Infrastructure information in the public domain

Trusted Information Sharing Network
for Critical Infrastructure Protection

A GUIDE TO MITIGATING SECURITY RISKS

Disclaimer

The focus of this guide is on creating general awareness of security implications that might impact you or other people from inappropriate publication of infrastructure information. It provides general information on ways that might be appropriate for you to conduct reviews of your policies and practices from this perspective. This guide is not intended to be definitive or comprehensive, nor does it constitute advice. It is your responsibility to ensure that any review you undertake or any action you contemplate is appropriate to you and your activities, and takes full account of your particular circumstances. Accordingly, you should base any action you take exclusively on your own methodologies, assessments and judgement, after seeking specific advice from such relevant experts and advisers as you consider necessary or desirable.

Inappropriate publication or distribution of information could also involve a breach of the law (for example by illegally publishing third party material or breaching privacy laws) or expose you to legal liability (for example where publication causes loss or damage to another person). Information on your legal obligations is outside the scope of this guide. You should retain your own legal counsel to advise you in respect to your legal obligations.

To the extent permitted by law, neither the Australian Government nor any of its personnel or agents make any representation or give any warrantee, expressed or implied, or accepts any legal liability or responsibility for, the accuracy, completeness of any information or material in, or use of, this guide or any related matter.

ISBN: 0 642 21198 1

TABLE OF CONTENTS

Do you publish or distribute information about your business operations or facilities?

Do you provide information about other organisations or businesses?

You may need to consider the security risks associated with having this information in the public domain.

This guide provides some general, non-prescriptive advice to operators of public information services who may have to manage security risks.

Who is this guide relevant to?

This guide is relevant to businesses that publish or distribute information about infrastructure in the public domain. This can include private organisations, organisations that represent or provide information on behalf of other businesses and government organisations.

While information about infrastructure exists in the public domain in many forms, there are three broad categories of information that this guide is intended to assist in evaluating:

1. information about a business or facility provided in a continuous or static form, such as a corporate web site with operational information or data
2. information provided for operational reasons by an organisation or company in response to specific requests from the public, such as 'dial-before-you-dig' services, and
3. general information provided on a commercial or service basis, often about businesses or facilities unrelated to the provider of the information, including satellite photography and spatial or survey data.

Infrastructure information can be provided as a means of marketing or profiling a business, as a way to mitigate the risk of accidental damage to equipment or installations or as a commercial service in its own right. It can also find its way into the public domain simply because there are no measures in place to make it secure.

It can take the form of technical specifications, information about the size or location of a facility, photographs or other images, timetables or operational schedules.

Why is this an issue?

The level of terrorist threat to Australia has increased since September 2001, with some evidence that terrorist groups around the world utilise public sources of information to identify targets and plan attacks. This increased threat needs to be taken into account in the security planning and risk management undertaken by businesses and organisations.

Businesses can also be exposed to a range of criminal activity ranging from vandalism to organised criminal attack, extortion and sabotage.

In all of these cases, publicly available information has the potential to assist in planning an attack. Providers of information need to identify potential risks and consider measures to deal with those risks.

Is this guide compulsory?

No. This guide is advisory only and intended to raise awareness of the security implications associated with publishing or distributing potentially sensitive infrastructure information. On the basis of examining the issues raised in this guide, organisations may decide to review information in the public domain or implement their own policies and internal guidelines on public information.

The material in this guide does not in any way affect your obligations to comply with all relevant legal obligations. The types of legal obligations that might be applicable include state, territory and Commonwealth laws, common law and contractual duties and obligations. It is your obligation to know, understand and comply with the law, and it is recommended that you obtain your own legal advice in respect to your information publication and distribution policies and practices.

While it is acknowledged that carrying out the measures outlined in the guide may incur additional expense, business owners and operators need to be aware that the cost and other consequences of inaction can be far greater. On this basis the cost of security and the mitigation of potential threats and risks should be viewed as an investment rather than a cost.

There are many perfectly legitimate uses of public information about businesses, facilities and infrastructure. Indeed, the public availability of information is often essential for occupational health and safety reasons or to maintain the core business of a company. It is not the purpose of this guide to suggest that these legitimate uses be curtailed, unless the benefits of having the information in the public domain are clearly outweighed by the identified security risks.

A public infrastructure information action summary is at **Annex A**.

How do I identify potentially sensitive information?

