Resilient infrastructure

Issue 02 - Autumn 2012
The Resilient infrastructure magazine is one of the many initiatives that Transport and Main Roads has implemented to facilitate the sharing of information with program stakeholders and promote awareness of security issues that are relevant to Queensland’s transport and critical infrastructure owners and operators.

We trust that you will find this publication informative and useful in your overall risk mitigation and business resilience activities. We also encourage your comments, suggestions and contributions for future editions of Resilient infrastructure.
Contents

Feature articles

4 Security arrangements at the Port of Brisbane
With over 2400 vessel calls each year, the task of protecting Australia’s third largest cargo port is complex and challenging

11 Project feature
Advanced surveillance to protect critical infrastructure

Regulars

6 Agency information

10 Exercising
Transport Security Branch conducts Transport and Main Roads’ largest counter-terrorism exercise

13 Training information
Protective Security Training Centre and ASIO T4 Security Practitioner Course

15 Research information
Exploring the development of critical infrastructure protection arrangements in Australia: changing concepts and definitions

Upcoming events

18 2012 Critical Infrastructure Protection Forum
An informative look at some of the key principles underpinning protective security
The Port of Brisbane Security Services team works 24 hours a day, seven days a week, covering both landside and waterside assets.

Case study: cruise ships

In 2012, over 120 cruise ship visits are scheduled for Brisbane. While most people are aware of the immense logistical task of processing thousands of crew and passengers, and tonnes of supplies and luggage, many may not realise what else goes on behind the scenes. Here’s how a typical cruise ship visit to the Portside Terminal pans out for the port’s security team in a 12-hour shift.

0400 hours
The day starts with a security briefing and vessel preparation, before an inspection of the berth is conducted by the port’s patrol vessel, Port Watch 01. The vessel is typically manned by a coxswain as well as a Maritime Security Guard.

0430 hours
Port Watch 01 joins the cruise ship at the mouth of the river and escorts it up the river to Portside.

The escort provides both a security and safety element for the cruise ship and other small craft using the river during the transit of this large vessel.

0530 hours
Port Watch 01 conducts a security clearance of the berth and once the vessel berths a 'waterside restricted zone' is activated. The waterside restricted zone is a maritime security zone activated in accordance with the Maritime Transport and Offshore Facilities Act 2003.

Landside security service providers at the Portside Terminal are responsible for the activation of landside restricted zones, access control procedures, and screening services.

The Port of Brisbane is Queensland’s largest general cargo port and the third busiest container port in Australia. With over 2400 vessel calls each year, the task of protecting this critical piece of infrastructure is both complex and challenging.
0630 hours
Security Coordinators board the cruise ship to sign a Declaration of Security agreement covering waterside security services.

0700 hours
The Maritime Security Officer on board Port Watch 01 conducts a security clearance of the cruise ship’s bunker barge crew, checks paperwork to ensure ship security clearances have been completed, and authorises access to the waterside restricted zone. Port Watch 01 will remain alongside the bunker barge for the duration of the bunker service, and provide it with an escort service for the bunker barge from the waterside restricted zone.

1000 hours
Throughout the duration of the cruise ship visit, the security team conducts random patrols and inspections around and within the area, monitoring the passage of small craft and other vessels. The random patrols are provided for high risk facilities and chemical, oil and gas vessels.

At the Port of Brisbane Security Control Centre, CCTV feeds are constantly monitored, and Port Security personnel are on standby in the event that maritime security communication systems and backup services are requested by Maritime Safety Queensland or the Queensland Police Service.

From the landside, the Port Security team provides random external security inspections of areas outside Portside Terminal boundaries and maritime security zones.

1400 hours
As the cruise ship begins its journey down river to exit the port, Port Watch 01 is again on hand as an escort, ensuring smaller recreational vessels are safely out of the path.

The Brisbane River is typically a very busy place, particularly on weekends, and Port Security have handled a number of challenging situations during cruise ship visits. These challenges include:

- towing vessels that have pulled their anchor, to ensure safe passage of the cruise ship
- moving small vessels where people are fishing in the channel, again to ensure safe passage of the cruise ships (on authority from Maritime Safety Queensland)
- assisting canoeists and kayakers caught in the current and drifting towards waterside restricted zones
- removing small vessels from underneath berths – a dangerous and unsafe practice.

