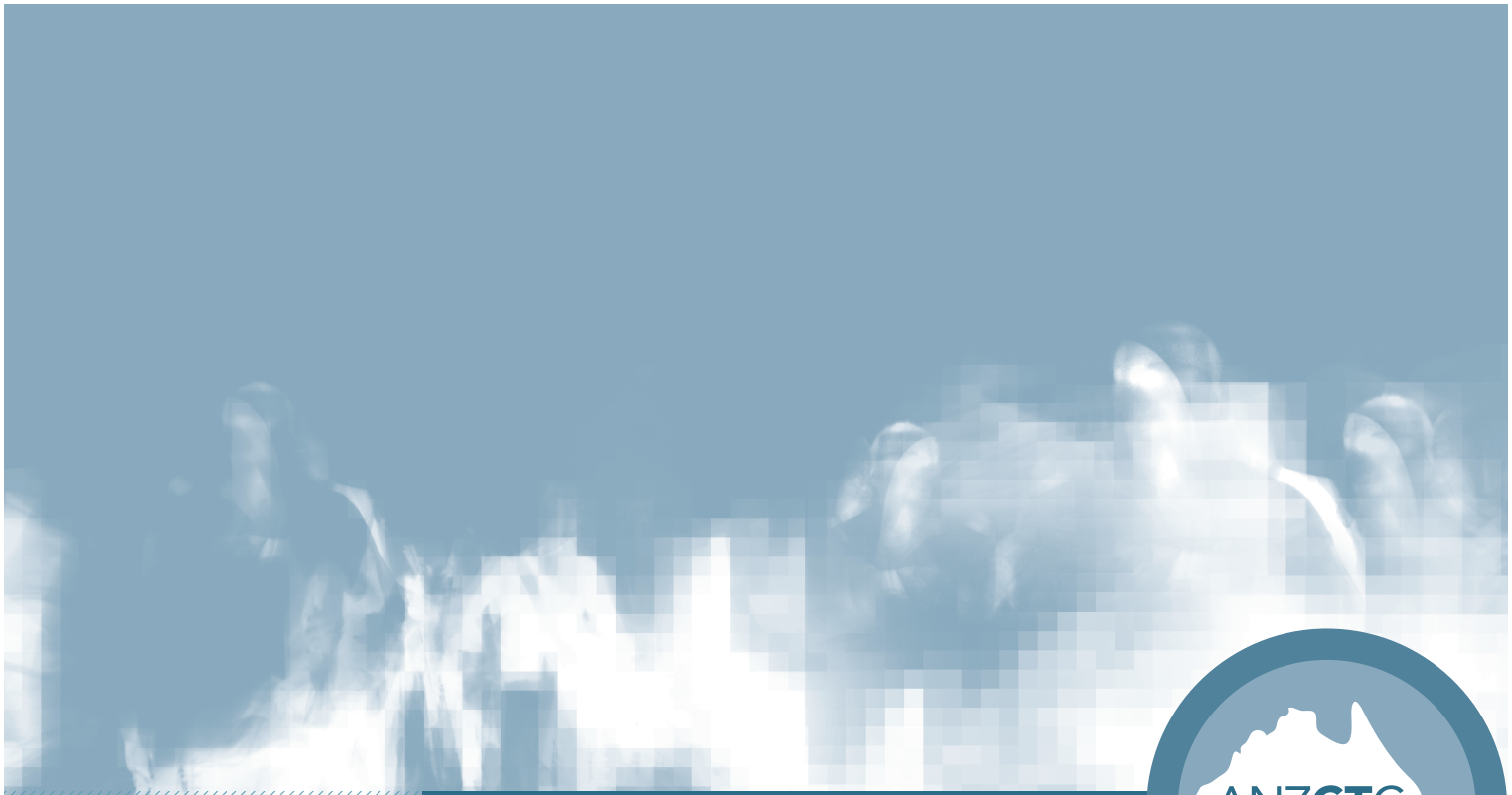

NATIONAL GUIDELINES FOR PROTECTING CRITICAL INFRASTRUCTURE FROM TERRORISM

AUSTRALIA-NEW ZEALAND **COUNTER-TERRORISM** COMMITTEE

NATIONAL GUIDELINES FOR PROTECTING CRITICAL INFRASTRUCTURE FROM TERRORISM

AUSTRALIA-NEW ZEALAND **COUNTER-TERRORISM** COMMITTEE

ISBN: 978-1-925290-42-4 (Print)
ISBN: 978-1-925290-43-1 (Online)

© Commonwealth of Australia 2015

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Commercial and Administrative Law Branch
Attorney-General's Department
3–5 National Cct
BARTON ACT 2600
Email: copyright@ag.gov.au