Sensitive information is information that could potentially be used by terrorists or criminals to identify vulnerabilities and plan attacks against a business, facility or infrastructure.

Examples of this type of information include:

- information about the location, position, or dimensions of a physical facility, such as maps, floor plans, photographs and computer imagery
- specific information about the purpose and use of a facility that would identify it as an attractive target
- information about hazardous or other materials stored at a site
- information about the construction of a facility, such as access points, perimeter protection, and design features
- information on important system topologies or key systems within a business or facility, such as Supervisory Control and Data Acquisition (SCADA) systems
- information about important business inputs, supply lines, and interdependencies with other businesses or facilities
- specific information about customers, staff, partners or suppliers that would identify a business as a possible target of interest

- information about security arrangements, business continuity plans and recovery plans
- live or real-time information that cannot easily be vetted for security purposes, such as live webcams
- timetables and operational schedules
- information about changes in traffic, volume, capacity or output, and
- information about incidents or attacks that happened previously or elsewhere.

Information which requires increased protection may be identified by considering the consequences of its unauthorised disclosure or misuse.

Government policy requires security classified information to be assigned a protective marking which indicates the level of protection that must be provided during handling, storage, transmission, transfer and destruction of the information.

While such a system may not be practical for your business or organisation, a similar tiered level of assessing potential harm resulting from the unauthorised disclosure or misuse of information may be useful.

Examples to consider:

MIGHT POSSIBLY CAUSE HARM—this could include information pertaining to personnel, property, finance or commercial conferences. Compromise could cause distress, financial loss or loss of potential income.

COULD REASONABLY BE EXPECTED TO CAUSE HARM—this could include information pertaining to research and development, business and marketing, trade and commerce. Compromise could endanger individuals or undermine the financial viability of organisations.

COULD REASONABLY BE EXPECTED TO CAUSE SERIOUS HARM—this could include information pertaining to budgets, key business relationships, trade secrets or sensitive processes (eg.cash handling). Compromise could threaten life or substantially impact on economic and commercial interests.

How do I decide whether something needs to be done about the sensitive information?

If you have identified sensitive information in the public domain, the next step is to determine whether measures need to be put in place to lower any security risks associated with it.

One question to consider is whether the information is already available from other sources or through other methods. For example, information about the dimensions of a facility could be obtained by physical observation or from other widely available sources, such as street directories. If this is the case, there may be little benefit in removing or changing the information that you provide.

Information may also be placed in the public domain for important reasons that override the security risk. For example, there may be a legal or regulatory obligation to disclose information, or you may need to make the information available so that members of the public do not unintentionally or accidentally disrupt your business. In such cases, simply ceasing to provide the information may not lessen the overall risk to your business. It may actually increase it.

In many circumstances, however, it is possible to do a cost-benefit calculation to determine whether sensitive information needs to be restricted. The costs in the calculation would relate to the security risk posed by having the information in the public domain. There will usually be a corresponding benefit in having the information available to the public.

If you publish or provide information about infrastructure owned by others, then you will not be able to fully assess the security risk to the infrastructure owner posed by having the information in the public domain. However, how you handle this information may affect your organisation's reputation and relationships with other organisations. You may like to contact the owner of the infrastructure to discuss issues surrounding public disclosure of information about their infrastructure.

What options are there for lessening the risk?

Should the security risk of publishing information outweigh the commercial or other benefits, there are numerous potential solutions and treatment options to consider. You should note that not all security requirements pass a cost-benefit analysis, but they are still required for good business.

Deletion or removal

The most obvious measure to lessen risk is to remove, delete or secure the information. However, this is only one treatment and is not always the best option, for the following reasons:

1. Removal or deletion is not always effective, especially if the information has been distributed through a medium like the Internet. Services such as the Google search engine store information in memory caches, which can allow retrieval long after the material has been deleted at its source. There are many other ways in which information on the Internet can be cached, mirrored or archived in ways that are not controlled by the originator. Individual users may also have simply saved or recorded the sensitive information already for their own purposes.

2. Deletion of information can be conspicuous, and can actually alert malicious users to its sensitivity. These users may then attempt to retrieve it from another source.

3. Deletion is not always the most effective option in terms of maximising the benefits and minimising the costs of the information. Other measures for distributing the information to members of the public may mitigate security risks while maintaining the benefits of having the information available.

A summary of some of these alternative measures follows.