Written by Karen Weatherburn
Senior Communications Officer
Port of Brisbane

For more information:
www.portbris.com.au
The Aviation Security quarterly reports are prepared by the Department of Infrastructure and Transport’s Office of Transport Security (OTS) as a quarterly update to inform the aviation industry about aviation security issues. They supplement the OTS Aviation Security Risk Context Statement of December 2010. It should be noted that the overall threat to Australian interests from terrorism remains unchanged. The National Terrorism Public Alert Level remains at MEDIUM - this indicates a terrorist attack could occur.

**Key points in the current quarterly report**

1. **Suspicious items discovered in-flight**

   Crew should be wary of suspicious items discovered during flight—particularly potential Improvised Explosive Devices (IED), which can be fashioned to appear as innocuous items. Remember, a functional IED must have a power source, switch, initiator, and main charge, and there is no ‘typical’ IED.

2. **Employee responsibilities**

   Aviation sector employees must understand and abide by security regulations and standard operating procedures. Not doing so can create vulnerabilities that may then be exploited by terrorists. For example, at one of our airports an employee with an Aviation Security Identity Card was permitted to take a small pocket knife into the sterile area in breach of regulations.

3. **Elimination of senior al-Qa’ida leaders**

   With the death of Osama Bin Laden, al-Qa’ida has received a significant impact on its leadership. However, while significant, this does not represent a change to the Australian aviation security environment. However, the capability of al-Qa’ida and its affiliates to conduct external operations in the short term has certainly been reduced. National agencies are constantly searching for more information on al-Qa’ida, and evaluating the effects of the loss of their leadership.

4. **GovDex**

   From January 2012, all Australian Government Transport Security Advisories and Aviation quarterly security reports will be distributed electronically via a portal at www.govdex.gov.au.

For assistance with using the portal or to obtain access please contact:
Phone: 02 6274 7141
Email: OTSP_securityanalysis@infrastructure.gov.au.
The Australian Security Intelligence Organisation’s (ASIO) Business Liaison Unit (BLU), established in October 2005, provides a public interface between Australian businesses and the Australian intelligence community.

The unit’s principal objective is to raise awareness with the owners and operators of critical infrastructure regarding matters related to national security. Additionally, the BLU aims to equip corporate security managers with credible, intelligence backed, unclassified reporting which will enable them to:

- make use of the knowledge gained from their risk management and continuity planning
- authoritatively brief executive management and staff.

The BLU provides reporting to the private sector through its secure, free subscription website. Reports on the BLU website cover a range of security-related topics, including:

- current security environment
- terrorist incidents
- threats to industry sectors
- issue motivated groups
- security risk management (physical, personnel and information security)
- threats to high-profile world events
- terrorist tactics and methodologies
- country security snapshots.

In addition to operating the security website, the BLU maintains the Register of Australian Interests Overseas. This database is a voluntary initiative allowing Australian companies to register the locations of their overseas facilities. By having this information, ASIO can contact companies immediately if it becomes aware of credible, imminent and serious threats. Companies operating in high risk areas such as South and South-East Asia, the Middle East and North and East Africa are particularly encouraged to register.

The BLU raises awareness of ASIO’s work by presenting at security industry events and other forums, and is also responsible for arranging high-level meetings between ASIO’s Director-General and company Chief Executive Officers.

For more information on the BLU, please visit the website at www.blu.asio.gov.au.

BLU can also be contacted on 02 6234 1668 or blu@asio.gov.au.

The ASIO BLU was established in 2005 with a principal objective of raising awareness with the owners and operators of critical infrastructure regarding matters related to security.
The Australian Government has made major changes to Australia’s protective security policies and now has a new Protective Security Policy Framework (PSPF). State and territory governments have provided input into developing the PSPF.

The PSPF applies mainly to Australian Government agencies and any organisations working on behalf of, or handling Australian Government information and assets. This may include other governments, and contract service or goods providers.


Any questions about the PSPF can be sent to pspf@ag.gov.au

The Directive on the Security of Government Business; governance arrangements and personnel, information and physical security core policies were released in June 2010.

