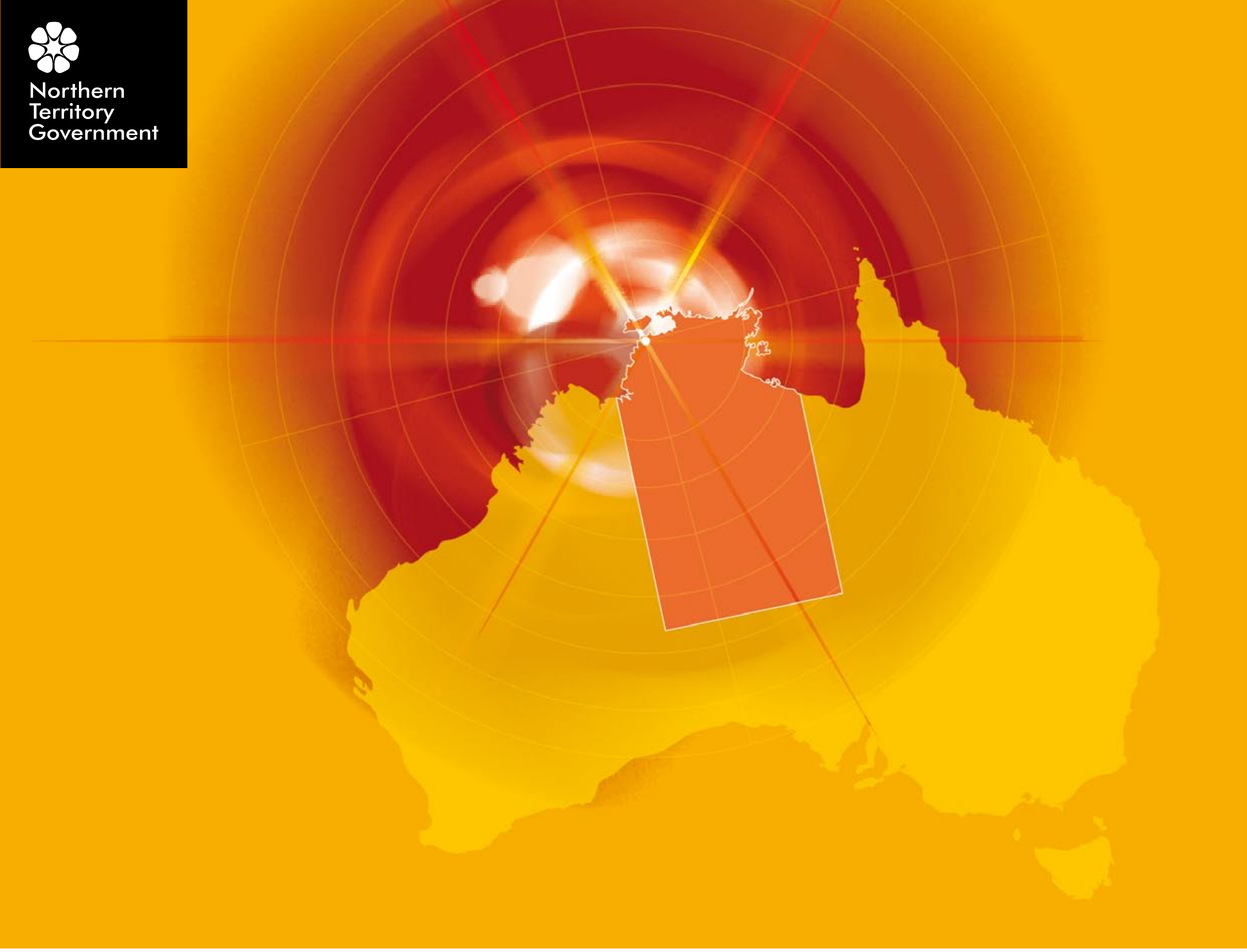
Northern
Territory
Government



Framework for the Protection of Northern Territory Critical Infrastructure

Version 1 January 2009

Contents

Letter of Promulgation

A core responsibility of government is the safety of its citizens. The ability of Northern Territory (NT) businesses and government to continue to operate in the aftermath of an emergency is crucial to the safety and well-being of all Territorians. The protection of critical infrastructure in the NT is a key element that involves a cooperative partnership between government at all levels, owners and operators of critical infrastructure and their representative bodies.