Disaggregation, censorship and classification

Sometimes you may publish or distribute more information than is necessary to achieve the desired purpose. It may be the unnecessary elements of the information that are sensitive or creating the security problem. Disaggregating the information so that only the core message is provided may lessen the risk.

The level of detail in information may be able to be changed so that it meets its purpose without causing security concerns. For example if the purpose of publishing a map is to allow people to find your location and know where to park, a high level not-to-scale map would meet this need just as well, or better, than using a highly detailed site plan that was prepared for another purpose.

A related measure is censorship. Sensitive parts of a data set or document can be removed without necessarily lessening the usefulness of the information to its audience.

If a document is already distributed to a defined group of users, you may wish to consider using some kind of caveat or classification system, which advises or requires those users to protect or secure the document in some way.

Request-based distribution

If sensitive information is being published in an open medium like the Internet, there may be value in targeting its distribution to those who actually have a use for it or have a defined 'need-to-know' the information. This could involve setting up a system to distribute information on the basis of specific requests (eg. through password protected web sites). While this would not necessarily create any barrier to misuse, a malicious party may be less willing to make a direct approach to request information.

Registration of users

A further measure to limit misuse may be a requirement for users of the information to register before making a request. This could involve a spectrum of requirements. The user could simply be required to volunteer a name, or verified proof of identity could be required, as well as other details like an Australian Business Number.

Record keeping and audit systems

You may wish to consider whether or not you should keep records of access to your sensitive information. Keeping records may help if there is an investigation of a security incident or threat. It may also allow you to identify suspicious trends. You may need to retain details of who has accessed your information or requested access, as well as the reason for their access and the subject matter.

You may wish to consider an audit system that can identify suspicious patterns of inquiry of unusual frequency or related to sensitive topics.

Escalation and reporting

If a request-based system is in place, and the provider of the information notes an unusual or suspicious pattern of requests, it may be worthwhile documenting the activity and reporting it to the National Security Hotline. The Hotline is available 24 hours a day on 1800 123 400. It is able to refer information to intelligence authorities and police.

State and territory authorities may also be able to assist and their contact details are listed at **Annex B.**

Developing an information policy

Your business or organisation may wish to write an internal policy or guideline with criteria for screening information for security risks before putting it into the public domain. This policy could include measures to ensure an appropriate level of accountability and sign off for decisions made regarding public access to information. Other businesses may already have policies in place, and may be of assistance as a source of experiences and ideas.

Staff awareness training

As part of the information policy there should be dedicated awareness training for staff and contractors regarding the risks associated with information security and the accepted methods to manage these risks. This will help to achieve the objective of the internal policy or guideline.

Securing information

Having identified sensitive information that is not for public access, you may need to store it securely. There are established standards for secure storage and management of information that you may wish to investigate.

*AS/NZS ISO/IEC 27001:2006 i*s the current Australian standard for information security management. Standards Australia also publishes *HB 231:2004: Information security risk management guidelines*, which is essentially a handbook for businesses and organisations of all types and sizes that need to risk-manage information.

Legal issues with treatment options

A comprehensive approach to treating risks to your organisation will include consideration of relevant legal issues.

Legal issues may arise if you change the way that information is collected, handled, shared or disclosed. Personal information can be particularly sensitive. For example, if you establish or change requirements for users to register their details before having access to information it is important to take privacy laws into account.

It is likely that your organisation will already have well developed policies in relation to the privacy of customer information, which can be adapted to apply in this situation.

You should also be aware that in some circumstances you may be legally required to disclose information, such as under companies' continuous disclosure obligations. There may also be circumstances where you would be legally prohibited from sharing information, such as where it would be prohibited anti-competitive conduct under the *Trade Practices Act 1974 (Cth)*.

Changes to practices or procedures of any kind could have potential legal implications. You should not assume that existing policies or previously obtained legal advice will cover the new or changed situations. It is therefore always desirable to obtain legal advice before proceeding with any change or new way of doing things.

Decision tree walkthrough examples and internal security, administration and information security procedures

A sample decision tree for assessing and mitigating risk in respect of information in the public domain is at **Annex C**.

Some walkthrough examples are at **Annex D**.

Some suggestions for implementing tighter information security procedures are at **Annex E**.

What do I do if someone else is providing information about my business or facility?

