



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

# CIP NEWSLETTER

For owners and operators of critical infrastructure

Vol 4 No 3—Legal issues

October 2007

## Contents

Critical infrastructure protection and the law	1
Business cooperation and national security	3
The TISN Secure web site—privileges and obligations	5
Trust the TISN Deed of Confidentiality	6
Responding to emergencies	7

## Critical infrastructure protection and the law

*The Australian Government's approach to critical infrastructure protection is based on cooperation rather than regulation. Nevertheless, the law can play a vital role in helping critical infrastructure owners and operators understand and fulfil their responsibilities.*



The Australian Government provides strategic leadership and coordination in the development and implementation of a nationally consistent approach to critical infrastructure protection. The Government's approach is based on cooperation with business and the view that the individual owners and operators of critical infrastructure are in the best position to understand and address their security needs. The very clear focus is on cooperation and consultation, rather than regulation and proscription. This approach is reflected in the *National Guidelines for Protecting Critical Infrastructure from Terrorism* and the *National Strategy for Critical Infrastructure Protection*.

This emphasis on cooperation does not mean the law has no role in setting boundaries for critical infrastructure protection and for providing critical infrastructure owners and operators with guidance about their responsibilities. The escalation of terrorist activity means

that, more than ever before, our critical infrastructure is under threat. It is important that we have the right laws in place to help in the task of protecting our critical infrastructure. In some key areas, such as aviation and maritime security, the Australian Government has put in place quite specific security legislation.

The *Aviation Transport Security Act 2004* (Cth) and the *Aviation Transport Security Regulations 2005* (Cth) establish minimum security requirements for civil aviation. These requirements include things such as screening, onboard security, persons in custody, and weapons and prohibited items.

The *Maritime Transport and Offshore Facilities Security Act 2003* (Cth) and the *Maritime Transport and Offshore Facilities Security Regulations 2003* (Cth) put in place regulations for individual security plans for ships, other maritime transport operations and offshore facilities.

*Continued on p. 2*

ISSN: 1833-5861 (Print)  
1833-5888 (Online)

Published on behalf of the  
Trusted Information Sharing  
Network for Critical  
Infrastructure Protection  
by the Australian Government  
Attorney-General's Department  
Critical Infrastructure Protection  
Branch

### Contact:

p. +61 2 6272 7150  
f. +61 2 6272 7190  
e. [cip@ag.gov.au](mailto:cip@ag.gov.au)  
[www.tisn.gov.au](http://www.tisn.gov.au)

## Critical infrastructure protection and the law

*Continued from p. 1*

There is no specific Commonwealth legislation dictating how owners and operators of critical infrastructure protect their assets. However, there is a range of other legislation which affects the protection of critical infrastructure in some way. Without attempting to be exhaustive, this legislation includes:

- The *Cybercrime Act 2001* (Cth) which creates offences that cover activities such as hacking, spreading computer viruses, unauthorised access to commercial or confidential information, denial of service attacks, interfering with web sites and trading in technology designed to damage or hack into another person's computer.
- The *Liquid Fuels Emergency Act 1984* (Cth) which gives the Commonwealth, in consultation with state and territory governments, contingency planning powers to ensure oil companies maintain reserves and develop emergency procedures to protect the supply of fuel in the event of an emergency.

- The *Terrorist Insurance Act 2003* (Cth) which was enacted in response to the progressive withdrawal of insurance cover for terrorism acts following the September 11, 2001 terrorist attacks in the United States. The Act renders terrorism exclusion clauses contained in eligible commercial property and business interruption policies ineffective in the event of a declared terrorist incident. Cover is then deemed to be provided for terrorism losses in accordance with the other terms and conditions of the insurance policy.

Attorney-General Philip Ruddock has also reminded businesses of their legal obligations under the Corporations Law to analyse the terrorist risk and take appropriate action. Speaking about national security, Mr Ruddock pointed out the legal obligation on managers and corporations in Australia to make proper decisions. He has also noted that all directors assume a degree of culpability in that role to look at and properly consider risk.

It is also worth noting that although there is no Commonwealth legislation specifically targeted at critical infrastructure owners and operators, the government of Victoria has enacted the *Terrorism (Community Protection) Act 2003* (Vic). Part 6 of the Act imposes obligations on the operators of specific essential services in planning for the protection of those services against potential acts of terrorism. Operators are required to prepare, audit and update risk management plans, and to conduct training exercises to test the operations of the plan each year.