The threat to critical infrastructure is wide ranging. Terrorist groups regard Australia and Australians as legitimate targets and attacks carried out by these groups around the world have targeted government buildings, hotels and tourist facilities, shipping, oil and energy infrastructure and aviation and land transport. Furthermore, the NT has numerous and regular threats from natural hazards and major industrial accidents are an ever present risk.

This document provides an overarching framework for critical infrastructure protection in the NT and outlines the management and governance arrangements to achieve it. It is relevant to both government and industry. It describes the roles and responsibilities of the three levels of government, specific NT Government agencies and the owners and operators of critical infrastructure.

The framework is consistent with national arrangements for critical infrastructure protection, adapted to the NT context. It adopts an all hazard approach whereby the infrastructure needs to be protected from all threats, whether they are natural or man made. It outlines the actions that owners and operators could take to enhance the security and continuity of their assets, and the interaction with government.

We commend the publication to those charged with the important task of building a stronger and safer NT.

Mike Burgess
Chief Executive
Department of the Chief Minister

27 August 2008

Paul White
Commissioner of Police and
Chief Executive, Fire and Emergency Services

27 August 2008

Introduction

Aim

The aim of this framework is to ensure the Northern Territory (NT) has a consistent and coordinated approach to the management of critical infrastructure protection (CIP) that fits within and complements the “all hazards” principle in managing emergencies.

The framework is intended for government agencies and owners and operators of critical infrastructure to ensure each is aware of existing arrangements and their respective roles and responsibilities.

The framework is consistent with the national arrangements for CIP.

The *Guidelines for the Management of Northern Territory Critical Infrastructure Protection Program* (NT CIP Guidelines) provide additional information and guidance to members of the Northern Territory Critical Infrastructure Protection Coordination Group (NT CIPCG) and are complementary to this Framework.

Government/Business Partnership

The protection of critical infrastructure is a shared responsibility between business and the NT Government. Potential threats are wide-ranging, complex and difficult to quantify. Similarly mitigating the risk posed by these threats is a difficult process requiring extensive understanding of individual businesses as well as potential vulnerabilities through linkages with other sectors. Information sharing and effective timely communication is therefore essential.

The most effective critical infrastructure process is one built on a strong government-business partnership. One where owners and operators actively address their own security and business continuity needs and where government provides the mechanisms and processes for information sharing between sectors, advice on critical infrastructure developments and methodologies, and rapid dissemination of relevant security and threat advice. Through an open partnership, the risks to NT critical infrastructure can be reduced to an acceptable level.

Management Framework

Definition

The NT acknowledges the nationally accepted definition of critical infrastructure described in the *National Guidelines for Protecting Critical Infrastructure from Terrorism* (the National Guidelines). That definition adapted to the NT context is:

> *Critical infrastructure is those physical facilities, supply chains, information technologies, communication networks or events which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the Northern Territory and its community.*

It is not possible to specify an exact period of time that is an extended period, as the impact of the unavailability of critical infrastructure will vary across sectors and assets. However, any period less than 24 hours should not generally be considered an extended period.

The NT adapts the national definition of significant impact from the National Guidelines as:

> *An event or incident that poses a major risk to public safety and confidence, threatens economic security, harms the Territory's competitiveness, or impedes the continuity of government and its services.*

The definition is necessarily broad as it is not possible to satisfactorily quantify or accurately describe all types of critical infrastructure which may include facilities, services, networks and events. Some critical infrastructure may be complete systems or elements of systems or it may be assets of a symbolic or iconic nature. Some assets may be designated critical infrastructure because another critical infrastructure facility or system is dependent on them. Accordingly the identification of critical infrastructure is not definitive and requires a considered and flexible approach.

All Hazards

Critical infrastructure can be damaged, destroyed or disrupted by natural disasters, negligence, accidents or deliberate acts of sabotage, terrorism, cyber attack, criminal activity or malicious damage. Although terrorism and security have assumed a higher profile in Australia in recent years, the protection of critical infrastructure against all threats and hazards is of equal importance.