Contents

1 PURPOSE **2**

2 INTRODUCTION **2**

Definition of critical infrastructure 3

Critical infrastructure sectors 3

3 IDENTIFICATION OF CRITICAL INFRASTRUCTURE **4**

4 AN INTELLIGENCE-LED, RISK INFORMED APPROACH **5**

4.1 Threat assessments 5

4.2 National Terrorism Threat Advisory System 7

4.3 Prevention and preparedness 8

4.4 Response and recovery 10

5 PUBLIC INFORMATION AND MEDIA MANAGEMENT **12**

6 ATTACHMENTS **13**

Attachment 1—Responsibilities 13

Attachment 2—Security measures to consider in relation to changes in the security situation 15

Attachment 3—Useful information 18

1 Purpose

The National Guidelines for Protecting Critical Infrastructure (CI) from Terrorism (the Guidelines) provide a framework for a national, consistent approach on the protection of CI from terrorism for the Australian, State and Territory governments and business. They are designed to aid owners/operators of CI in their discussions with jurisdictions (including the Australian Government) about protecting CI from terrorism. The Guidelines recognise that the treatment of individual CI assets will depend on an assessment of the criticality of the asset in question, the nature of the security environment and the risk profiles for that asset or relevant sector.

2 Introduction

All governments recognise that the threat of terrorism is enduring and requires sustained mitigation efforts. An intelligence-led, risk informed approach is required to develop adequate levels of protective security for Australia's CI, minimal single points of failure, and rapid, tested recovery arrangements.

Although governments have a role in the protection of CI, it is a matter of responsibility and good corporate governance that owners/operators of CI address the security of their assets and continuity of their business. Owners/operators of CI should consider terrorism as one of the hazards in an 'all hazards' risk management approach to their operations. Governments need to work with business to provide sufficient information on which owners/operators can base their decisions. All jurisdictions regularly review their administrative and legislative arrangements to better address the terrorist threat.

For more information on the responsibilities of CI stakeholders, see Attachment 1.

The current national CI protection arrangements focus on protecting CI against the threat of terrorist attack. They are coordinated under the auspices of the Australia-New Zealand CounterTerrorism Committee (ANZCTC), a national body which contributes to the security of Australian and New Zealand communities through coordination of a nation-wide cooperative framework to counter terrorism and its consequences. It comprises representatives from the Australian, State and Territory governments. These Guidelines have been endorsed by all jurisdictions through the ANZCTC.

Terrorist act definition

A 'terrorist act' is an act or threat intended to advance a political, ideological or religious cause by coercing or intimidating an Australian or foreign government or the public, by causing serious harm to people or property, endangering life, creating a serious risk to the health and safety of the public, or seriously disrupting certain types of critical infrastructure, electronic systems or trade.

For more information, refer to the *Criminal Code Act 1995* [Cth]

At the national level, the term Critical Infrastructure Protection (CIP) is used only to describe actions or measures undertaken to mitigate the specific threat of terrorism. Critical Infrastructure Resilience (CIR) is the term used to describe an 'all hazards' approach to CI and includes activities across the spectrum of prevention, preparedness, response and recovery, for hazards including natural disasters, pandemics, negligence, accid ents, criminal activity, computer network attack and terrorism. The Australian Government supports CIR through the Trusted Information Sharing Network (TISN) for CIR and the Critical Infrastructure Advisory Council (CIAC).

These Guidelines focus on CIP arrangements.

These Guidelines support, acknowledge and complement the:

- key responsibility of owners/operators in protecting CI
- *Critical Infrastructure Protection Risk Management Framework for the Identification and Prioritisation of Critical Infrastructure*
- National Counter-Terrorism Plan
- National Counter-Terrorism Handbook (a classified document setting out internal government arrangements)
- *Australian Government Critical Infrastructure Resilience Strategy*
- relevant Australian standards
- relevant legislative and international obligations that may apply to specific industries such as transport or offshore oil and gas production.

Definition of critical infrastructure

At the national level, CI is defined as, *'those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security'*.

'Significant' in the context of this definition is defined as an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia's international competitiveness, or impedes the continuity of government and its services.

Critical infrastructure sectors

CI extends across many sectors of the economy, including banking and finance, transport, energy, water, health, food and grocery and communications. It also includes key government services, manufacturing and supply chains.

The ubiquitous nature of CI and our collective reliance on it means that protecting and ensuring its continuity is essential to the nation's economic prosperity, national security and social wellbeing. The continuity of supply of any one component of CI is often dependent on the availability of other CI. For example, the telecommunications sector is dependent on the supply of electricity and food supply is dependent on transport.

3 Identification of critical infrastructure

The Australian, State and Territory governments work with business to identify CI, including interdependencies between different elements of CI within their respective jurisdictions, and to keep this information current. State and Territory governments identify CI within their respective jurisdictions critical to their mission. The Australian Government identifies those elements of our CI which are federally regulated, support national security and defence, the continuity of government, the delivery of its services and any infrastructure of additional national importance.

