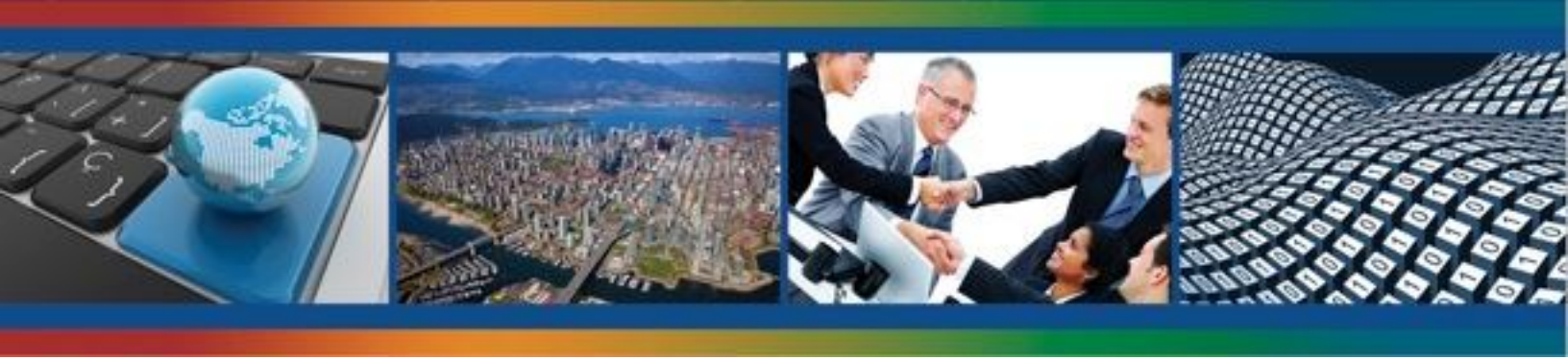

CANADIAN GEOSPATIAL DATA INFRASTRUCTURE
INFORMATION PRODUCT 15

Best Practices for Sharing Sensitive Environmental Geospatial Data

Amec Earth and Environmental

2010

Natural Resources Canada | Ressources naturelles Canada

Canada

BEST PRACTICES FOR SHARING SENSITIVE ENVIRONMENTAL GEOSPATIAL DATA

Version 1.0
2010

Prepared for:
Natural Resources Canada
GeoConnections

Prepared by:
AMEC Earth & Environmental
a division of AMEC Americas Limited

Cet document est disponible en français sous le titre : Pratiques Exemplaires Pour Le Partage Des Données Géospatiales Environnementales Sensibles

For more information about the GeoConnections program and the Canadian Geospatial Data Infrastructure (CGDI) or for additional copies of this document, contact:

GeoConnections Division
615 Booth Street
Ottawa, Ontario K1A 0E9
e-mail: info@geoconnections.org
tel.: 1-877-221-6213
fax: 613-947-2410

Also available on the Internet at www.geoconnections.org

EXECUTIVE SUMMARY

With the advances in geomatics technologies (i.e. applications, data storage capacities and communication bandwidth), the extensive efforts expended in collecting geospatial data (field surveys, monitoring systems, imagery) and the pervasiveness of the Internet, geomatics users expect easy access to an unprecedented variety of geospatial datasets. This expectation is mirrored in the basic principles of most government data management organizations which encourage the sharing of data for the greater societal good.

However, while access to data is increasing, there is also a growing recognition of the extent to which barriers exist in sharing or accessing of sensitive geospatial data. A 2006 Environics survey not only identified the barriers in sharing data (privacy and confidentiality issues, licensing and ownership issues, and liability issues and broader data sensitivities) but found that removing such barriers to sharing data were felt to be the most important data issue to mitigate. In a 2006 workshop facilitated by GeoConnections, communities engaged in land management, environmental impact assessments and sustainable development (collectively referred to as the Environmental and Sustainable Development (E&SD) communities) identified several data sharing issues including the need to develop data-sharing agreements, facilitate open access, conduct further investigations and provide guidance on how to share data of a sensitive nature.

To respond to these needs, GeoConnections contracted AMEC Earth and Environmental to conduct research and stakeholder consultation in supported of the development these Best Practices.

The purpose of these Best Practices is to educate Data Contributors, Owners, Custodians, Stewards and Consumers of the issues and concepts associated with protecting, sharing and utilizing sensitive geospatial data, with a focus on supporting programs, services, businesses and / or applications related to the Environment and Sustainable Development (E&SD) community. The intention is to provide practical guidance to those interested in developing their own sensitive environmental geospatial data sharing policies and protocols.