Additional protocols and guidelines expand on the core policies. The Personnel Security Management Protocol and guidelines were released in time to support the start of centralised vetting in the Australian Government Security Vetting Agency in October 2010. The Information and Physical Security Management Protocols and Guidelines were published in July 2011.

The Commonwealth Attorney-General’s Department recently provided briefings on the PSPF to staff with protective security responsibilities in all states and territories.

See Something, Say Something

Critical Infrastructure and Priority Sites (CIPS)

- If you see something that is suspicious or doesn't seem right then report it to the Queensland Police Service. You and your staff know your business and surroundings better than anybody else. You will know what is unusual or suspicious.
- Suspicious activity may include:
  - Taking notes or drawing maps or plans
  - Photographing facilities
  - Purchasing an unusual quantity of particular products
  - Overdressed considering the weather
  - Interference with security related features of your infrastructure
  - Asking detailed questions about security or other processes
- Reporting should be done by:
  - Filling in the CIPS template
  - Emailing the CIPS template to PolicelinkPriority@police.qld.gov.au
  - When sending a report via the above email put 'CIPS' in the subject line
- If you want further information or require the CIPS template call the Stakeholder Engagement Unit on 3406 3677 or you can download the CIPS template from www.safeguarding.qld.gov.au
- If you need urgent Police assistance call Triple Zero 000
- For non-urgent matters, you can still call Policelink on 131 444
- Benefits of using PolicelinkPriority@police.qld.gov.au includes:
  - System designed specifically for key industry/government stakeholders
  - Ensure information is promptly passed to both specialist intelligence officers and regional intelligence officers so a swift assessment can be made
  - Ensure you are provided feedback on your report
Queensland Police Counter-Terrorism Strategic Policy Branch

In November 2011 the Queensland Police Service announced a new process for reporting suspicious activity in and around Critical Infrastructure and Priority Sites.

The reporting template was sent to all owners and operators of critical infrastructure and priority sites. The reporting template can also be located at [www.safeguarding.qld.gov.au/suspicious.htm](http://www.safeguarding.qld.gov.au/suspicious.htm).

Owners and operators of critical infrastructure and priority sites are encouraged to complete the template following an incident and send it to PolicelinkPriority@police.qld.gov.au.

Maritime sector stakeholders can continue to submit Maritime Event Reports when reporting suspicious activities.

Please remember that this process is to be used to report suspicious activity that does not need police to attend your site.

If police are needed to attend your site, call 000 (if the need is urgent) or Policelink (if the need is not urgent) on 131 444. If police attend your site, you do not need to complete the template as the attending police will complete a report of the incident.

Summary

- PolicelinkPriority@police.qld.gov.au is only to be used by owners and operators of Critical Infrastructure and Priority Sites.
- This process does not need to be used by Brisbane, Gold Coast and Cairns airports (these airports should continue to report suspicious activity to on site Australian Federal Police).
- This process is to be used to report suspicious activity when police have not attended the site.
- Maritime sector stakeholders can submit Maritime Event Reports to this address that fulfils the above mentioned criteria.
- All other sector stakeholders should use the reporting template previously provided or located on [www.safeguarding.qld.gov.au](http://www.safeguarding.qld.gov.au).

![Snapshot of the Critical Infrastructure and Priority Sites reporting template](image-url)
In November 2011, Transport and Main Roads conducted its largest counter-terrorism exercise, Exercise Primus. This was conducted over a 24-hour period and involved Ports North, four ferry operations in Cairns and the Queensland Police Service. The main objective of the exercise was to evaluate how Ports North and the ferry operators would implement additional security measures during an elevated security threat.

Exercise Primus is a drill style exercise designed to assist Security Identified Surface Transport Operations (SISTO) validate their counter-terrorism risk management plans.

In the absence of actual operations, exercises are essential to ensure that plans and procedures are workable and effective, and that individual, team, group and inter-organisational performance training and responses can support those plans.

The exercise was delivered in three parts. Part one was a pre-brief for all participants, including setting the scene with a fictitious and evolving terrorism scenario. Part two saw the maritime security level (notionally) raised from one to two, which meant that the ferry operators and Ports North had to implement additional security measures. The exercise was designed to occur concurrently with normal business activities, so staff boarded the ferries for the day to observe the crew practising the additional security measures. Part three included the post activity debrief and lessons observed.