Scope of Critical Infrastructure Protection

Protection of all infrastructures from all threats is clearly not possible. By applying risk management techniques, attention can be focused on areas of greatest risk, taking into account the threat, relative criticality, vulnerability, the existing level of protective security and the effectiveness of available mitigation strategies for business continuity.

CIP is not a new discipline, but is a coordinated blending of existing specialisations (many of which overlap), including:

- national security and defence;
- market and government regulation;
- law enforcement and crime prevention;
- counter terrorism;
- emergency management;
- protective security (physical, personnel and procedural);
- e-security;
- risk management; and
- business continuity planning.

CIP brings together a significant number of existing strategies, plans and procedures that deal with the prevention, preparedness, response and recovery arrangements for disasters and emergencies.

Layers of Critical Infrastructure

The identification and management of critical infrastructure is a responsibility of all levels of government – national, state or territory and local. Accordingly, critical infrastructure located in the NT may be identified as:

- **National Critical Infrastructure** – assets identified by the Australian Government from a national perspective, with considerations based on national social wellbeing, their contribution to the gross domestic product, defence and national security;

- **NT Critical Infrastructure** – assets identified by the NT Government from a Territory perspective using Territory determined measures; or

- **Local Critical Infrastructure** – assets identified by local governments as essential to the social or economic wellbeing of their communities.

This framework is primarily concerned with NT critical infrastructure. However some assets may be identified by more than one level of government. For example some critical infrastructure may be identified at both the national and NT level. In these cases coordination across the levels of government will be managed by the NT CIPCG.

Interdependencies

The continuity of services supplied by critical infrastructure is usually dependent, to some extent, upon availability of other infrastructure, and 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. Owners and operators of critical infrastructure are encouraged to work together to identify these interdependencies and apply appropriate strategies to reduce risk where possible. The Critical Infrastructure Protection Modelling and Analysis (CIPMA) Program examines relationships and dependencies between critical infrastructure systems.

Places of Mass Gathering

Places of mass gathering are characterised in the *National Approach for the Protection of Places of Mass Gathering from Terrorism* as:

> *"….. the concentration of people on a predictable basis, in venues or precincts that are open or enclosed."*

Although places of mass gathering do not meet the definition of critical infrastructure, they are subject to the same threats. Therefore there may be situations where the determination of places of mass gatherings as critical infrastructure is appropriate, noting however the important distinction that the risk management considerations are based on the protection of people and not the protection of physical infrastructure. In addition it is not appropriate to impose an arbitrary numerical threshold.

Critical Infrastructure in the Security Context

There are a number of factors which must be considered by critical infrastructure owners and operators to place their assets in the appropriate context. Information to assist with this can be found in the following documents or advice.

Current Security Environment

The Australian Security Intelligence Organisation (ASIO) produces a document which outlines Australia's current security environment. The document is not security classified, it is updated as required and is available from the Department of the Chief Minister or NT Police (see contacts).

Alert Levels

The National Counter Terrorism Alert System is a range of four levels, described in the table below, that communicate an assessed risk of terrorist threat to Australia. The National Counter Terrorism Alert System guides national preparation and planning. It also promotes increased precaution and vigilance when necessary to minimise the risk of a terrorist incident occurring.

Alert Level	Meaning
Low	Terrorist attack is not expected
Medium	Terrorist attack could occur
High	Terrorist attack is likely
Extreme	Terrorist attack is imminent or has occurred

Increases in security and resources required to maintain a higher alert level may have a significant impact on a community, and on the operation of critical infrastructure. Australian Governments may change the alert level for the nation. Alternatively, to avoid unnecessary disruption to communities not affected by a particular situation, the alert level(s) may be changed for one or more impacted communities, locations or sectors as required.

A change in alert level(s) will be communicated by the Prime Minister or representative. Subsequent to any change in alert level(s), the NT Government will release public information and advice specific to the NT. In addition NT Police will contact owners and operators of critical infrastructure that may be directly affected by changes in the security environment affecting the NT.