In reviewing the literature, surveying organizations and practitioners, and through consultation by workshops, it was determined that perspectives range widely on what might be considered sensitive environmental geospatial data. It was also found that there is no consistent mechanism for assessing whether a dataset should be classified as sensitive or not. What was revealed was that the concept of sensitivity changes with context (time and recent events), an organization's regulatory environment (legislation, policy, competition, etc.), jurisdictions and the personal views of Data Contributors/ Owners/Custodians and in actuality, there is considerable intertwining of these elements. Anyone who is assessing a dataset to determine whether it should be considered sensitive or not should be aware of these elements and the potential impact on the credibility of their organization if sensitive data is mistreated.

The first significant question to be answered is "What is sensitive geospatial data?" and how is it determined to be sensitive or not. What defines data as sensitive is related to legislation, regulations and policies governing an organization as well as standards adopted by the organization.

With the focus on the E&SD community, the emphasis is on sensitive "environmental" geospatial data as a subcategory of sensitive geospatial data. The Guidelines consider environmental geospatial data to be thematic geospatial data that could be used for analysis in areas such as environmental impact assessments, land use planning, land management, sustainable development, resource management, airshed management, etc.

Due to the diversity of what can make a dataset sensitive, these Guidelines propose a categorization of sensitivity to assist an assessor (typically the Data Custodian) in understanding which aspect of sensitivity may apply to the dataset they are reviewing. In addition, each organization has to establish and publish its own criteria that allow the assessor to determine whether the dataset being reviewed is sensitive and justify why or why not. These criteria have to be established on an organization by organization basis due to the diversity of the data organizations handle and the specifics of the regulatory environment under which each operates.

It is prudent that each organization develops these criteria independent of any specific dataset, establish them in advance of any dataset assessment, document the criteria and have it vetted by an authorized organizational representative (legal or policy). This step is critical in establishing not only the process but provides a documented baseline for justifying the classifying of a dataset as sensitive if challenged at a later date.

Understanding these categories will also assist in defining the metrics for establishing what is to be considered sensitive data. Data can generally be categorized as sensitive geospatial data if it meets any of the following criteria:

1. *Legislation/Policies/Permits* – the data is identified by legislation as requiring safeguarding. The most prominent legislation in this regard is the federal *Privacy Act* – safeguarding the data is required if an individual can be identified, either directly by georeferenced information (such as the geo-coordinates of an address) or indirectly through the amalgamation of geospatial data and related attributes;
2. *Confidentiality* – the data is considered confidential by an organization or its use can be economically detrimental to a commercial interest;
3. *Natural Resource Protection* – the use of the information can result in the degradation of an environmentally significant site or resource;
4. *Cultural Protection* – the use of the information can result in the degradation of an culturally significant site or resource; or
5. *Safety and Security* – the information can be used to endanger public health and safety.

Numerous articles have identified the need for organizations to establish frameworks for identifying and sharing sensitive data. This need is driven by:

- The requirement to support open government by making data readily accessible unless there is a legitimate and documented reason not to;
- Be consistent within an organization and across jurisdictions so that the mechanisms required to share the data are also applied consistently; and
- Document criteria and processes so that users can search out that the data exists, be made aware of any decisions relating to the safeguarding of the data and know who to contact to request access to safeguarded data.

The Best Practices identify basic principles that can be applied to assessing sensitive environmental geospatial datasets in order to classify sensitivity consistently:

1. Unless the dataset is classified as sensitive it can be provided free of restrictions;
2. Information can not be considered sensitive if it is readily available through other sources or if it is not unique;
3. The Data Custodian of the information is the only agency that can determine whether an environmental geospatial dataset is to be classified as sensitive;
4. Data Consumers of sensitive environmental geospatial datasets must honour the restrictions accompanying the information in the form of an agreement, license and/or metadata; and
5. Organizations should document and openly publish their process, criteria and decisions.

These Best Practices also present an example decision framework for assessing whether an environmental geospatial dataset is to be classified as sensitive. This framework has been adapted from the US Federal Geographic Data Committee (FGDC) document Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns. As the FGDC guidelines are primarily concerned with Security and Public Safety, this framework has been modified to accommodate sensitive environmental geospatial data.