Overall, all exercise participants performed very well, and successfully actioned almost all elements of their counter-terrorism risk management plans during the exercise. As a learning activity, the exercise proved to be successful. The department has delivered individual reports to each participant to assist future learning and development.

At the post-exercise debrief, the Security Manager, Mr David Good, commented that the exercise had been a great way for the operators to evaluate their counter terrorism risk management plans.

This exercise is the first of a series that will be developed in partnership between SISTOs, Transport and Main Roads, and the Queensland Police Service to assist individual SISTOs in meeting the full exercise provisions of the Transport Security (Counter-Terrorism) Act 2008.
Advanced surveillance to protect critical infrastructure

Commercial ports, railway stations, airports and other crucial infrastructure are at constant risk from security incidents which halt operations, incurring huge costs and, more worryingly, put the general public in harm’s way. This is a reality around the world and Australia is no different.

Intelligent Computer-Assisted Video Surveillance certainly has the potential to help protect us. Such systems actively serve several purposes as they:

- reduce monitoring costs while also increasing effectiveness of business continuity and resilience
- deter and mitigate potential threats to national security
- play a key role in terms of investigating leads and assisting with the prosecution of suspects.

One technology that can be employed in this context is Automated Number Plate Recognition (ANPR) technology. If (or when) a network of ANPR cameras is rolled out nationally, law enforcement officers will be able to locate a suspect’s vehicle much faster or get a lead on a case based on the vehicle’s registration information.

Another emerging technology applicable to national security is video biometrics. For example security agents using face in the crowd technology could potentially match a passer-by’s face against various databases, such as a terrorist watch-list.

While no biometric is 100% accurate (that is correct detections with no false alarms), it can still be used as a complementary tool to provide further leads for investigation.

Through such technology, even poor quality images obtained - from CCTV footage, covert surveillance operations or even taken by mobile phones - could help identify and track suspects.
At present this technology does not exist commercially, but emerging innovations are getting very close. National ICT Australia Limited (NICTA) Advanced Surveillance Research Group based at the University of Queensland is a strong team of 20 scientists and engineers who have been at the forefront of this development for the past six years and have recently won several international awards.

In collaboration with numerous state, federal and international agencies the Advanced Surveillance Research Group has pioneered the evaluation, development and pilot deployment of various intelligent and state-of-the-art technologies to enhance national security.

Examples include:

1. Low Resolution Non-Cooperative Face Recognition Technologies:
   - live video face recognition for border control
   - forensic face recognition for police operations
   - multi-camera person tracker based on face recognition (the idea is to track all passengers at all times in an airport or public space)
   - smart phone face recognition

2. The CBRN Wireless Sensor Network:
   - measures background radiation levels, wind speed, wind direction and temperature
   - petrochemical sniffing for up to 17 chemicals
   - solar powered with no wiring
   - over one km range from the base station via wireless network (extension to underwater surveillance is anticipated)

3. Real-time video enhancement for rainy and foggy days, to enable visibility through rain.


5. Robust detection of moving cars and pedestrians from shaking cameras.

6. Wrong way detection for passengers breaching the sterile zone at airports.

7. 3D immersive CCTV presentation (using advanced commercial systems).

8. Automated Number Plate Recognition from Video (using advanced commercial systems).

9. Surveillance from urban UAVs at port and rail.

Written by
Abbas Bigdeli, Senior Researcher and Technology Manager, NICTA (QLD)
Professor Brian Lovell, Project Leader Advanced Surveillance, NICTA (QLD)

Email safeas@nicta.com.au
A unit within the Commonwealth Attorney-General’s Department, PSTC is a Registered Training Organisation registered by the National Vocational Education and Training Regulator.

PSTC training programs are aimed at staff across all levels of government – Commonwealth, state, local, and all government contractors.

PSTC programs are particularly relevant to any staff required to manage and implement government security policy as outlined in the Australian Government’s Protective Security Policy Framework.

