ABN 31 722 153 579

Approved by ANZLIC Council 16 July 2004

DISCUSSION PAPER
ACCESS TO SENSITIVE SPATIAL DATA

Investigation of issues related to access to sensitive data has identified three key needs:

1. A generic guideline for agencies holding sensitive data;
2. A specific set of issues relating to potential national security restrictions on publicly available data from both government and commercial sources, most notably supply of high resolution imagery and detailed data over security-sensitive sites;
3. Ongoing access to sensitive data needed by emergency management and counter-terrorism agencies for operational purposes.

This discussion paper provides a generic guideline. The other two areas will need to be addressed separately and in more detail. The guidelines will need to be reviewed given experience gained from projects applying spatial data for these purposes.

The need for a policy on access to sensitive spatial data

There are times when certain classes of spatial data need to be withheld from public access and usage. Tracks in forestry areas, location of critical infrastructure, defence establishments, detailed bathymetry of harbour approaches, culturally sensitive sites and location of endangered species have arisen as examples. Relevant factors include privacy and national security.

There are also times when withholding data can degrade decision-making processes, including areas such as emergency planning and response, and environmental management, especially in time-critical situations. It is clear that some data have not been made available to processes carried out in the public interest, such as updating topographic mapping.

While it is recognised that some data cannot be made public because of its sensitivity, the data should still form part of data sets managed by nominated authorities. Authorised users can be given access to it for appropriate purposes, while ensuring privacy, national security or other sensitivities are not compromised. It is ANZLIC's view that the issue is not about whether spatial data should be collected and made accessible, but what restrictions will be applied to its usage and how this should be decided.

The increasing availability of high resolution imagery of the earth's surface brings the issue of access to sensitive data into clear focus. New satellite imaging capabilities showing all visible features to high levels of resolution (anything bigger than half a metre) are available to any users on demand. The resolution is expected to be around a quarter of a metre by 2008. These images are collected and held by both the public and private sectors. There are no existing laws or guidelines in Australia and New Zealand on how this imagery may be made available and used. Issues about access to sensitive data are not widely understood within either the public or private sectors.

There are some analogies to the issues which have already been addressed under privacy legislation. A guide to these issues can be found in the ANZLIC "Spatial Information Privacy Best Practice Guideline". However, the triggers and means of addressing access to data deemed sensitive for other reasons are different to those for privacy.

ANZLIC proposes that a number of policy principles be applied to resolve the issue of collection, management and access to sensitive spatial data and provide certainty to the operations of data collectors, managing authorities and users.

Who is responsible for implementing a policy?

ANZLIC has produced a number of non-binding national policies related to spatial information. As it comprises senior representatives of all Australian governments and the Government of New Zealand, it is able to offer leadership to government agencies on appropriate and effective spatial data policies. Implementation of the policies is the responsibility of individual jurisdictions and their constituent agencies.

Who is covered by the policy?

The policies have been tailored for government agencies within the ANZLIC jurisdictions. Other sectors are invited to consider adopting or adapting these policies, or drafting equivalent policies to suit their circumstances.

Access restrictions on spatial data

Whether certain spatial data are made available or not, and to whom, is the decision of the data custodian (see ANZLIC "Guidelines for Custodianship"). Regrettably, many of these decisions have not been transparent. In some cases it appears that government agencies are making judgements dictated by a desire not to compromise agency operations or relationships with their partners, or to minimise risk of exposing poor data management practices.

However, decisions to withhold data should be based solely on privacy, commercial-in-confidence, national security considerations or legislative restrictions. The decision to withhold needs to be transparent and the criteria on which the decision is made need to be based on a stated policy position.

If data restrictions are to apply, agencies should seek to have these restrictions explicitly contained in a policy document or placed in legislation or regulations that are open to public scrutiny, not left to individual employees to decide on a case by case basis or through institutional inertia.

An alternative to denying access to certain data is to "generalise" or aggregate it to overcome the basis for its sensitivity. Many agencies will supply statistical data which has been derived from the more detailed data collected by surveys. Some agencies will supply data that has lower spatial resolution than the original data collected, such as for culturally-significant sites or locations of endangered species.

It is important that users of spatial data services and products be made aware that certain data has been withheld or modified, since this can limit processes or transactions they are involved in and the quality or utility of the information product produced. One remedy is for data custodians to make clear in publicly available metadata records and as explicit statements on spatial data products that there are limitations applied to the data supplied or shown which could affect fitness for use.