The Australian Government has produced the *Critical Infrastructure Protection Risk Management Framework for the Identification and Prioritisation of Critical Infrastructure*. This Framework, accepted by the ANZCTC, identifies and prioritises CI in terms of criticality from a national perspective. This is done by identifying those CI assets/facilities which are nationally critical (as opposed to critical from a State/Territory perspective), followed by determining the level of criticality of those assets/facilities.

While the Framework may have some applicability at the State and Territory level, it does not negate the requirement to develop tailored risk management assessments and strategies for individual CI sectors or assets.

Criticality levels

vital—alternative services and/or facilities cannot be provided nationally or by States or Territories. Loss or compromise will result in abandonment or long term cessation of the asset

major—if services and/or facilities are severely disrupted, major restrictions will apply and the service/facility will require national assistance

significant—services and/or facilities will be available but with some restrictions and/or less responsiveness and/or capacity compared to normal operation. The service may be provided within the State or Territory but reliance may also be placed on other States or Territories

low—services and/or facilities can be provided within the State, Territory or nationally with no loss of functionality

unknown—insufficient data is available for evaluation.

4 An intelligence-led, risk informed approach

Australia relies upon a strong intelligence-led, prevention and preparedness regime to support our counter-terrorism arrangements. This approach encompasses targeted prevention and preparedness measures based on risk management principles and maintaining capabilities to manage various types of terrorist threats, attacks and their consequences. Intelligence and criminal investigations are ongoing and carried out by the Australian Security Intelligence Organisation (ASIO) and law enforcement agencies in order to prevent, respond to, and investigate terrorist threats and attacks in Australia.

Communicating CI terrorist threat information to owners/operators of CI quickly and appropriately enables those owners and operators to make better informed risk management decisions and undertake effective risk mitigation measures, in response to the threat environment. The responsibility for managing risk to physical facilities, supply chains, information technologies and communication networks primarily rests with owners/operators. The sharing of intelligence and other information relating to threats and vulnerabilities from terrorism will assist owners/operators of CI to better manage risk.

4.1 Threat assessments

ASIO is the national security intelligence body and the authority for assessing threats to security. ASIO's threat assessments indicate levels of threat against, and the probable nature of, terrorism, politically motivated violence, espionage, foreign interference, violent protest and sabotage. Threat assessments can be produced for specific events, facilities, people or sectors and are separate from the National Terrorism Threat Level.

ASIO distributes threat assessments to relevant Australian Government agencies, State and Territory governments, the Australian Federal Police, and State and Territory police. Owners/operators of CI are also provided with a copy of the national terrorism threat assessment used to determine the threat level in Australia. This information should be used by owners/operators in their preparation and planning processes. ASIO provides threat advice to the private sector and to government agencies via the Business Liaison Unit.

Where there is particular urgency, ASIO will contact State and Territory police and other relevant organisations, including owners/operators of CI, as soon as possible and in advance of the dispatch of the written advice.

While ASIO threat assessments consider the intent and capability of terrorists, they do not assess the vulnerability or adequacy of existing security of CI. Subsequently, threat assessments should be used in security risk analysis to determine the requirement and type of mitigation measures for any one CI facility.

Risk analysis, when applied in accordance with HB167:2006 Security risk management, uses factors of threat combined with vulnerability to better determine the actual likelihood of the event occurring at a CI facility.

Threat assessments

It is important for owners/operators of CI to note that the terrorism threat level specifically for their sector may be different than the National Terrorism Threat Level.

Example

- the National Terrorism Threat Level may indicate that a terrorist attack is PROBABLE
- against this background, intelligence could be received about a threat to a particular CI asset/sector in a particular region of Australia, such as electricity generation in Victoria
- this intelligence may not be sufficient to increase the National Terrorism Threat Level, but it may result in an increase in the terrorism threat level for the specific CI threat assessment to PROBABLE or EXPECTED
- in this scenario, owners/operators of the relevant CI should increase their security measures accordingly, in consultation with relevant law enforcement agencies
- while there is no specific threat for other Australian electricity generation infrastructure, the owners/operators of that infrastructure would also be advised of the threat
- they may consider adopting additional security measures as a precaution.

State and Territory police intelligence and information

State and Territory police also develop security intelligence and protective security information to combat terrorism and politically motivated violence. State and Territory police advise owners/operators of CI on the national and local security threat context. This local security threat context, combined with relevant threat assessments, provides the key information to guide owners and operators of CI in the development of protective security measures and on-site emergency plans.

Risk assessment

ISO 31000:2009 provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organisation, and is the standard by which all CI will be assessed to assist with the review of risk management plans for prevention (including security), preparedness, response and recovery. ISO 31000:2009 defines risk as a combination of likelihood and consequence. HB167:2006 Security risk management should also be referenced as a prescriptive guide to managing security risk in context of threat, vulnerability and criticality.

In accordance with ISO 31000:2009, it is necessary to consider the strategic context for actual and potential threats. Any specific threat and vulnerability analyses for the CI and/or sector should be incorporated into the risk assessment.