In some instances, other organisations or individuals may be providing information, data, or imagery related to your business, which you may regard as a genuine security issue. This can range from a webcam on a personal web site providing live pictures of an area that happens to include your facility, to dedicated spatial data and satellite imagery providers.

In such cases, it is worth, in the first instance, approaching the provider of the information with your concerns. It will usually be possible to resolve the situation informally.

Sources of further information

Some sources of further information and advice are listed at **Annex F**.

Annex A: Public infrastructure information action summary

1. Survey the infrastructure information you provide in the public domain.
2. Undertake a risk assessment to determine if any of this information poses a security risk to your, or another organisation.
3. Where sensitive information has been identified, undertake a cost-benefit analysis to determine whether the security risk of providing the information to the public outweighs the benefits.
4. If the security risk outweighs the benefits, determine whether there are options available to mitigate the risk.
5. Choose and implement the best option.
6. Where necessary, put in place an internal policy or periodic review to handle these issues in the future.

Annex B: Useful contact numbers

National numbers		
National Security Hotline	Tel	1800 123 400
	TTY	1800 234 889
Crime Stoppers	Tel	1800 333 000

Australian Capital Territory
Refer to national numbers

New South Wales		
Counter-Terrorism & Disaster Recovery NSW Premier's Department	Tel Email	(02) 8374 5133 ctdr@premiers.nsw.gov.au

Northern Territory
Refer to national numbers

Queensland		
Refer to national numbers		
Police — Non-life threatening emergencies	Tel	(07) 3364 3555 (Metro) or local police as per phone directory
Infrastructure protection enquiries *(Counter Terrorism Coordination Unit)*	Tel Fax Email	(07) 3364 6791 (07) 3211 4915 counter.terrorism@police.qld.gov.au

South Australia		
Refer to national numbers		
For police assistance to report non-urgent crime	Tel	13 1444 or your local police station

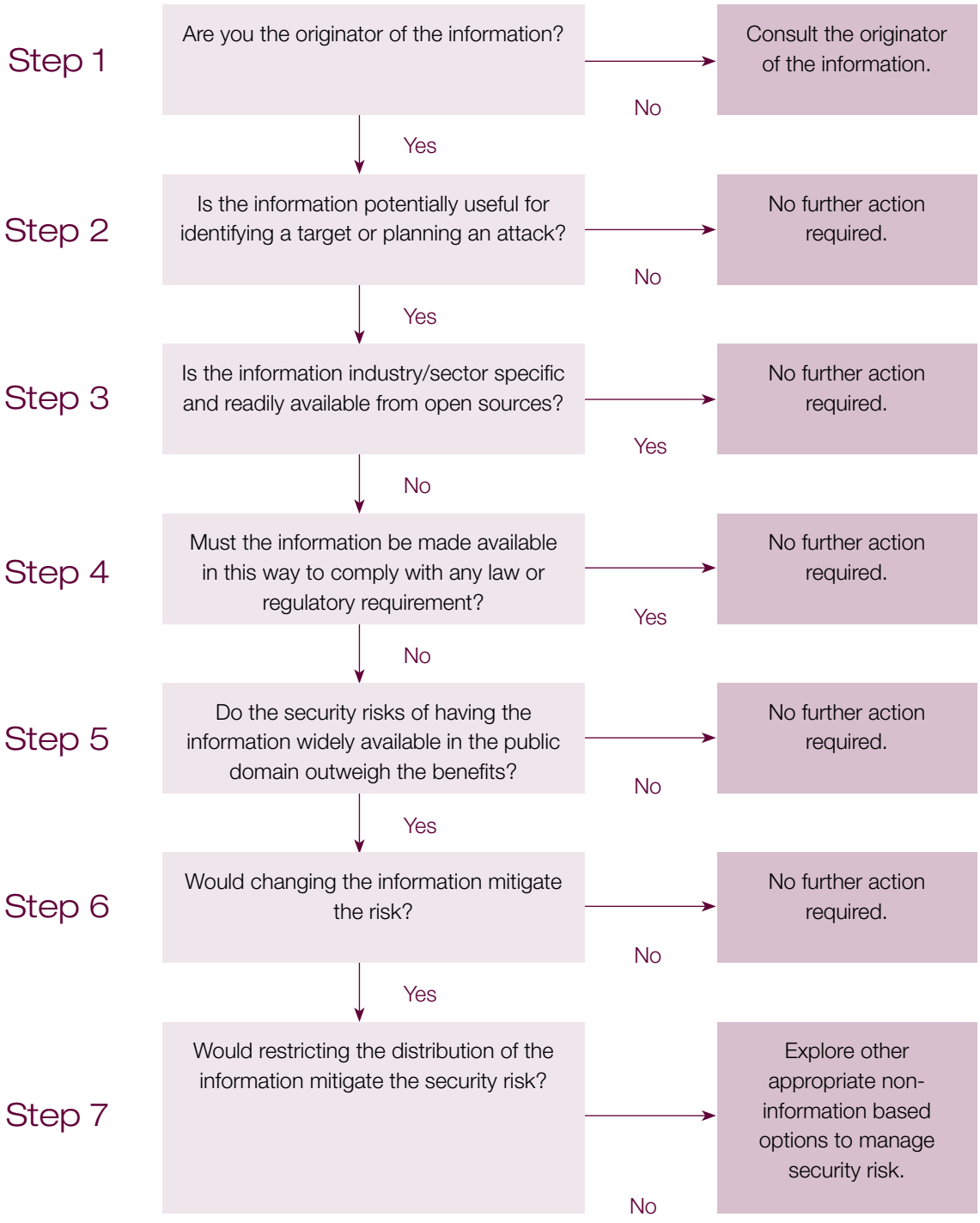
Tasmania		
Refer to national numbers		
Police attendance (for non-urgent matters)	Tel	13 1444
State Security Unit, Tasmania Police	Tel Email Web	(03) 6230 2500 counter.terror@police.tas.gov.au http://www.statesecurity.tas.gov.au
Assistant Director – Counter-Terrorism Security Policy, Department of Infrastructure, Energy and Resources	Tel	(03) 6233 3573