Participants can specialise in the security field most relevant to their requirements. Security training programs contribute to a number of career pathways, including:

- protective security
- personnel security (vetting)
- physical security
- security risk management
- protective security management
- government investigations.

PSTC can award participants nationally-recognised qualifications and statements of attainment. Qualifications can be undertaken through participation in training programs (courses) and completion of workplace projects and assignments or can be achieved wholly, or in part, through assessment by recognition.

The majority of PSTC training programs are mapped to nationally recognised qualifications and units of competency contained in the PSP04 Public Sector Training Package version four. Qualifications include:

- Diploma of Government (Security)
- Certificate IV in Government (Security)
- Certificate IV in Government (Investigation)
- Certificate IV in Government (Personnel Security)

Most of our courses are conducted at the Kenneth Bailey Building, a training facility in Canberra. However, the two day Introduction to Protective Security and Introduction to Security Risk Management courses are scheduled in most capital cities at least once a year.

Recognition of Prior Learning

In addition to training services, the Protective Security Training Centre offers an assessment service providing Recognition of Prior Learning (RPL) for the qualifications listed above.

RPL is an assessment process that assesses a person’s formal and informal learning to determine the extent to which that person has achieved the required competency outcomes, or standards for entry to, and/or partial or total completion of, a qualification. It involves identifying, collecting and evaluating a portfolio of evidence that relates to work you have personally performed while working in a protective security environment.

Tailored training

Building on its well established programs and courses, the Protective Security Training Centre develops and delivers tailored protective security training solutions designed specifically to address an organisation’s unique requirements.

A tailored training solution provides a cost effective option without the additional cost of travel, accommodation, and the many other incidental expenses.
Australian Security Intelligence Organisation (ASIO) T4 Security Practitioner course

A guide to the practical application of protective security within government.

What is Protective Security?
Protective Security is a combination of procedural, physical, personnel and information security measures designed to provide government information, functions, resources, employees and clients with protection against security threats.

What is T4?
The Australian Security Intelligence Organisation’s (ASIO) Protective Security Section (T4) provides protective security advice in support of Australian government policy, to Australian Government departments, agencies and business enterprises. Key services that T4 provides include:

- protective security risk reviews
- Certificate of Zone 5 (Top Secret) facilities
- equipment testing to determine suitability for use in the protection of Australian Government facilities and material (including security information)
- technical surveillance counter measures
- specialised training including the Security Practitioner course which has been specifically developed for government security practitioners across Australia.

The ASIO-T4 Security Practitioner course

The ASIO-T4 Security Practitioner course (a guide to practical application of protective security within government) is a course run over four days and is designed for Australian Government Agency Security Advisors and agency security personnel.

The aim of the course is to provide participants with an understanding of key elements of protective security and an enhanced appreciation of the practical application of protective security within their departments and agencies. The course subject matter is delivered by T4 officers who offer expertise, experience and knowledge in contemporary and emerging protective security practices and procedures. Course participants are encouraged to actively contribute to group discussions and, where appropriate, share their experiences, ideas and approaches to protective security challenges that have presented within their work environments.

The ASIO-T4 Security Practitioner course also provides participants a unique opportunity to meet and establish valuable contacts with a wide variety of security practitioners across government.

The course programme covers a very diverse range of protective security elements, including:

- physical security and certification requirements for security zones
- role of the Security Zone Consultant
- perimeter security (fences, detection systems, bollards, vehicle barriers)
- type 1 security alarm systems
- overview of detectors
- safes and Security Containers
- security lock and hardware devices
- basic lock maintenance and changing combinations
- access control and door configurations
- technical surveillance counter measures
- physical security requirements of IT systems
- CCTV concepts and issues
- design principles of mail and delivery rooms
- protection of classified information and the management of classified waste
- key and secure entry systems
- administrative security.

The course includes a range of presentations from guest speakers including officers from the Attorney-General’s Department who will provide briefings on the Protective Security Policy Frameworks and their implications.