Jurisdictions have addressed risk assessment with owners/operators of CI in various ways, although the following key elements are common:

- identification of essential or key elements within a CI asset (critical nodes)
- consideration of whether the CI is a producer of products that could be used by a terrorist
- identification of possible threats
- determination of risks that require/do not require treatment
- means by which an attack could be mounted
- vulnerability assessment covering personnel and the site
- consequence levels, and
- off-site interdependencies.

All risk assessments should be reviewed to ensure changing circumstances relating to the risk(s), the business, and/or the community have not altered risk levels or priorities, and therefore the treatment strategies. In some industries, such as transport and off-shore oil and gas production, this matter is covered by regulations.

4.2 National Terrorism Threat Advisory System

The National Terrorism Threat Advisory System informs Australians about the likelihood of an act of terrorism occurring in Australia in broad terms to help guide national preparation and planning. When the alert level is elevated, additional precautions are required. Information on the relevance of the national threat advisory to the local security context is available from State and Territory police.

The National Terrorism Threat Advisory System comprises: the National Terrorism Threat Level a five tier scale (Chart 1)—that will be made public; and an accompanying public statement (or narrative) which provides further information such as the nature of the terrorist threat facing Australia and our interests. The purpose of the National Terrorism Threat Advisory System is to inform Australians about the likelihood of an act of terrorism occurring in Australia in broad terms. The National Terrorism Threat Level is derived from assessed intelligence by the National Threat Assessment Centre, housed within ASIO. ASIO's classified assessment of the threat informs the unclassified advice of the threat level, and accompanying public narrative.

The National Terrorism Threat Advisory System will also help ensure that all necessary national preparedness and planning is undertaken by governments, and that an appropriate level of precaution and vigilance is maintained to minimise the risk of a terrorist incident. The National Terrorism Threat Advisory System applies on a national basis—across all States and Territories. Changes or updates to the National Terrorism Threat Level will be informed by a classified ASIO Threat Assessment provided to relevant Australian, State and Territory governments and their agencies. This detailed threat assessment will not be publically released as it is likely to contain specific intelligence which, if released publically, could compromise operations.

The Australian Government will explain, through an unclassified public narrative, why a change in the National Terrorism Threat Level has occurred. This narrative will be attached to the classified threat assessment, enabling governments to add jurisdiction-specific talking points or comments to the narrative as required. The narrative will provide as much specific information about the nature of the threat as is possible. The public narrative will contain information deemed sufficient to enable a behavioural response by individuals. The degree of specificity in the narrative will increase in-line with the Threat Level. The Australian Government will regularly review the security environment and will make adjustments to the National Terrorism Threat Level and/or the public narrative as required.

CHART 1

Relevance to CI protective security

CI owners and operators are encouraged to adopt an intelligence led, risk management based approach to protective security planning and to develop protective security contingency plans and emergency response arrangements based on a security risk assessment that incorporates the current security context. While CI owners and operators should consider any changes to the National Terrorism Threat Advisory System, these changes may have no specific implications for some or all CI. Any adjustments to CI protective security arrangements should not rely solely on changes to the National Terrorism Threat Advisory System, but instead should primarily be based on an assessment of the local security situation, in liaison with local law enforcement agencies. Further information on generic security measures to consider in relation to changes in the security situation is at Attachment 2.

4.3 Prevention and preparedness

Intelligence and information management

Governments and business recognise the need to share intelligence and information on threats and vulnerabilities and appropriate measures and strategies to mitigate risk. From time to time, specific risks or threats may emerge that require an immediate response. On these occasions, a well-coordinated but more operationally focused response will be required from governments and business.

Responsibility for the distribution of relevant intelligence and information is summarised below.

- ASIO has responsibility to provide relevant threat information to the appropriate Australian Government departments, the Australian Federal Police (AFP) and State and Territory police.
- State and Territory police liaise with owners/operators of CI, in accordance with jurisdictional arrangements, to provide information on the national and localised security threat context. Police will communicate directly with owners/operators of CI where there is an imminent and specific threat and will coordinate the operational response. Police also gather and disseminate intelligence to relevant agencies as required and appropriate.
- State and Territory governments liaise with owners/operators of CI, in accordance with jurisdictional arrangements, to promote the harmonisation of prevention and preparedness, response and recovery plans, and procedures between government and owners/operators of CI.
- The owners/operators of CI are expected to provide adequate security of their assets, including staff, and pass information to the police on incidents and suspicious activities such as hoaxes/threats, unusual purchases or thefts, unusual training, or apparent surveillance.

It is important that owners/operators of CI have plans to protect their infrastructure and recover from an incident. As discussed in the risk assessment section, these plans need to consider relevant risks and how to respond to any changes in these risks. A guide to the types of security measures that could be considered by owners/operators of CI in response to changing terrorist threat is provided at Attachment 2. This is a generic guide and it is expected that owners/operators of CI will develop their own model that reflects the nature of their infrastructure and the local security context. Many owners/operators of CI already have such plans.