Victoria		
Refer to national numbers		
Victorian Government Safety and Emergencies Site	Web	http://www.safety.vic.gov.au

Western Australia		
Refer to national numbers		
Critical Infrastructure Coordination Unit – Western Australia Police	Email	critical.infrastructure.unit@police.wa.gov.au
Security Planning and Coordination Unit – Department of the Premier and Cabinet	Email Web	spcu@dpc.wa.gov.au http://www.securityplanning.dpc.wa.gov.au

Annex C: A public infrastructure information 'decision tree'

The following is a simplified and adapted version of a 'decision tree for providing appropriate access to geospatial data in response to security concerns', published by the United States National Spatial Data Infrastructure in May 2004. It may need to be adapted further to suit your organisation's needs.



Annex D: Walkthrough examples

Company X maintains a web site profiling its products. The web site includes a 'facts and figures' page that details the physical dimensions and construction specifications of its key production facilities. The page serves no real purpose other than to provide users of the web site with interesting data about the company.

Company X makes an assessment that the benefit of having the information in the public domain is negligible, and that there is a potential security cost in the sense that the information may assist an attacker in selecting a target or planning an attack.

Company X decides to amend the information on its web site to ensure it is more general.

Company Y provides information on request about the location of underground cables to registered excavation contractors. The purpose of providing the information is to prevent accidental damage to the underground cables.

Personnel in **Company Y** note an unusual series of requests from a single user whose registration details appear to be incorrect or incomplete.

Company Y reports the activity to the National Security Hotline.

Company Z is in the business of providing aerial photographs of locations and sites anywhere on the Australian mainland to paying customers.

Company Z is contacted by other organisations concerned about the potential misuse of the photography by criminals or terrorists to attack their facilities.

Company Z is not in a position to assess security risks in respect of other organisations, so it discusses the options with the owners of the facilities and implements a system requiring customers to register their details before photographs can be purchased. It also logs the photographs provided to customers. This information will assist future coordination with authorities or affected organisations to evaluate security risks.

Company A produces a comprehensive asset review report which includes maps, photographs and a detailed inventory.

Due to the sensitive information contained in the report, the Security Information Officer in **Company A** takes a risk managed approach to the report and gives it a classified status.

Company A restricts distribution of the report to management and those officers with a 'need-to-know' through established document management security protocols.

Annex E: Internal security administration and information security procedures

Business owners and operators may wish to consider implementing tighter information security procedures to mitigate the risk of sensitive information being released. Effective information security also enhances the confidentiality, accuracy and integrity of an organisation's information and gives confidence to customers, shareholders and other interested parties. Documents that may provide guidance on information security management are listed in the following annex.