Threat Assessments

ASIO is the national threat assessment agency and they prepare threat assessments for specific events, facilities and sectors. Threat assessments relating to critical infrastructure fall into two broad categories:

- those that assist preparedness and planning; or
- those that require an immediate response either to a specific threat or to a heightened assessment of threat.

The dissemination of threat assessment information concerning industry sectors is undertaken by ASIO in conjunction with the Department of the Chief Minister and NT Police. This takes the form of briefings to all relevant industry representatives, both government and non-government.

Threat assessments are necessarily security classified and are retained by NT Police. ASIO update threat assessments as required and relevant changes will be advised to owners and operators of critical infrastructure.

Risk Context Statements

Risk context statements are derived from ASIO threat assessments and are prepared by the relevant Australian Government agency in consultation with industry. They are designed to complement strategic risk and threat assessment information available from other sources. They provide a strategic risk context to assist owners and operators in determining their own local security risk context.

Risk context statements can be obtained from the Department of the Chief Minister or NT Police (see contacts). Should new or revised risk context statements be produced, owners and operators will be notified by the Department of the Chief Minister or NT Police and appropriate briefings will be arranged.

Specific Threat Intelligence

Arrangements have been established for passing specific or immediate threat intelligence or information between relevant government agencies at both Australian Government and NT Government levels and direct to owners and operators of critical infrastructure where necessary. ASIO will contact NT Police who will in turn contact owners and operators of critical infrastructure. Where there is particular urgency about a threat, ASIO may contact owners and operators of critical infrastructure directly.

It is also essential that owners and operators of critical infrastructure report back to the NT Police on incidents and suspicious activity. Relevant information may lead to a police response or investigation. It will also be passed to ASIO for consideration in the updating of threat assessments.

Governance Arrangements

Diagram 1 outlines Australia’s critical infrastructure arrangements.

National Arrangements

The Australian Government has a coordinating role in the development of a nationally consistent approach to the protection of critical infrastructure, including:

- coordination and leadership in areas of joint responsibility and on international issues;
- producing and communicating relevant intelligence and information to stakeholders; and
- promoting CIP as a national research priority.

The Australian Government is also responsible for identifying those elements of critical infrastructure which are federally regulated, support national security and defence, support the continuity of the Australian Government and the delivery of its services, and any additional infrastructure of national importance.

Managed by the Critical Infrastructure Protection Branch of the Australian Government's Attorney-General's Department, the Trusted Information Sharing Network (TISN) is the mechanism which allows governments, industry lead agencies and critical infrastructure owners and operators to share information at a national level on issues such as business continuity and resilience, consequence management, threats and vulnerabilities. The network provides an online forum for Infrastructure Assurance Advisory Groups (IAAGs) representing identified business sectors. These groups are overseen by the Critical Infrastructure Advisory Council (CIAC), which advises Government on a national approach to CIP, priorities and relationships between critical infrastructure sectors. CIAC also has Expert Advisory Groups (EAG) to provide advice on specific areas of interest, as well as Communities of Interest (COI). (refer diagram 1).

CIAC comprises representatives from each of the sector groups, representatives from each state and territory, and relevant Australian Government agencies.

The National Committee on Critical Infrastructure Protection (NCCIP) comprises representatives from the Australian and state and territory governments. This committee is the forum which facilitates the sharing of relevant information between jurisdictions on government critical infrastructure strategies and intentions, ensures complementary approaches and enhances coordination.

The Australian Government has also established the Business Government Advisory Group on National Security (BGAG) to provide senior business leaders with an opportunity to provide input into the strategic direction of Australia's national security policy at Ministerial level. Although the BGAG provides advice on CIP issues, it is not part of the TISN and it addresses a wide range of security issues.

Critical Infrastructure Sectors and Sub-sectors

The NT has embraced the sector approach, consistent with national arrangements, for the management of critical infrastructure. Each sector consists of sub-sectors, with most being interdependent for the provision of their service.