Preventive investigation

The *Criminal Code Act 1995* (Cth) criminalises a range of terrorist activity, including preparatory and support activity, which allows suspected terrorists to be investigated, arrested and charged with serious offences before they can commit their intended attack. Terrorists in their preparatory activity may also commit other offences, such as relating to the acquisition of arms and explosives, for which they could be charged under State and Territory law.

All Australian police forces maintain the capabilities to investigate suspect terrorists. They work collaboratively with other law enforcement and intelligence agencies through Joint Counter Terrorism Teams (JCTTs) in each capital city to build briefs of evidence permitting such preventive arrests where possible.

It is important that owners/operators of CI maintain effective security arrangements to maximise the likelihood that terrorist preparatory activity, such as site reconnaissance, is identified quickly. Any such suspicious activity should be reported to the police or the National Security Hotline on 1800 1234 00 or hotline@nationalsecurity.gov.au immediately.

Planning and exercises

It is important that owners/operators of CI fully understand the government response arrangements in the area and jurisdiction within which the CI is located. It is also imperative that response agencies are familiar with the characteristics of CI within their jurisdictions and the security and related plans and arrangements of the owners/operators of the CI.

Essential plans that owners/operators of CI require are a business continuity plan, security plan and an on-site emergency plan linked to local emergency plans and arrangements. In some cases these plans may already exist, but without considering terrorism. Security plans should address the full range of issues including, but not limited to access control arrangements, identification of authorised personnel, response procedures for breaches, personnel security vetting arrangements, security arrangements for visitors and deliveries by suppliers, and protection of information systems. Once in place these plans need to be audited, exercised and reviewed. This may involve industry regulators.

Australia-New Zealand National Counter-Terrorism Committee exercises

The ANZCTC conducts a range of counter-terrorism exercises each year in order to enhance national counter-terrorism capability and interoperability across and between all levels of government and their agencies. The exercises:

- test current plans and arrangements to identify capability gaps
- validate and confirm levels of capability achievement
- validate training and inform training requirements
- develop and maintain interoperability
- inform the review and development of security legislation, policy, plans, arrangements and processes
- maintain consistency in the application of the national counter-terrorism arrangements.

Training and development

State and Territory governments and a number of private institutions/organisations conduct crisis and consequence training.

In addition, the Australian Emergency Management Institute (AEMI) provides a range of programs that may be relevant to professionals working in business and government in protecting CI from terrorism.

Interdependencies

All CI is dependent to some extent on the continued supply of energy, water, information systems, transport, telecommunications and emergency services. The degree and complexity of interdependency varies between services. The Australian Government, in conjunction with the States and Territories, will identify CI and over time provide information on interdependencies.

Interdependencies also include the supply chain to the CI, so if a relevant terrorism threat level increases, suppliers need to be aware of the increase and the implications for supply arrangements. Owners/operators of CI also need to be aware of other infrastructure or facilities that might be a target and are physically adjacent to their infrastructure.

4.4 Response and recovery

Response and recovery activities do not occur in a linear fashion and are likely to occur concurrently in a complex operating environment.

Response

Response in the counter-terrorism context relates to actions taken immediately before, during, and immediately after a terrorist act or threatened terrorist act. These actions are designed to:

- prevent or minimise loss of life, injury, damage to property and damage or disruption to infrastructure
- facilitate investigations into the threat or act, including the prosecution of offenders
- ensure that people affected by the threat or act are given immediate relief and support.

State and Territory governments and their agencies have operational responsibility for dealing with a terrorist incident or act in their jurisdiction. Where an incident or act is suspected to be terrorism-related, police agencies exercise overall command and control of the response. Australian Government agencies will support State and Territory governments.

If a State or Territory judges that an incident is/may be terrorism-related, it will contact the Australian Government Crisis Coordination Centre, ASIO and AFP. Coordination between governments in the event of a terrorist attack is detailed in the National Counter-Terrorism Handbook.

In any response, the objectives are to:

- maintain community safety
- save lives
- prevent injury
- protect property
- mitigate loss
- investigate the incident
- recover from the incident.

Where an incident involves a CI asset, crisis and consequence managers at each level need to have access to appropriate expertise/authority and be familiar with the infrastructure concerned in the incident.

At the incident site this would mean a person with:

- access to all parts of the infrastructure
- the authority to contact the executive levels of the owners/operators of the CI
- access to technical expertise
- an understanding of the implications of actions taken on-site.

At the State/Territory management level, access will be required to the executive levels of the infrastructure owners/operators, as decisions may be required that have significant implications for infrastructure owners/operators.

Recovery

Recovery is the coordinated process of supporting disaster-affected communities in the reconstruction of the physical infrastructure and the restoration of emotional, social, economic and physical wellbeing.