It is clear that the law has an important role to play in guiding and assisting good decision making. The task is to maintain a legislative framework which works in harmony with good risk management, good business continuity strategies and good corporate governance to keep our national critical infrastructure as safe and secure as possible.

*The escalation of terrorist activity means that, more than ever before, our critical infrastructure is under threat*



## Business cooperation and national security

*The TISN facilitates information sharing between the owners and operators of critical infrastructure and between business and government. Sharing information is all very well, but it is absolutely essential that this flow of information does not compromise competition or distort market mechanisms. In response to concerns raised by business about the legal issues associated with increased information sharing, the Attorney-General's Department has considered the key laws relating to continuous disclosure obligations in the Corporations Act, the competition policy provisions in the Trade Practices Act, and access to documents under the Freedom of Information Act.*



In order to ensure that investors have timely and equal access to price-sensitive information, the *Corporations Act 2001 (Cth)* and the Australian Stock Exchange (ASX) Listing Rules place a general obligation on listed entities to immediately inform the ASX of information likely to materially affect their share price. Non-listed entities are required to provide such price-sensitive information to the Australian Securities and Investment Commission.

Concerns have been raised that these reporting obligations may be compromised by the general exchange of information at TISN meetings, or where a company has been confidentially advised by security agencies of an imminent security threat.

The Australian Government's position is that existing exemptions to the continuous disclosure regime adequately cover both situations.

However, companies need to consider their disclosure obligations on a case-by-case basis.

TISN members can enter into a Deed of Confidentiality to assist in the protection of the confidential status of information they share within the TISN. The Deed is intended to allow the confidential status of information discussed within TISN to be preserved, and may assist signatories to share information about their vulnerabilities without activating their continuous disclosure obligations.

The precise nature of the information being shared will influence whether the disclosure requirements under the ASX Listing Rules apply. Analysis must be undertaken by participating organisations on a case-by-case basis and assessed on the particular facts. Participants should satisfy themselves that everyone present at a meeting has signed a copy of the Deed before disclosing confidential information.

*Information sharing and participation in the TISN is helping businesses manage risks and it is also contributing to a more secure Australia.*

*Continued on p. 4*

## Business cooperation and national security

*Continued from p. 3*

If a security or law enforcement agency shares confidential information concerning an imminent security threat with a company, it needs to work with the agency to balance both the company's requirements to meet its disclosure obligations and national security interests to keep the information secure. In this instance it is recommended that company directors use their discretion and negotiate with the security agency to determine the scope of the information they may release in order to meet their disclosure obligations.

Companies should look to the Companies Update 01/07 released by the ASX on 29 January 2007 to assist them in this task. That Update states that 'the ASX would expect that any information concerning an event would be limited to a factual description of the potential material effect of the event on the listed entity and would not include details or comment on the operational response of government agencies'

Knowledge of continuous disclosure requirements is not necessarily uniform across security and law enforcement agencies. Accordingly, it is recommended that companies ensure the agency they are dealing with has a clear understanding of the company's need to disclose certain information to meet its continuous disclosure obligations, and know the importance of *both* parties consulting with each other prior to the release of information. It is also recommended that companies establish internal protocols or contacts with relevant security and law enforcement agencies well in advance of any security events occurring. This will raise awareness of each party's obligations and constraints, and assist the coordination process.

The ASX Companies Update 01/07 can be found at: [https://](https://www.asx.com.au/resources/newsletters/companies_update/archive/CompaniesUpdate_20070129_0107_HTML.html)

[www.asx.com.au/resources/newsletters/companies\\_update/archive/CompaniesUpdate\\_20070129\\_0107\\_HTML.html](https://www.asx.com.au/resources/newsletters/companies_update/archive/CompaniesUpdate_20070129_0107_HTML.html).

### Competition Policy and the Trade Practices Act

Some businesses participating in the TISN have raised the possibility that discussion of security issues may transgress the anti-competitive provisions of the *Trade Practices Act 1974 (Cth)*.

The focus of the Trade Practices Act is on contract arrangements or understandings which seek to lessen competition, fix prices, divide markets or restrict output.

