

Owners or operators need to have sound risk management and business continuity strategies in place, taking into account that being part of Australia's critical infrastructure can in fact increase the risk of attack on their assets.

Although the threat posed by a terrorist attack has a high priority in assessing the risk to critical infrastructure assets, owners and operators need to take an "all hazards" approach. This involves examining different types of threat likely to affect their business, such as natural disaster, accident, human error, and poor maintenance.

Emergency services and the emergency management organisation have a significant role to play in assisting owners and operators of critical infrastructure in developing emergency management plans which, along with security plans, form an important element of their risk management and business continuity strategies. Emergency services also have a role in testing and reviewing emergency management plans and in many cases have established close working relationships with infrastructure owners and operators.

Sound business continuity planning can ensure that a business can minimise interruption to its services, and consequently minimise economic loss.

The Attorney-General's Department

There are three areas of the Attorney-General's Department with critical infrastructure protection responsibilities.

The Critical Infrastructure Protection Branch is responsible for the development and co-ordination of the Australian Government's policy as well as international liaison. The branch has four sections—Critical Infrastructure Policy, National Information Infrastructure, Major Projects, and National Security Business Partnership. It serves as a co-ordination point for liaison between the TISN sector groups and provides secretariat services to the Critical Infrastructure Advisory Council, and the banking and finance, icons and public gatherings and water services sector groups.

The two major projects currently being undertaken by the branch are the Computer Network Vulnerability Assessment (CNVA) project and the Critical Infrastructure Protection Modelling and Analysis project.

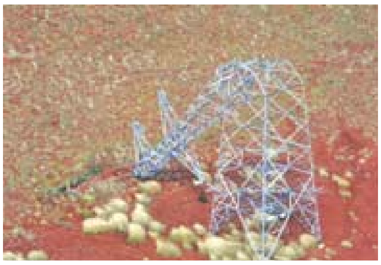
The CNVA Program has been developed to support the TISN's work. It has two components—one for the private sector and another for the public sector. The Attorney-General's Department is responsible for the private sector component while the Defence Signals Directorate is responsible for the public sector component. The private sector component involves working with critical infrastructure owners and operators to identify major vulnerabilities in their computer systems and interdependencies between connected computer networks. It will also test the systems' abilities to resist exploitation.

The overall aim of the Modelling and Analysis project is to develop a capability to model, simulate and analyse the primary interdependencies between national critical infrastructures and the flow-on consequences of a critical infrastructure failure in a particular sector.

Emergency Management Australia and the Protective Security Coordination Centre are also part of the Attorney-General's Department.

Emergency Management Australia is the Commonwealth Government agency which has responsibilities in relation to protection of life and property resulting from the impact of natural, technological and human caused disasters.

The Protective Security Coordination Centre manages the Government's protective security responsibilities and performs a coordination role in marshalling resources in preventing, or responding to, threats to Australia's national security. It maintains close working relationships with all



Disruptions to major electricity infrastructure test the adequacy of back up supplies

Australian Government departments and agencies, Federal, State and Territory police services, Premiers' and Chief Ministers' Departments and security agencies.

Emergency services and the TISN

The Emergency Services Infrastructure Assurance Advisory Group represents the sector in the TISN. Its members are drawn from relevant Australian Government agencies, State and Territory emergency services, emergency services national peak bodies and the Australian Red Cross. The group is chaired by the Director General of Emergency Management Australia, Mr David Templeman, who is also a member of the Critical Infrastructure Advisory Council, the National Counter-Terrorism Committee and the Australian Emergency Management Committee. This provides an invaluable cross-linkage between the various agencies involved in counter-terrorism, critical infrastructure protection and emergency management.

The group centres its activities on ensuring continuity of service provision by the emergency services. To date it has shared information on a range of issues including identification of critical emergency services infrastructure, risk assessment tools and methodologies, threats and vulnerabilities, mitigation strategies, treatment options and interdependencies with other industry sectors. It has also held a discussion exercise examining dependencies and interdependencies on other industry sector groups.

Its forward work program includes work on defining the emergency services critical infrastructure and the development of emergency services-specific preparedness guidelines for each counter-terrorism alert level, based on the model outlined in the *National Guidelines for Protecting Critical Infrastructure from Terrorism.*

In 2004 the group was involved in a discussion exercise conducted by the TISN. This exercise broadly examined the interdependencies between different sectors in a scenario which had Victoria suffering a prolonged major disruption to its electricity supply. The exercise proved invaluable in challenging assumptions in all sectors about the availability of back up resources including generators, water and fuel supplies.

Conclusion

The emergency services sector forms part of Australia's critical infrastructure. Through its involvement in the Trusted Information Sharing Network for Critical Infrastructure Protection it is able to share vital information on security issues with other critical infrastructure sectors.
Its representation on the Critical Infrastructure Advisory Council helps inform that body in its input into the National Counter Terrorism Committee and the Council's advice to the Attorney-General.

Further information about critical infrastructure protection can be found on the TISN website—www.tisn.gov.au, or by contacting the Attorney-General's Department Critical Infrastructure Protection Branch (email: cip@ag.gov.au, phone: 02 6272 7100).