Recovery is a significant element of counter-terrorism policy and practice, requiring the collaboration of government, business, non-government organisations and the community. Recovery activities following a terrorist act are likely to be complex and require integrated and sustained coordination for an extended period. A terrorist act poses unique consequences that are likely to include impacts on public confidence, individuals and businesses beyond the geographic place of the incident.

State and Territory governments are operationally responsible for recovery from a terrorist act. The principal goals for recovery, including recovery from a terrorist act are:

- the re-establishment of essential services
- restoration of public confidence
- delivery of psycho-social and health support
- reconstruction of physical infrastructure
- restoration of the economic and natural environments.

However, owners/operators of CI are primarily responsible, as a part of their corporate governance, for the security of their assets and the continuity of their businesses.

Governments will continue to encourage owners/operators of CI to undertake a risk management process, and prepare and exercise business continuity planning to –in the event of a major disruption—facilitate the timely resumption of essential business activities.

The *Terrorism Insurance Act 2003* (Cth) is aimed specifically at mitigating any economic impact resulting from the failure of the private insurance market to provide available and affordable terrorism insurance for certain commercial property and infrastructure. Established Australian, State and Territory government relief and recovery funding arrangements could also be applied in managing the impacts on business following a terrorist act, should governments determine this is necessary.

Criminal investigation

At the onset of a counter-terrorism investigation, agreements between relevant police commissioners provide and establish a nationally consistent governance framework for the strategic management of counter-terrorism operations in the relevant jurisdiction. The JCTTs, comprising the AFP, State and Territory law enforcement agencies and relevant intelligence agencies, provide a flexible and adaptive terrorism investigative resource. In response to an incident that could be a terrorist act, a major investigation will be initiated. Agencies will collaborate to establish an agreed reporting framework, investigative structures and disciplines as determined by the circumstances and by the jurisdiction.

The senior investigating officer must ensure that all relevant information and evidence acquired in the course of the investigation is managed in accordance with agreed investigative arrangements. Some information, by its nature, needs to be kept confidential by investigators during and after the investigation, subject to the possible use of such information in a coroner's inquest or other judicial process.

5 Public information and media management

One of the key aims of terrorism is to generate fear and insecurity within a community and undermine public confidence in government and national security systems and organisations. There is an ongoing role for all national security related agencies to ensure that information and media activities work to:

- improve the public's understanding of Australia's national security arrangements
- generate confidence in Australia's ability to investigate and respond to any terrorism threat or activity
- create public trust that governments and national security agencies are open and accountable and will release all information possible within the confines of operational and security considerations.

In the event of a terrorist incident, it is paramount that a common message is provided by all jurisdictions and owners/operators. Coordination of public information in the States and Territories will be in accordance with their standing arrangements and may vary across jurisdictions. If a terrorist incident/issue involves business or non-government organisations, appropriate steps should be taken by the owners/operators of CI to consult and coordinate with all relevant stakeholders, according to Australian Government and State/Territory standing arrangements.

Jurisdictions, owners of CI and relevant peak business organisations should endeavour to develop coordinated media management arrangements that can be activated in the event of an incident and recognise any statutory responsibilities of the CI owners/operators.

The Commonwealth Attorney-General's Department media team acts as a central hub for sharing public information with States and Territories and other relevant Commonwealth agencies during a national security incident.

General public information on CIP will be available on the National Security website www.nationalsecurity.gov.au and the TISN website www.tisn.gov.au.

For further information contact media@ag.gov.au.

6 Attachments

Attachment 1—Responsibilities

Owners/operators of CI

Owners/operators of CI are ultimately responsible for determining and discharging their own legal obligations and managing the risks to their operations that might have a material, financial, legal or reputational impact on the organisation, or harm staff, customers or other parties. Owners/operators do this through appropriate risk management practice including the development and review of business continuity plans, and the provision of adequate security for their assets.

Governments expect that owners/operators should:

- maintain an awareness of their operating environment
- provide adequate security for their assets, based on threat and risk
- actively apply risk management techniques to their planning processes
- conduct regular reviews of risk assessments and security, emergency and contingency plans
- report any incidents or suspicious activity to State or Territory police
- develop and regularly review business continuity plans, including identifying interdependencies
- conduct training and exercise their security, emergency and contingency plans
- participate in government exercises to assist in harmonising prevention, response and recovery arrangements with relevant controlling agencies.

While assistance may be available to perform these functions, governments' expectations are that owners/operators of CI have the primary responsibility for discharging these functions.

Australian Government

While the majority of CI in Australia is owned or operated by the private sector and the States and Territories, the Australian Government has a broad range of roles, responsibilities and interests in the protection of CI.