Advice to date is that general discussions within the TISN are not likely to raise issues relating to competitiveness in the market place as they are generally in relation to security policies, threats and vulnerabilities. A similar view is taken of TISN meetings, at which government officials are present, as they are not a forum for detailed price and market information to be shared between competitors. Where representatives do wish to discuss information that could result in reaching some sort of agreement, it may be appropriate to seek authorisation from the Australian Competition and Consumer Commission (ACCC). The Attorney-General's Department has prepared a paper on this issue endorsed by the Chairman of the ACCC, Mr Graeme Samuel.

### Freedom of Information

A final concern of some businesses has been that information provided to the government for national security purposes, or as part of participation in the TISN, may later be made publicly available under the *Freedom of Information Act 1982 (Cth)* (FOI Act).

The Attorney-General's Department has a high level of confidence that sensitive business information would fall within existing exemption provisions under the FOI Act and would not need to be disclosed. Under these exemptions, documents can be withheld if:

- their release would compromise security or defence of the Commonwealth or adversely affect public safety or law enforcement, or
- the documents contain information provided in confidence, or business information including trade secrets, or information which has a commercial value.

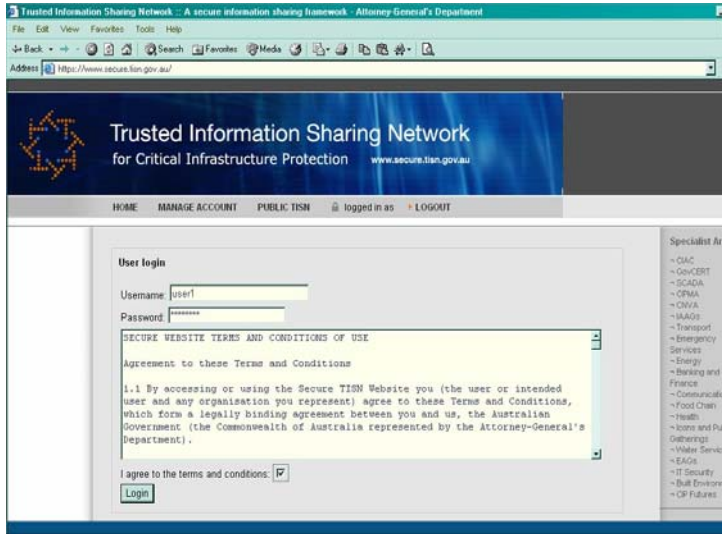
In all probability these exemptions would apply to most information shared for national security and TISN purposes.

Additionally, businesses would have the opportunity to comment on, and highlight, any concerns they may have about business information that may potentially be released. The Australian Government is acutely aware of the need to protect business privacy and foster cooperative and trusting relations with business. This would be reflected in any deliberations about re-releasing such information provided by business.

### Conclusion

More than ever, businesses are working with each other, and with government, to address security issues. Information sharing and participation in the TISN is helping businesses manage risks and is also contributing to a more secure Australia. With prudence, foresight and goodwill, both business and government are promoting security without compromising competition in the market place.

## The TISN secure web site—privileges and obligations



*Taken as a whole these terms and conditions ensure the TISN secure web site is used responsibly and fairly by all TISN members, and they ensure that the site and its confidentiality can be trusted by all those who use it*

*Access to the TISN secure web site has its privileges, but it also carries obligations. Critical infrastructure owners and operators may use the web site to share confidential information, but they must also respect the site's legal requirements.*

The TISN secure web site is an exclusive online area for members of the TISN. The web site enables members to exchange confidential information and engage in discussion forums. It also allows the Australian Government to post sensitive information which it cannot send to members electronically.

The web site has sub-sites for the private use of each of the TISN's Infrastructure Assurance Advisory Groups, Expert Advisory Groups and the Australian Government Computer Emergency Readiness Team (GovCERT.au). These groups may allow others to access their sites for coordination purposes. Of course, this access is subject to the existing confidentiality requirements governing such access.

These requirements are contained in the Terms and Conditions of Use, which have been developed to regulate use of the TISN secure web site, and to protect the confidentiality of its information. Persons applying for access to the web site must sign an application form agreeing to these Terms and Conditions. It is not necessary for applicants to be signato-

ries to the TISN Deed of Confidentiality, which imposes separate obligations. Each time users access the site they are required to electronically renew their acceptance through a legally binding 'click-wrap' agreement.