Sector	Sub-sectors
Energy	Gas, Petroleum Fuels, Electricity Generation and Transmission.
Utilities	Water, Waste Water and Waste Management.
Transport	Air, Road, Sea, Rail and Inter-modal (cargo distribution centres).
Communications	Telecommunications (phone, fax, Internet, cable, satellites), Electronic Mass Communications and Postal Services.
Health	Hospitals, Public Health, and Research and Development Laboratories.
Food Supply	Bulk Production, Storage and Distribution.
Finance	Banking, Insurance and Trading Exchanges.
Government Services	Houses of Parliament, Key Government Departments, Emergency Services (Police, Fire, Ambulance, etc).
Icons and Places of Mass Gathering	Commercial Centres, Buildings, Cultural, Sport and Tourism.

Northern Territory Arrangements

NT Critical Infrastructure Protection Coordination Group

The NT Critical Infrastructure Protection Coordination Group (NT CIPCG) is a key element for CIP in the NT. Its purpose is to monitor national strategies and trends for relevance to the NT and to oversee the on-going management of this framework and other directions from government. The NT CIPCG is chaired by the Department of the Chief Minister and NT Police and includes representation from those NT Government agencies that have IAAG membership responsibilities. Other agencies or industry representatives may be requested to provide representation for specific issues. The NT CIPCG is also a conduit for the provision of advice and recommendations to industry sectors and owners and operators of critical infrastructure in relation to trends, alert levels or threat information.

NT Principles

CIP principles have been nationally agreed to ensure cooperation and information sharing between owners and operators who often operate in more than one jurisdiction, regulators, professional bodies, industry associations and governments at all levels. These principles have been adapted for the NT.

- The NT framework will support and complement the national approach to CIP.
- CIP is centred on the need to minimise risks to public health, safety and confidence, ensure the Territory's economic security and ensure the continuity of government and its services.
- The objectives of CIP are to identify critical infrastructure, analyse vulnerability and interdependence, and protect from, and prepare for, all hazards.
- NT CIP arrangements are based on the identification of assets within the Territory (excluding off-shore facilities) which significantly contribute to community wellbeing and the economy.
- As not all critical infrastructure can be protected from all threats, appropriate risk management techniques are used to determine relative criticality (refer to the NT CIP Guidelines), the level of protective security required, and set priorities for the allocation of resources to apply mitigation strategies.
- Government agencies have the responsibility to prepare threat assessments and advise appropriate industry sectors and owners and operators of critical infrastructure.
- The responsibility for managing risk within physical facilities, supply chains, information technologies and communication networks primarily rests with owners and operators.
- CIP needs to be undertaken from an 'all hazards' approach with full consideration of interdependencies between businesses, sectors, jurisdictions and government agencies.
- CIP requires a consistent, cooperative partnership between the owners and operators of critical infrastructure and NT Government agencies.
- The sharing of information relating to threats and vulnerabilities will assist governments, and owners and operators of critical infrastructure to better manage risk.

Engagement Protocols

For the government/business partnership in relation to CIP to be successful, effective engagement is necessary. The NT CIP Guidelines detail how this will be achieved. The engagement mechanisms are as follows:

- an annual forum of owners and operators of critical infrastructure, managed by the NT Government;
- a visit to each NT critical infrastructure owner and operator by the Department of the Chief Minister representative on the CIAC, NT Police (including local police if appropriate) and the government agency representative on the relevant IAAG;
- briefing relevant owners and operators, industry representatives and appropriate government agency staff when a new or revised threat assessment or risk context statement is issued;
- the provision of newsletters and other information of interest or relevance to owners and operators of critical infrastructure, industry representatives and government agencies;
- the provision of advice and information to owners and operators of the issues being considered by the IAAG relevant to their sector or sub-sector; and
- participation in exercises when possible.

NT Critical Infrastructure Boundaries

The whole of the gazetted area of the NT is considered for CIP management, except identified off-shore areas.

For specific off-shore areas, particular arrangements are in place for counter terrorism activities only. In all other matters (such as emergency management) normal procedures apply. Responsibility for counter terrorism prevention, interdiction and response capabilities and activities, including the protection of off-shore oil and gas facilities and the off-shore interdiction of ships, is the responsibility of the Australian Defence Force coordinated through the Australian Government's Border Protection Command. This responsibility applies to areas seaward of the Territorial Sea Baseline (low water mark). The NT retains responsibility for internal waters and within port limits.