National security considerations

There have always been restrictions placed on release of certain information through mechanisms such as the Official Secrets Act or equivalent. It is not known what spatial data is covered or not covered by these types of mechanisms. In the past, restrictions on sources such as high resolution imagery have been through control of the source itself, usually by the military. More of these types of data are becoming available through other (commercial and governmental) sources. It is known that some restrictions are applied on the commercial data supplier by the US Government through a reporting procedure.

Sensitivities have been heightened by recent terrorist incidents. Potential threats to security could create pressure to restrict access to a wider range of currently publicly-accessible spatial data.

Currently, there are some data types that are available but not currently accessible to a wide audience, such as location and characteristics of critical infrastructure assets. There still remains the issue about who should have access, and when, and that it is important to apply consistent criteria when deciding any restrictions.

Providing access to sensitive data

The Australian Spatial Data Infrastructure (ASDI) sponsored by ANZLIC supports open access to spatial data for all users, wherever possible. However, ANZLIC acknowledges that access to sensitive data may need to be restricted and the issue is who has access and how this is decided.

Given many issues transcend jurisdictional boundaries and institutional 'silos', it is frequently necessary to access spatial data from multiple sources. Accordingly, there needs to be a consistent approach to applying restrictions to the same types of data held by different agencies, enterprises or jurisdictions. For example, it would be counter-productive for some critical data to be available to emergency services in one jurisdiction but not in another. There is a need to apply consistent national access arrangements to agreed spatial data types.

In applying access restrictions for national security or other purposes, it may be necessary for an authority to develop guidelines and negotiate a code of practice with the spatial information industry which deals with managing requests for data lodged with providers in the public, private and research sectors. An example is a request from a client to a private company to provide detailed data over a defence establishment. If guidelines indicate the data is sensitive, the provider may be required to report the request to the proper authority which would then have to deal expeditiously with the report and provide clearance.

On the other hand, there are a number of sensitive spatial data sets that need to be accessed to help manage emergency situations, including data about critical network infrastructures. In some cases, they are held by utilities which are either corporatised government entities or private companies. While cooperation can be requested, there is currently no obligation on these bodies to supply data. Where there is a clear business case for access to sensitive data under specified circumstances, some form of code of practice or regulatory regime may need to be developed that covers all data needed for emergency response management.

In most cases the same collection, management, skills and tools will be used for both sensitive and non-sensitive data. For reasons of economy and efficiency, management and access to sensitive data should be based on the ASDI governance, access, quality, interoperable and integratable guidelines and mechanisms as for all other spatial data, but made accessible only to authorised users.

A number of government jurisdictions have anticipated the need to restrict access to certain sensitive spatial data and are constructing State/Territory spatial data infrastructure systems that have predetermined access rules built into them. The lessons being learned from this experience may be useful nationally.

This issue may be addressed through creation of virtual national repositories, such as a counter-terrorism "data library" which is built "on top" of the ASDI. Access to this data library can then be decided by the counter-terrorism and emergency management authorities within the governance arrangements set down for the data library. A more detailed analysis of the national data library concept was developed as part of the ANZLIC sponsored study into the needs of counter-terrorism agencies.

POLICY POSITION ON ACCESS TO SENSITIVE SPATIAL DATA

Policy guidelines

1. ANZLIC restates its commitment to encouraging open access to spatial data set out in its "Guiding Principles for Spatial Data Access and Pricing Policy".
2. Unless there are specific, compelling reasons to restrict access to spatial data, custodians should provide access for all users to their spatial data holdings under appropriate conditions, in line with the ANZLIC "Guidelines for Custodianship".
3. Decisions on restricting access to data should be based on privacy, commercially sensitive, national security, environmental sensitivity or legislative requirements.
4. Where data are sensitive, custodians should give consideration to providing access to generalised or lower-resolution data that would meet user needs while not compromising any sensitive issues.
5. In applying restrictions on access to their data, custodians should take into account impact of the data not being available for public interest outcomes such as topographic mapping, emergency management, national security and consider providing controlled access for these purposes.
6. If restrictions are placed on access to spatial data, custodians should seek to have these restrictions explicitly contained in a policy document or placed in legislation or regulations that are open to public scrutiny, not left to individual employees to decide on a case by case basis.
7. An overarching principle is that, if spatial data exists, its custodian should advise its existence and any access restrictions in metadata records accessible through the Australian Spatial Data Directory, or equivalent.
8. Data sources having a classification by any government of Secret or above, fall outside these requirements and access will be dictated by the relevant legislation or responsible agency.

Related documents

ANZLIC documents referred to in this policy can be found at www.anzlic.org.au/publications. The study into the needs of counter-terrorism agencies is not publicly available.