Apart from confidentiality obligations, the web site's Terms and Conditions impose other obligations on users, which in essence relate to responsible use of the TISN secure web site. Clause 1.8 prohibits use of the web site in a way that infringes the copyright or other intellectual property rights of third parties. Users who breach this clause will have their access to the site suspended.

To comply with the conditions of Clause 1.8, users must ensure that they do not post on the site any material in which copyright is owned by third parties unless they have obtained the written permission of those parties. To draw attention to third party material, it may be preferable for users to summarise it or quote an insubstantial portion of it, and acknowledge the source by providing a URL link or reference to

where the material may be found.

The Terms and Conditions also contain an indemnity clause, Clause 1.21, which operates to indemnify the Commonwealth against liability for unauthorised use of the site, including copyright infringements. This clause is necessary to protect the Commonwealth. Without it, the Commonwealth could be held liable to third parties that suffer loss as a result of site information posted by a site user.

Taken as a whole these terms and conditions ensure the TISN secure web site is used responsibly and fairly by all TISN members, and they ensure that the site and its confidentiality can be trusted by all those who use it.

The hosting of the TISN secure web site will shortly be transferred from the Defence Signals Directorate to the Attorney-General's Department. Because the new server will be running different software there will be some changes to the look and feel of the site. These changes will be minimal and training will be available for all administrators and users as soon as practicable.

## Trust the TISN Deed of Confidentiality

*Critical infrastructure protection requires the active participation of the owners and operators of the infrastructure, regulators, professional bodies and industry associations, in cooperation with all levels of government, and the public. In some cases, these bodies operate on an informal or semi-formal basis in cooperation with one another. In other cases, more formal arrangements are entered into, such as Memoranda of Understanding and Agreements. Essentially, the arrangements are tailored to suit the needs of the parties and the context of the critical infrastructure potentially at risk.*

### TISN Deed

The TISN's success rests on the ability of owners and operators of critical infrastructure to share information on security issues. In order to achieve its objectives, TISN participants need to be able to freely and frankly discuss issues. As these discussions could involve the disclosure of confidential and sensitive information, arrangements have been put in place to ensure that such information is properly managed and reasonably protected from unauthorised use or disclosure.

A key aspect of these arrangements is the TISN Deed of Confidentiality. The Deed is intended to facilitate information sharing within the TISN and assist companies to meet their existing legal obligations. It requires signatories to ensure that confidential and commercially sensitive information is properly managed and reasonably protected from unauthorised use or disclosure.

Not all information that is the subject of discussion within the TISN will be confidential. The Deed applies only to information that is clearly confidential in nature and where it is necessary for the information to be handled in such a way that its confidentiality is maintained and its distribution limited.

An additional benefit of the TISN Deed is that it may assist businesses to meet their continuous disclosure obligations under the *Corporations Act 2001 (Cth)* and Australian Stock Exchange Listing Rules, while shar-

ing information about security procedures and vulnerabilities. (See our article on business cooperation and national security on page 3 for further discussion.)

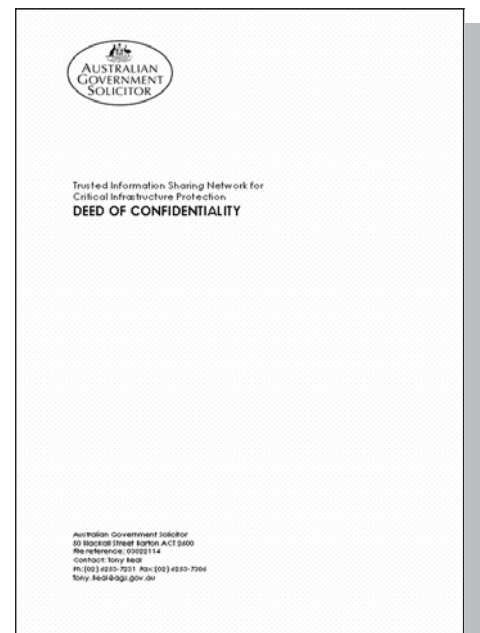
The TISN Deed may be signed on behalf of a company or by participants in their individual capacity. TISN participants who have not signed the Deed may have only limited access to information discussed within the TISN. Participants should satisfy themselves that everyone present at a meeting has signed a copy of the Deed before disclosing confidential information.