Further information regarding course dates, costs and conditions for application may be obtained from the ASIO website www.asio.gov.au T4 Protective Security quick link or by calling T4 direct on (02) 6234 1217.
Exploring the development of critical infrastructure protection arrangements in Australia: changing concepts and definitions

The Australian Research Council Centre of Excellence in Policing and Security (CEPS) is a research centre working across four universities:
• Griffith University
• The Australian National University
• The University of Queensland
• Charles Sturt University

CEPS was established in 2007 to boost policing and security research capacity and excellence in Australia amid the growing complexity and internationalisation of transnational crime and security issues in the post 9/11 environment.

In *A Brief History of Critical Infrastructure Protection in the United States*, Kathy Ann Brown (2006) artfully traces the development of federal critical infrastructure protection arrangements in the United States of America from the 1790s, through the Great War, World War II and the Cold War, and into the post-Cold War environment. In so doing, she reminds her readers that there have always been assets considered vital or critical to nations.

While the same is likely to be true of Australia, this short article will explore the changing terms and definitions of what is now termed 'critical infrastructure' from 1978. Understanding how critical infrastructure has been defined is a crucial first step in understanding the development, impact and reach of critical infrastructure protection policy in the Australian environment.

In modern policy, the terms used to describe and define Australia’s key civil infrastructures, have included 'vital installations' and 'vital national installations' dominant in the 1980s and 1990s, 'lifelines' in the 1990s, and 'critical infrastructure' and 'designated critical infrastructure', dominant in the post-9/11 period.

As part of the Australian Government’s policy response to the bombing outside the Hilton Hotel on 13 February 1978, then Prime Minister Fraser announced the appointment of Mr Justice Hope, a New South Wales Supreme Court Judge, to conduct a wide ranging protective security review. In his Protective Security Review Report (PSR Report), Justice Hope gave specific thought to how to best protect Australia’s key civil infrastructures. Justice Hope distinguished between key civil infrastructure (what he termed 'vital points') and key defence infrastructure (termed 'key points') (Commonwealth of Australia, 1979, p.150-155).

Although a clear definition is not evident in the PSR Report, 'vital points' were described in the following ways:

'... installations whose unimpeded operation is necessary for the orderly life of the community ...'

'... installations upon which the well-being and orderly life of modern industrial cities depend. They include power stations, water supply pumping stations, petroleum refineries, off shore oil rigs, natural gas pipelines and computer installations (Commonwealth of Australia, 1979, p.151).

There are two versions of the Protective Security Review Report: an unclassified version released publicly in 1979 and a classified version that has now been released publicly by the National Archives of Australia. It is in the classified version that Justice Hope’s considerations for how a Vital Installations Program could operate is found.

Apology: Transport and Main Roads apologises for publication errors in issue 1 within the article 'Case Study - Hilton Bombing 1978', which omitted reference details. Revised copies of this article can be obtained on request by emailing tsb@tmr.qld.gov.au.
Although Justice Hope recommended Australia develop a Vital Points Program, a program designed to protect Australia’s key civil infrastructures, it was the term ‘vital installations’ that was adopted in Australia through the establishment in the 1980s of the Vital Installations Program (VI Program). The VI Program was designed for the identification and protection of ‘important parts of the civil infrastructure’ from terrorism (Sheldrick, 1986, p.512).

Importantly, there were two tiers of civil infrastructures that formed part of the VI Program: Vital Installations and Vital National Installations. The definitions were settled in the following way:

A Vital Installation is a facility, installation or resource, the loss of the products or services of which would severely disrupt the orderly life of the community, or which, if damaged, would cause a major public hazard.

A Vital National Installation (VNI) is a vital installation in which the Commonwealth and one or more State/Territory Governments have substantial interests and responsibilities, and/or the installation is of major national economic importance (Shedrick, 1986, p.512).

By distinguishing between the tiers of key civil infrastructure, those assets identified as Vital National Installations could be considered the ‘super-infrastructures’ of the time.

While the VI Program was operating, the term ‘lifelines’ was also used to describe Australia’s key civil infrastructures. Between 1995 and 1997, the Tasmanian Government, supported by Emergency Management Australia undertook the Tasmanian Lifelines Project. The project comprised three sub-projects focused in different geographical areas in Tasmania that delivered three separate reports (O’Donnell, 2011, p.31).

The reports focus on the concept of ‘lifelines’, which are formally defined as ‘systems or networks, which provide for the circulation of people goods and services and information upon which health, safety, comfort and economic activity depend’ (Tasmanian Government, 1997a, p.5).