Once a dataset is defined as sensitive and the organization's regulatory environment is understood then the appropriate mechanisms for sharing become apparent. In most cases instruments such as agreements or licenses are sufficient, in other cases the sensitivity must be removed from the dataset before it is shared and in other cases approval is given to a Data Consumer on a case by case basis. Regardless of the mechanism put in place, it essentially comes down to the Data Custodian trusting that the data will be adequately safeguarded by the Data Consumer and the mechanisms they have in place sufficiently limit the risk of inappropriate treatment of the data. Furthermore, there are numerous examples of data collection programs where Data Contributors contribute sensitive data content on a regular basis to the Data Custodian and the Data Contributors trust that their contributions are adequately safeguarded otherwise future contributions may be terminated.

At its core, the successful long term sharing of sensitive environmental geospatial information is about trust, risk management, the credibility of the participating organizations and their overriding desire to disseminate information.

Successful sharing of sensitive geospatial information lies within the mechanisms used to: present the underlying knowledge yet remove the sensitivity; the instrument that defines the conditions of use and protection; and, training of participants to ensure that they are cognizant of their roles and responsibilities. Those sharing or accessing geospatial data may use a combination of mechanisms to ensure data is shared and used responsibly and that the credibility of the process is maintained.

It is intended that these Best Practices provide the reader with sufficient insight and links to resources in order to assist them in implementing a consistent and documented approach to managing and sharing sensitive environmental geospatial data within their organization. The document is intended as a living document, and may be updated as related practices mature and the user-community needs evolve.

Table of Contents

1 INTRODUCTION

1.1 Background to the Best Practices

Sharing Sensitive Geospatial Information

With the advances in geomatics[1] technologies (i.e. applications, data storage capacities and communication bandwidth), the extensive efforts expended in collecting geospatial data (field surveys, monitoring systems, imagery) and the pervasiveness of the Internet, geomatics users expect easy access to an unprecedented variety of geospatial datasets. This expectation is mirrored in the basic principles of most government data management organizations which encourage the sharing of data for the greater societal good. Benefits of sharing geospatial information include:

- Providing an open flow of information between the government and user communities;
- Providing data important to advancing economic and scientific enterprises;
- Providing information needed to implement and enforce laws and regulations for the protection of public health and safety, the environment, land management and other public purposes; and
- Promoting the efficient and effective management and maintenance of data in the public interest including the avoidance of data duplication.

However, while access to data is increasing, there is also a growing recognition of the extent to which barriers exist in sharing or accessing of geospatial data considered to be sensitive. A 2006 Environics survey not only identified the barriers organizations find in sharing data (privacy and confidentiality issues, licensing and ownership issues, and liability issues and broader data sensitivities) but found that removing such barriers to sharing data were felt to be the most important data issue to mitigate.[2] In a 2006 workshop facilitated by GeoConnections, participants engaged in land management, environmental impact assessments and sustainable development (collectively referred to as the Environmental and Sustainable Development (E&SD) communities) identified several data sharing issues including the need to develop data-sharing agreements, facilitate open access, and conduct further investigations and provide guidance on how to share data of a sensitive nature.[3]

To further support the Environment and Sustainable Development community GeoConnections' recognized the need to develop Best Practices to assist organizations in

[1] Geomatics is the science and technology of gathering, analyzing, interpreting, distributing and using geospatial data. Geomatics encompasses a broad range of disciplines including surveying, global positioning systems, mapping, remote sensing and cartography. GeoConnections Glossary http://www.geoconnections.org/en/resourcetool/glossary;jsessionid=97C08C25D19F9681155866D79E8DD0D0.app1#G

[2] Environics Research Group. 2006. Survey of Geographic Information Decision Makers. Prepared for GeoConnections, Natural Resources Canada.

[3] Geospatial Information Needs for Integrated Land/Marine Management (IL/MM) — Workshop Report, Policy Research Institute. 2006, ISBN 0-662-44236-9

developing their policies, procedures and mechanisms to support the sharing "sensitive" environmental geospatial data, over the internet, in Canada.

The purpose of these Best Practices is to educate Data Contributors, Owners, Custodians, Stewards and Consumers of the issues and concepts associated with protecting, sharing and utilization of sensitive geospatial data, with a focus on supporting programs, services, businesses and / or applications related to the E&SD community. These Best Practices:

- Provide an overview of what is considered **sensitive geospatial** information and more specifically what is considered to be **sensitive environmental geospatial** information: and
- Present principles and frameworks for identifying whether content **should be categorized as sensitive** environmental geospatial information and therefore requires safeguarding[4] and mechanisms (agreements, licensing, data and metadata treatments, protocols and/or policies) that enable organizations to meet the inherently conflicting requirements of securing data and making it readily accessible.