The Australian Government:

- identifies national CI and develops and maintains a database of national CI
- works closely with State and Territory governments and owners/operators to identify CI that, if disrupted or destroyed, could have significant multi-jurisdictional or national impacts
- works closely with security regulated aviation, air cargo, maritime and offshore oil and gas industry participants to ensure they meet the preventive security regulatory requirements of the relevant Australian Government legislation that seeks to safeguard against unlawful interference with aviation, maritime and offshore oil and gas infrastructure
- in consultation with State and Territory governments, shares information with owners/operators of CI, to build capacity to counter terrorism
- liaises with overseas governments on CIP issues
- promotes CIP as a national research priority.

Australian Security Intelligence Organisation (ASIO)

ASIO:

- is the primary source of threat advice in relation to terrorism, politically motivated violence, espionage, foreign interference, violent protest and sabotage which is provided where appropriate to Federal, State and Territory police, owners/operators of CI and other relevant stakeholders
- will liaise with Federal, State and Territory police, owners and operators of CI and other relevant stakeholders, where there is knowledge of a specific and imminent threat

- conducts Protective Security Risk Reviews of government owned CI rated as nationally vital and, where requested, may undertake similar reviews for privately owned nationally vital CI on a cost recovery basis
- supports the Business Liaison Unit (BLU), which provides an interface between Australian business and ASIO. The BLU aims to ensure that owners/operators of CI can access timely ASIO information on matters affecting the security of the assets for which they are responsible.

Australian Federal Police (AFP)

The AFP enforces Australian criminal law and protects Australian Government and national interests from crime. The AFP is the Australian Government's primary law enforcement body and provides services to assist in the prevention and investigation of crime in relation to Australian interests both in Australia and overseas.

The AFP:

- protects Australian Government CI and essential Australian Government services, such as nominated Australian Defence Force sites, Parliament House and the Australian Nuclear Science and Technology Organisation (ANSTO)
- in partnership with State and Territory police , other law enforcement agencies and intelligence agencies in JCTTs, conduct criminal investigations with the intention of disrupting terrorism and/or bringing criminal prosecutions for breaches of terrorism legislation. gathers and disseminates intelligence to relevant agencies.

State and Territory governments

State and Territory governments and their agencies assist owners/operators of CI with prevention, response and recovery planning, and operations in their jurisdictions. States and Territories have a complex set of roles, responsibilities and interests in critical infrastructure protection.

State and Territory governments:

- identify and maintain a database of CI in their jurisdictions
- provide guidance to owners/operators in developing relevant security, emergency and contingency plans and capabilities to protect CI and ensure continuity of service
- harmonise prevention, response and recovery plans and arrangements between government and owners/operators.

State and Territory police

State and Territory police have operational responsibility for preventing and responding to acts of terrorism and investigate terrorist activity, threats and incidents.

State and Territory police:

- assist in the provision of protective security guidance (as deemed appropriate by the respective police service/force) to owners/operators of CI and develop protective security strategies to counter terrorism
- advise owners/operators of CI on the national and local security threat context, in accordance with jurisdictional arrangements
- communicate directly with owners/operators of CI where there is an imminent and specific threat and coordinate the operational response
- establish and maintain liaison with owners/operators of CI in accordance with jurisdictional arrangements
- gather and disseminate intelligence to relevant agencies
- support and participate in exercises involving CI.

Attachment 2—Security measures to consider in relation to changes in the security situation

The following table provides some generic examples of security measures that could be considered by owners/operators of CI in relation to changes in the security situation, where such changes have relevance to their infrastructure or location. These security measures assume that protective security, on-site emergency and business continuity plans and arrangements are in place, including an ability to increase security measures as required. It is expected that individual contingency measures may be developed separately for specific infrastructure sectors and that owners/operators of CI would consult with State and Territory police and relevant government agencies when considering implementing new security measures.

Protective security measures and on-site emergency planning and preparedness will continue to be guided by risk assessments incorporating:

- specific information on the terrorism threat, tailored to the individual industry sector, in the form of industry sector terrorism threat assessments and risk context statements
- contextual information and guidance from State and Territory police.

The National Terrorism Threat Advisory System remains primarily a public information tool that enables governments and the Australian public to discuss the risk of terrorism in broad terms. Although owners/operators of CI should consider any changes to this system, these changes may have no specific implications for some or all CI owners/operators.

An increase in a terrorism threat level will be conveyed to the relevant CI owners/operators in a timely manner to assist them to mitigate the increased risks. However, it should be noted that terrorism threat assessments take time to develop and, depending on the situation, changes to terrorism threat levels and the National Terrorism Threat Level may not occur quickly. Owners/operators of CI should monitor their security environment and, if they consider their risks are escalating, take measures to mitigate these risks including increasing their protective security arrangements. Where practicable this should occur in consultation with State and Territory police, in accordance with jurisdictional arrangements.

These security measures should be considered in conjunction with the section on prevention and preparedness.