Some suggestions that owners and operators may wish to consider include:

- reviewing the company's information security policy. The policy could address the issues of awareness, privacy, responsibility, behaviour and deterrence, and could define:
    a. the company's dependence on its information resources and the importance of protecting them
    b. who is responsible for ensuring the objectives are met
    c. who is responsible for enforcing the policy
    d. what the agency expects from those who have authorised access to its information resources, and
    e. the consequences for those who breach the policy or circumvent protective security measures
- make staff aware of their responsibilities when handling sensitive information
- implement physical security procedures and systems for classified documents. These measures should not only cover hard and soft copies but also the medium on which the documents are created or contained (eg. protection/sanitisation of hard drives from redundant computers which end up at public auctions)
- consider introducing a 'need-to-know' policy for sensitive documents
- consider appropriate storage and handling of sensitive documents in work areas to ensure that the public are unable to inadvertently access them
- issue guidelines on document protection through suitable formatting, the inclusion of document control, distribution, receipt and destruction protocols, page and copy numbering, classification marking and the creation of a classified document register, and
- ensure companies have the resources available and the ability to identify and investigate security breaches caused by the inappropriate release, handling or loss of documents. The appointment of a Chief Security Officer with responsibility for the management of information security may assist in this area.

Annex F: Further information and advice

Security guidance

On 11 February 2005 the *National Guidelines for Protecting Critical Infrastructure from Terrorism* (the guidelines) was released to assist operators of critical infrastructure develop and implement security planning. The guidelines were developed by the National Counter-Terrorism Committee and endorsed by the Council of Australian Governments.

If your business is an operator of critical infrastructure, your state or territory police service (contact details listed in Annex B) will be able to help you obtain and provide advice on implementing the recommendations of the guidelines.

The threat environment

ASIO and state and territory police services are responsible for collecting and disseminating threat intelligence in Australia. In general they will initiate contact with the affected persons or businesses where there is specific intelligence relating to a particular threat.

General information about the threat environment can be obtained from the national security web site at http://www.nationalsecurity.gov.au or your state or territory authorities as listed in Annex B.

The ASIO Business Liaison Unit (BLU) was established to enhance the flow of national security information to the private sector. The BLU operates a secure website at http://www.blu.asio.gov.au which contains general as well as sector-specific threat information. Instructions for how to obtain log-in access can be found on the website.

Consultation and information sharing

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) consists of a number of consultative groups where businesses with shared threats and vulnerabilities can share information on security planning and risk management. Further information on the TISN can be obtained from http://www.tisn.gov.au

Your relevant industry association and state or territory government may also have information on opportunities for consultation and information sharing on security issues.

Existing documentation on handling public infrastructure data

The United States National Spatial Data Infrastructure has published a guide for US Government providers of geospatial information. This is available at http://www.fas.org/sgp/news/2004/05/fgdc050304.pdf. It encompasses many of the issues raised in this guide.

The United States National Academies Press has published a report entitled *Licensing Geographic Data and Services*. It highlights perspectives and experiences of major stakeholders regarding licensing, whereby the producer of geographic data restricts distribution. An executive summary is available at http://www.nap.edu/execsumm_pdf/11079.pdf

ANZLIC, the Spatial Information Council, published a discussion paper in 2004 on *Access to Sensitive Spatial Data*. It is available at http://www.anzlic.org.au/policies.html

Information security documentation

Standards Australia publishes standards documentation for information security, including *AS/NZS ISO/IEC 27001:2006*, which is the current Australian standard for information security management, and *HB 231:2004: Information security risk management guidelines*, which is a handbook for businesses and organisations of all types and sizes that need to risk manage information. More information is available on the web site of Australian standards distributor SAI Global at http://www.standards.com.au

The Defence Signals Directorate (DSD) in the Department of Defence has developed the *Australian Government Information and Communications Technology Security Manual* (also known as ACSI 33) to provide policies and guidance to Australian Government agencies on how to protect their information and communications technology systems. The unclassified version of the Manual can be accessed at http://www.dsd.gov.au

Privacy

Further information about privacy law is available from the web site of the Office of the Privacy Commissioner at http://www.privacy.gov.au

Legislation

Commonwealth legislation can be accessed though the ComLaw website at http://www.comlaw.gov.au The web site also has links to state and territory legislation.