However, it is clear that ‘lifelines’ as a term was far from settled. Within the three reports, while ‘lifelines’ is used as an umbrella term, other terms are effectively used interchangeably. They included: essential services; essential services (lifelines); lifeline systems; essential infrastructure lifelines; essential community infrastructure (lifelines); key essential services; essential lifelines.

The terminology used to describe Australia’s key civil infrastructures settled in the post-9/11 environment through the adoption of the term ‘critical infrastructure’.

While the term 'critical infrastructure' itself has remained constant, the definition has proven to be malleable, though it has remained notably and deliberately constant since the mid 2000s. The current Australian definition of 'critical infrastructure' includes a focus beyond the bricks and mortar so evident in the earlier definitions. The settled Australian definition of critical infrastructure is now:

Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security.

In this context significant means an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia’s international competitiveness’, or impedes the continuity of government and its services (Commonwealth of Australia, 2010a, p.8).

The concept of ‘designated critical infrastructure’ emerged in 2006 through the Defence Legislation Amendment (Aid to Civilian Authorities) Act 2006 (Cth). The Act amended the Defence Act 1903 (Cth) and included:

**Infrastruture** includes physical facilities, supply chains, information technologies and communication networks or systems.

**Designated critical infrastructure** means infrastructure, or a part of infrastructure, that is declared under section 51CB.

These definitions are significant as they give rise to specific legislative powers to protect designated critical infrastructure, in particular the use of lethal force by the Australian Defence Force. In so doing, it reinvigorated the earlier policy concept of 'super-infrastructure' but for a new era.

---

**REFERENCES**


Legislation

*Defence Act 1903 (Cth)*

*Defence Legislation Amendment (Aid to Civilian Authorities) Act 2006 (Cth)*
Protective security for critical infrastructure

Transport and Main Roads is proud to host its first Critical Infrastructure Protection Forum for 2012

Previous forums in this series have looked at topical and relevant issues for the transport sector including pandemic planning, natural disasters, exercising, business continuity and resilience. This forum will provide industry and government with an informative look at some of the key principles underpinning good practice in protective security.

Protective security is a broad concept. It is the steps an organisation takes to safeguard assets from foreseeable risks, protect assets from loss or misuse and support the continued delivery of essential business in an ‘all hazards’ risk environment.

Consistent with its aim of enhancing business resilience in the Queensland transport sector, the department is holding this forum to discuss the tenets of protective security and its relevance in safeguarding an organisation’s people, information and assets.

Topics of discussion will also provide industry and government with insights on recent developments in closed circuit television (CCTV) technology and policy.

The forum will feature a series of brief presentations:

1. The role and responsibilities of Australian Security Intelligence Organisation’s (ASIO) T4 Protective Security Branch:
   - services and products that T4 provide to government
   - the testing program and Security Construction and Equipment Committee
   - technical surveillance counter measures – looking for ‘bugs’
   - training courses provided by T4.

2. The role and responsibilities of ASIO’s Critical Infrastructure Protection Branch, with an emphasis on the importance of liaison information provided by critical infrastructure owners and operators:
   - Australia’s current security environment with a focus on recent events overseas.
   - recent developments in the threat environment for transport sub sectors (aviation/air cargo, land freight, mass passenger transport, maritime ports and shipping).

3. The role of ASIO’s Business Liaison Unit.

4. Protective security measures and arrangements at the Port of Brisbane.

5. The ‘Advanced Surveillance to Protect Critical Infrastructure’ project undertaken by National Information and Communications Technology Australia (NICTA).


Please note that attendance to this event is free, with complimentary catering provided.

In order to register your interest for this event please email your name, contact details and any special dietary requirements to:
Email: tsb@tmr.qld.gov.au
Phone: 07 3253 4082
Critical Infrastructure Protection Forum
Protective Security for Critical Infrastructure

8.45 am - 1.00 pm
Friday 27 April 2012
Marriott Brisbane
Queen Adelaide Room, 515 Queen Street, Brisbane

Attendance to this event is free. Please RSVP your interest to tsb@tmr.qld.gov.au by no later than 13 April 2012.