The Guideline's scope is focussed on "sensitive" environmental geospatial information composed of operational data used to support environmental assessments, sustainable development and land management. It is not focussed on public health, emergency management, critical infrastructure or national security all of which deal with a considerable amount of sensitive geospatial data. However, where examples, techniques and practices within these sectors that are applicable to the scope of this document they are referenced.

Data or information that is geospatial falls into two broad categories, framework and thematic data:

> Geospatial framework data – is the set of continuous and fully integrated geospatial data that provide context and reference information for the country[5]. These data-sets defining the spatial structure which serves as context for the collection, analysis, and interpretation of social, economic and environmental data and support myriad societal functions; typical framework data includes roads, topography, digital elevation models, political boundaries, typonomy, etc. GeoBase is commonly seen as a portal for Canada's framework data.
>
> Geospatial thematic data – data-sets describing the variation/distribution of a theme across space (e.g. social, economic, environmental indicators, facility locations). GeoGratis and the National Atlas are commonly accessed thematic data portals.

This document addresses geospatial thematic data since framework data are by definition an underlying reference layer and by their nature considered non-sensitive.

[4] In terms of this Guide, safeguarding means the data has to be treated as sensitive and protected from unauthorized access or use.
[5] GeoConnections Framework Data Guide. 2009.
http://www.geoconnections.org/publications/framework_data_guide

GeoConnections contracted AMEC Earth and Environmental to conduct research and stakeholder consultation in supported of the development of these Best Practices. The document has been developed through reviewing literature, surveying organizations and practitioners in Canada, and through consultation by workshops and content critique. The organizations and practitioners that were surveyed and consulted reflect the documents intended audience and are acknowledged for providing valuable insight contributing to these Best Practices (see Appendix E). This document is intended as a living document, and may be updated as related practices mature and the needs of the user community evolve.

GeoConnections

The development of this document has been sponsored by GeoConnections. As a national partnership program led by Natural Resources Canada (NRCan), GeoConnections, has been mandated to promote the use and development of the Canadian Geospatial Data Infrastructure (CGDI). Since 2005 GeoConnections has been focused on four priority areas: public health; public safety/security; sustainable development and the environment and matters of importance to Aboriginal People. The programs objectives are to respond to the needs of the above communities by enabling access to required geospatial data; maintaining, operating and expanding the technological standards and infrastructure required; and supporting consistent geomatics policy development federally, nationally, and locally, to reduce duplication and improve use of geospatial information via the CGDI.

The priority issues addressed by GeoConnections for the E&SD community are related to supporting land-use planning and environmental assessment processes by encouraging the discovery of, access to, use and sharing of geospatial data that support effective decision-making.

Canadian Geospatial Data Infrastructure

The Canadian Geospatial Data Infrastructure (CGDI) operates through collaboration for the effective, efficient discovery and access of interoperable geospatial information, which is achieved through Leadership, Policies, Framework Data, Standards and Technologies, in order to respond to priorities related to the Economy, Environment, Society and Community from local to global.

This Internet/web based infrastructure is comprised of the developments of the federal, provincial, territorial and private sector partners who are collaborating on the technology, standards, access systems, protocols and policies necessary to harmonize Canada's geospatial data, and make these assets available using the Internet.

As such, the CGDI:

- Provides easier access to historical and up-to-date authoritative geospatial framework data maintained by public agencies throughout Canada;
- Facilitates access to leading framework and thematic sources of Canadian geospatial information;
- Increases awareness and understanding of the benefits of the use of geographic information in support of the environment, economy, society and local to global community for the benefit of all Canadians;

- Enables decision-making and policy development to address Canadians' priority issues, such as health, security and safety, cultural, economic, and natural resources;
- Promotes the development and implementation of geospatial standards, specifications and innovative technologies;
- Nurtures partnerships for sharing geospatial information across all sectors, at all levels of government, and internationally; and
- Works to develop and harmonize policies to protect the interests of Canada's citizens and businesses.

The CGDI continues to evolve through national collaboration to develop this online resource for Canadians. The CGDI brings order to the multitude of layers of geospatial information being collected across the country. The CGDI is working to reduce duplication; to identify authoritative sources for geospatial data; and to improve the discovery, access, visualization, and use of data. Tremendous progress has been made to realize the vision of enabling access to the authoritative and comprehensive sources of Canadian geospatial information to support decision-making.