Security policies at major airports and ports are dictated in the *Commonwealth Aviation Transport Security Act 2004* and the *Commonwealth Maritime Transport and Offshore Facilities Security Act 2003* respectively. These Acts and their associated regulations are oversighted by Australian Government agencies and require specific plans, preparations and responses by the facilities. Nevertheless, major NT airports and ports are still considered NT critical infrastructure, whether or not they are also identified by national agencies as national critical infrastructure.

Should identified NT critical infrastructure cross the border with an adjoining jurisdiction, the Department of the Chief Minister and NT Police will make appropriate arrangements with that jurisdiction. These will include procedures for information sharing and a coordinated response should it become necessary.

Local Government

The NT CIP Guidelines contain specific responsibilities for local government in relation to critical infrastructure protection.

In addition, the application of this framework recognises the importance of local government in local counter disaster arrangements in bringing together local police, emergency services, major industry, community based representatives and local council/shires to prepare for and manage recovery from emergencies or disasters. While not specific to this CIP Framework, the application of these well practised procedures is consistent with the all hazards approach to business continuity.

NT Critical Infrastructure Incident Management Arrangements

In the event of an incident or emergency involving critical infrastructure, the normal management arrangements relevant to other incidents and emergencies will apply.

Counter disaster, emergency management and consequence management arrangements are in accordance with the *Disasters Act* and the *Northern Territory All Hazards Emergency Management Arrangements*. Recovery operations will be coordinated by the Department of the Chief Minister in accordance with the *Northern Territory Emergency Recovery Management Plan*.

Should the event be a terrorist incident or suspected to be a terrorist incident, the response will be managed by the NT Police in accordance with nationally agreed guidelines.

In cases of emergency or disaster, provisions under the *Essential Goods and Services Act* may apply. The Act allows the control and management of prescribed goods and services during periods of shortage or for other purposes.

Enhancing Preparedness

As part of their normal governance owners and operators of critical infrastructure employ techniques and systems to identify vulnerabilities and plan mitigation or redundancy arrangements accordingly. In the context of maintaining the availability of critical infrastructure the following areas are particularly pertinent and should be considered by owners and operators:

- risk management;
- security planning;
- onsite emergency response planning;
- business continuity planning; and
- communication planning.

Risk Management

The current *Australian and New Zealand Standard for Risk Management* (AS/NZS 4360:2004) is the standard by which critical infrastructure risk management should be assessed. In addition Emergency Management Australia has developed a useful tool, the *Critical Infrastructure Emergency Risk Management and Assurance Handbook* that supports AS/NZS 4360:2004, and which describes the risk management process and assists owners and operators in undertaking the risk management process. The *National Guidelines for protecting Critical Infrastructure from Terrorism* are also relevant (refer to references).

Risk Treatment

When a risk assessment has been completed by owners or operators, an appropriate risk treatment strategy is required. This strategy should encompass all hazards that have been considered, with security being one. Treatment strategies for owners and operators of critical infrastructure will involve security planning, on-site emergency response planning and business continuity planning.

Security planning should be risk based, commensurate with the threat and able to be escalated if required. Security arrangements should provide protection through deterrence, detection, delay and response procedures. Owners and operators should consult with NT Police to ensure security plans can respond to changes in the level of threat. Security plans should be consistent with the Standards Australia *Security Risk Management Handbook* (HB 167:2006).

On-site emergency response plans and procedures must cover all hazards and include issues such as evacuation, fire, shelter, threats (bomb, mail, telephone, etc), suspicious objects (mail, parcels, bags, etc) and internal responsibilities and contacts.

The aim of business continuity planning is to ensure timely resumption and delivery of essential business activities in the event of a major disruption by maintaining the key business resources required to support delivery of those services. Overall business resilience of owners and operators of critical infrastructure should be assessed using the *Business Continuity Management Handbook* (HB 221:2004) developed by Standards Australia.

Communication Planning

Effective protection of critical infrastructure is reliant on a cooperative partnership between owners and operators and government agencies. This is underpinned by effective engagement and communication between them. Agreed contacts with critical infrastructure owners and operators and NT Government agencies (Department of the Chief Minister and NT Police) will be established and maintained.