### Government Representatives

The Deed only needs to be signed by private sector participants. Government representatives, whether Federal, state or territory, are not required to sign it due to their extensive existing statutory and other legal obligations for the handling of information. All government representatives who participate in the TISN are required to sign a Government Representative Confidentially Acknowledgement to expressly acknowledge these obligations.

Further information about the TISN Deed of Confidentiality can be found on the *TISN Deed of Confidentiality* fact sheet. This fact sheet can be downloaded from the TISN ([www.tisn.gov.au](http://www.tisn.gov.au)) or obtained in hard copy by emailing [cip@ag.gov.au](mailto:cip@ag.gov.au).

*The Deed is intended to allow the 'confidential' status of information discussed within TISN to be preserved*



## Responding to emergencies

*Responding to an emergency situation can be difficult and demanding. There are many immediate and pressing issues that need to be dealt with quickly and effectively. But, as was discovered at a meeting on legal issues organised by the Critical Infrastructure Protection Branch, emergency situations can raise a multitude of legal, ethical and moral dilemmas.*

Effective handling of emergency situations requires the ability to assess the situation quickly and make rapid decisions. Failure to act, or to act quickly enough, can have significant consequences, particularly where critical infrastructure is involved. However, acting without gathering sufficient information or taking due care can be equally dangerous.

The best way to respond to this dilemma is to ‘be prepared’.

Participating in the CIP Branch legal issues workshop, Critical Infrastructure Advisory Council chairs tussled with a number of scenarios which highlighted the complications and sensitivities involved in dealing with an emergency.

A sample of the hypothetical scenarios discussed at the meeting provides an insight into the dilemmas an emergency situation can create.

### Scenario 1—Pandemic influenza

As an owner and operator of a supermarket chain, how would you deal with an influenza pandemic?

- What happens when supermarket crowds start to constitute a health hazard to you and your employees?
- What if your staff are infected and pass the virus to customers?
- If food shortages arise, is it acceptable to sell stock that is past its ‘use by’ date?
- Would it be acceptable to sell goods in high demand at inflated ‘market’ prices?

- If the Government was to institute a standard basket of foodstuff to be home delivered to the sick and infirm, how would this be organised and who would bear the cost?



### Scenario 2—City-wide evacuation

What happens to a financial institution’s ‘hot site’ when faced with a series of seemingly conflicting directions from emergency services?

- If a lawful direction is given to evacuate a building, what does that mean for staffing of the ‘hot site’?
- What if loyal staff volunteer to attend the ‘hot site’ and waive any indemnity to the firm?
- What is the legal weight of a verbal directive from an emergency area commander agreeing that staff can attend the ‘hot site’ in

*Failure to act, or to act quickly enough, can have significant consequences for both yourself and others, particularly where critical infrastructure is involved.*

*Continued on page 8*

## Responding to emergencies

*Continued from page 7*

order to meet Australian Prudential Regulatory Authority requirements?

### Scenario 3—Prioritisation and fault restoration

- How would a large telecommunications carrier's continuity plans work in the event of two major disasters?
- What services should be restored first?
- What happens if different parts of government give conflicting directions?
- Under what circumstances would business hand control of the situation to government?

- How does a company balance the need to cooperate with government directions and act as a good corporate citizen when its contractual obligations may require it to act otherwise?

### Conclusion:

It was clear from the vigorous debate and discussion on the day that there are no easy answers to complex situations. What is essential is that owners and operators of critical infrastructure have emergency management plans in place, are ready to think 'outside the square', and be open to advice and views of all types. Unfortunately, there is no such thing as a

perfect plan. The challenge is to be as prepared as possible and to be flexible enough to manage new circumstances and dilemmas as they arise.

It is also wise to try to think through the legal issues relevant to your business which might arise in emergency situations and seek advice on these well in advance.

### Other scenarios:

The Attorney-General's Department Critical Infrastructure Protection Branch is keen to develop further scenarios and welcomes your input on these matters.



Image courtesy EMA