SECURITY SITUATION	SECURITY CONSIDERATIONS
Terrorist attack is not **expected**	Identify the risks associated with the normal business operating environment, for example criminal activity, natural disasters and accidents Ensure a security audit is undertaken and security plans are developed which include: • procedures are in place to report any unusual activity or phone calls to police • after-hours contact details of key personnel and a procedure to ensure that police have access to the contact details • training staff, including contractors • develop facility bomb threat and evacuation procedures • designation of security controlled areas • implement effective access and identification controls, and • cleaning up facilities so they are easier to search and monitor • establish and communicate a risk management philosophy including the development of a risk management plan that articulates the level of acceptable risk, beyond which risk must be managed • ensure a business continuity plan has been developed • comply with State and Territory regulations in relation to dangerous goods • have the necessary systems, plans and processes in place to respond to increased levels of risk or threats.
Terrorist attack is **possible**	Includes considerations if an attack is possible, but **not expected**, plus: • ensure all staff, including contractors are aware of the increased risk, particularly those with key responsibilities • review delivery arrangements from suppliers • reinforce security practices and policies • check warning and evacuation procedures • tighten access controls for people and vehicles, e.g. all visitors escorted • identification checks on entry and exit points • review location of, and access to, external rubbish skips, storage containers etc • review buildings and activities in adjacent buildings • have the necessary systems, plans and processes in place to respond to increased levels of risk or threats • ensure the business continuity plan has been tested and apparent shortfalls rectified • detect and respond to security breaches within 48 hours.

SECURITY SITUATION	SECURITY CONSIDERATIONS
Terrorist attack is **probable**	Includes considerations if an attack is **possible**, plus: • ensure all staff, including contractors are aware of the increased risk and measures being implemented • review delivery arrangements from suppliers • compulsory identification of staff, suppliers and visitors at all times • activate operations centre as required and consider preliminary activation of the business continuity plan • review response procedures for suspicious articles being found • screening of packages, mail deliveries and external deliveries to facility • facilitate closer liaison with emergency services • have the necessary systems, plans and processes in place to respond to increased levels of risk or threats • detect and respond to security breaches within 24 hours • increase vigilance using existing resources for suspicious people, items or vehicles eg check facility each 24 hour period • establish contact with police.
Terrorist attack is **expected**	Includes considerations if an attack is **probable**, plus: • ensure all staff, including contractors are aware of the increased risk and measures being implemented • review delivery arrangements from suppliers • consider service alteration • deploy resources to provide constant monitoring and guarding • implement perimeter security and restrict parking in the near vicinity • detect security breaches within 12 hours. • heightened vigilance for unattended vehicles etc—eg check facility every 12 hours • deploy additional security resources, particularly on entry/exit points.
Terrorist attack is **certain**	Includes considerations if an attack is **expected**, plus: • continuous patrols of critical nodes and points of vulnerability • restrict access to essential personnel only • activate operations centre on a 24/7 basis • activate the business continuity plan • detect and respond to security breaches as soon as possible.

Attachment 3—Useful information

NATIONAL CONTACT INFORMATION

In the event of an emergency (police, ambulance, fire)	000
To report possible signs of terrorism National Security Hotline for TTY users: Email:	 1800 1234 00 1800 234 889 hotline@nationalsecurity.gov.au
Crime Stoppers	1800 333 000
Australian Federal Police AFP Hotline (after hours contact) urgent police assistance at major Australian airports	www.afp.gov.au/policing 1800 813 784 131 237 (131 AFP)

FURTHER INFORMATION

National Security website	www.nationalsecurity.gov.au
Emergency management section of the Attorney-General's Department website	www.ag.gov.au/emergencymanagement
Trusted Information Sharing Network	www.tisn.gov.au
Australian Security Intelligence Organisation (ASIO)	www.asio.gov.au

New South Wales

secureNSW	www.secure.nsw.gov.au

Northern Territory

secureNT	www.securent.nt.gov.au

Queensland

Safeguarding Queensland	www.safeguarding.qld.gov.au

South Australia

South Australia Police Critical Infrastructure Support Group	sapol.sacis@police.sa.gov.au

Tasmania

Special Response and Counter-Terrorism Unit	www.alert.tas.gov.au/prepare/Pages/Terrorism.aspx

Victoria

Emergency Victoria	www.emergency.vic.gov.au

Western Australia

Office of State Security and Emergency Coordination	www.ossec.dpc.wa.gov.au

Australian Capital Territory

ACT Emergency Services Agency	www.esa.act.gov.au

RELEVANT STANDARDS

Website: www.standards.org.au

AS/NZS ISO 31000:2009 Australian/New Zealand Standard Risk management—Principles and guidelines	HB221: 2004 Standards Australia Handbook Business Continuity Management
AS 3745-2002/Amdt 1-2004 Emergency Control Organisation and Procedures for Buildings, Structures and Workplaces	HB 167:2006 Standards Australia Handbook Security risk management
HB 231: 2004 Standards Australia Handbook Information Security Risk Management Guidelines	HB 292-2006 Standards Australia Handbook A Practitioner's Guide to Business Continuity Management

3278