Review and Evaluation

Owners and operators of critical infrastructure should review, evaluate and exercise their security, on-site emergency response and business continuity plans at least annually to ensure currency and validity. These reviews can be conducted by organisations either within or external to the critical infrastructure.

Glossary

ASIO	Australian Security Intelligence Organisation
BGAG	Business Government Advisory Group
CIAC	Critical Infrastructure Advisory Council
CIP	Critical Infrastructure Protection
CIPMA	Critical Infrastructure Protection Modelling and Analysis Program
COI	Community of Interest
EAG	Expert Advisory Groups
EMA	Emergency Management Australia
IAAG	Infrastructure Assurance Advisory Group
NCCIP	National Committee on Critical Infrastructure Protection
NT	Northern Territory
NT CIPCG	Northern Territory Critical Infrastructure Protection Coordination Group
SCADA	Supervisory Control and Data Acquisition
TISN	Trusted Information Sharing Network

A **risk** is the chance of something happening that will have an impact. A risk rating is determined by the measurement of consequences and likelihood.

A **threat** is a potential source of harm. It is a declaration of an intent to cause harm or the assessment that a hazard may cause harm. Threats can therefore be of a security nature (e.g. a terrorist threat) or a non-security nature such as natural disaster (e.g. cyclone or flood), a global economic downturn or other non-security related event.

References

National Documents

- National Guidelines for Protecting Critical Infrastructure from Terrorism, National Counter Terrorism Committee, 2004
  (available on www.tisn.gov.au)
- Critical Infrastructure Emergency Risk Management and Assurance Handbook, Emergency Management Australia, 2004
  (available on www.ema.gov.au)
- National Approach for the Protection of Places of Mass Gathering from Terrorism, National Counter Terrorism Committee, 2006
  (available on www.tisn.gov.au)
- Infrastructure in the Public Domain: A Guide to Mitigating Security Risks, Australian Government Attorney-General's Department, 2006
  (available on www.tisn.gov.au)
- Good Security Good Business, Australian Government Attorney-General's Department, 2006
  (available on www.tisn.gov.au)

Standards

- AS/NZ 4360:2004 Risk Management, Standards Australia, 2004
  (available on www.tisn.gov.au)
- HB 221:2004 Business Continuity Management Handbook, Standards Australia 2004
  (available on www.standards.org.au)
- HB 167:2006 Security Risk Management Handbook, Standards Australia 2006
  (available on www.standards.org.au)

Northern Territory Legislation and Documents

- Disasters Act
  (available on http://www.nt.gov.au/dcm/legislation/current.html)
- Terrorism (Emergency Powers) Act
  (available on http://www.nt.gov.au/dcm/legislation/current.html)
- Essential Goods and Services Act
  (available on http://www.nt.gov.au/dcm/legislation/current.html)
- Considerations for Owners and Operators of Mass Gatherings, NT Police, 2006
  (available by contacting NT Police – see Contacts)
- Northern Territory All Hazards Emergency Management Arrangements, NT Counter Disaster Council, 2007
  (available on www.pfes.nt.gov.au)
- Northern Territory Emergency Recovery Management Plan, Department of the Chief Minister, 2007
  (available on www.nt.gov.au/dcm)

Contacts

For further information about the framework or critical infrastructure protection in general, contact:

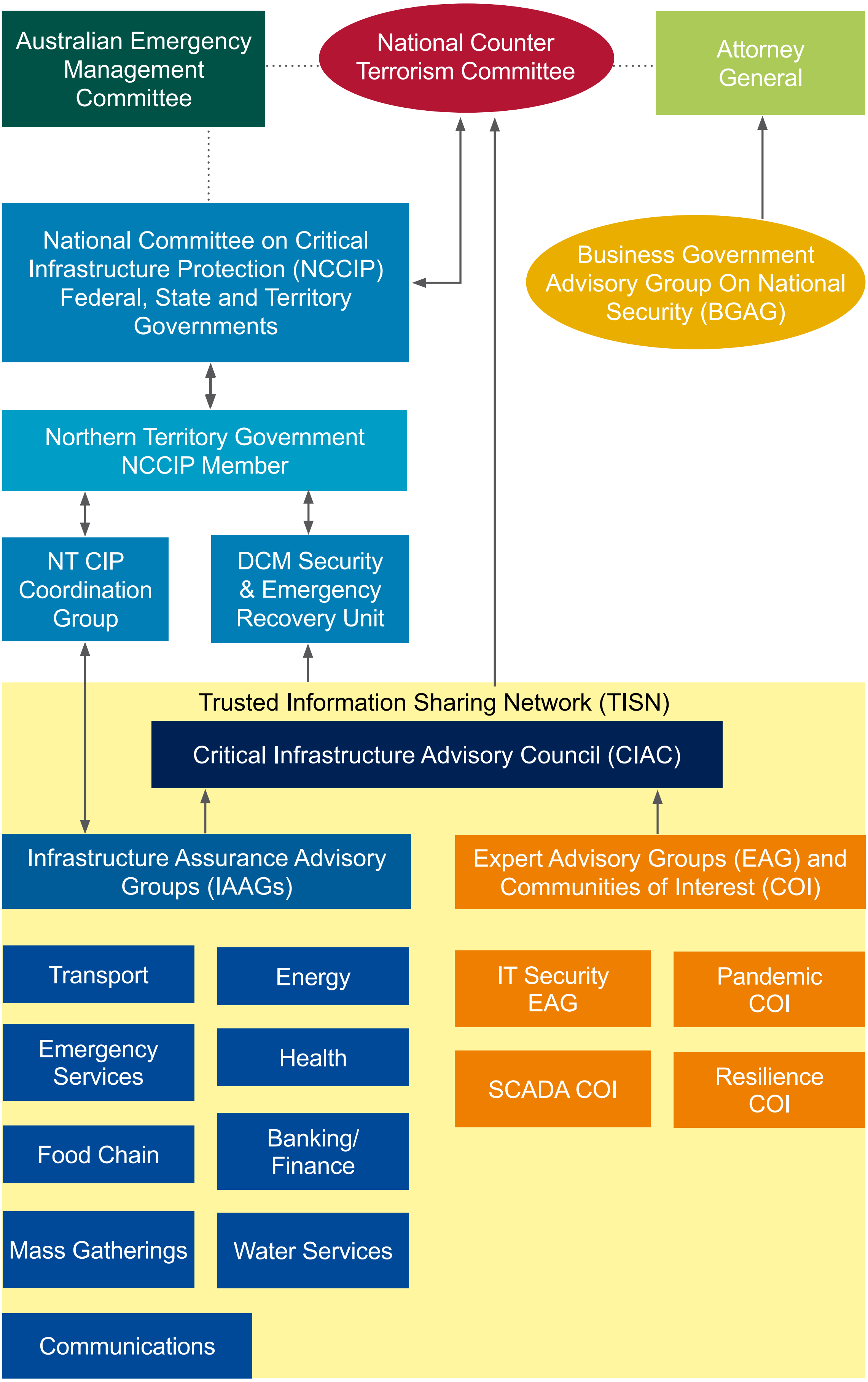
Department of the Chief Minister
Security and Emergency Recovery

Phone:	08 8999 8971 (business hours)
Fax:	08 8999 7402
Email	security.dcm@nt.gov.au

Northern Territory Police
Counter Terrorism and Security Coordination Division

Phone:	08 8901 0301 (business hours)
Fax:	09 8901 0311
Email	ctsecurity@pfes.nt.gov.au

Diagram 1


Australian Emergency Management Committee
National Counter Terrorism Committee
Attorney General
National Committee on Critical Infrastructure Protection (NCCIP) Federal, State and Territory Governments
Business Government Advisory Group On National Security (BGAG)
Northern Territory Government NCCIP Member
NT CIP Coordination Group
DCM Security & Emergency Recovery Unit
Trusted Information Sharing Network (TISN)
Critical Infrastructure Advisory Council (CIAC)
Infrastructure Assurance Advisory Groups (IAAGs)
Expert Advisory Groups (EAG) and Communities of Interest (COI)
Transport
Energy
Emergency Services
Health
Food Chain
Banking/ Finance
Mass Gatherings
Water Services
Communications
IT Security EAG
Pandemic COI
SCADA COI
Resilience COI