Four of the CGDI's Guiding Principles that are particularly relevant to these Best Practices are[6]:

- **Cooperative:** The CGDI will facilitate the cooperation and collaboration of participating organizations from all sectors, levels of government, and academia;
- **Self-organizing:** The CGDI will enable various levels of participating organizations to contribute geospatial information, metadata, services and applications;
- **Closest to Source:** The CGDI will build upon its principle of self organization by encouraging organizations that are closest to source to provide data. This will increase quality and efficiency by eliminating duplication and overlap; and
- **Secure:** The CGDI will be secure and protect data that is sensitive or proprietary.

1.2 Document Structure

This document consists of four (4) Sections. Section 1: Introduction, has provided a brief background on the issue of sharing sensitive environmental geospatial data and puts context around the role of GeoConnections and CGDI with regard to the sharing of sensitive geospatial data.

Section 2: Sensitive Environmental Geospatial Data, provides greater detail on issues and concepts related to sensitive geospatial data such as the movement to open sharing of data, factors influencing what an organization considers to be sensitive data, definition of sensitive environmental data and examples of potentially sensitive environmental geospatial data. The objective of this section is to provide the reader with an

[6] The Canadian Geographic Data Infrastructure, GeoConnections, 2005, http://www.geoconnections.org/publications/tvip/Vision_E/CGDI_Vision_final_E.html

understanding of what they need to consider in establishing policies, procedures and mechanisms for sharing sensitive geospatial data.

Section 3: Framework for Defining Sensitive Geospatial Data, identifies the commonly held principles associated with assessing whether data should be considered sensitive and provides an example framework for assessing whether data should be classified as sensitive or not. This section also points to examples of other frameworks that are used to assess sensitive data. The objective of this section is to give the reader an idea as to the approaches that can be adapted to meet their specific organizational situation.

Section 4: Mechanisms for Sharing Sensitive Data discusses mechanisms that can be used to allow an organization to at least share the knowledge encapsulated in a dataset which has been identified as sensitive. The objective is to give the reader information to assist them in identifying what mechanism or combination of mechanisms would best support their organization's ability to share sensitive data.

A key appendix is Appendix B, which provides links to key resources (legislation, regulations, policies, etc.) which while not an exhaustive list does provide links to resources essential to an organization implementing sensitive geospatial data assessment processes.

2 Sensitive Environmental Geospatial Data

This section provides an overview of issues and concepts related to sensitive geospatial data. A simple Google search of "geospatial sensitive data" identified dozens of relevant documents. The topics ranged from digital licensing, to steps to take in defining sensitive data, to means of removing the sensitivity from data, to relevant legislation and how a variety of agencies are dealing with the issues. For the purposes of this document the use of the term "sensitive" refers to all geospatial data that may be considered restricted for purposes of dissemination and therefore requires some form of safeguarding.

The purpose of this section is to assist the reader in understanding the context in which to assess whether a dataset that is being reviewed could be determined to be sensitive or not.

2.1 The Movement to Share Geospatial Data

In recent years there has been a growing movement in government agencies that collect and disseminate geospatial data to move away from revenue generation and cost recovery models to a model that emphasizes the societal benefits of disseminating data by making it readily accessible, thereby reflecting governments' philosophies of openness and transparency. This model emphasises that the financial benefits to governments derived from innovation and new services will far surpass any revenue lost from the sale of data. As a result of reducing the cost of data and the licensing restrictions placed on data the consumption of geospatial data has increased dramatically in the past decade.

In fact in the past five years alone the increase in inexpensive or free geospatial data from the private sector (GIS/GPS vendors, open source collaborations, Google Earth and Virtual Earth (BING)) have greatly increased the integration of geospatial data into mainstream business processes and personal activities (witness the extent to which GPS has become a common instrument in vehicles and more recently with Google Street View the ability to see house numbers and people in their front yards).

The principle of interoperability and the ability to share data is at the heart of the world's Spatial Data Infrastructures. The movement to ensure the sharing of geospatial data has become well entrenched in Canada. The 2001 Proposed Canadian Government Action Plan on Geospatial Data Policy states that "Digital geospatial data that are collected by any level of government should be made as readily available electronically to the public as possible by improving access mechanisms and processes, unless there are privacy, security or competitive reasons not to do so."[7] While more generally, the World Wide Web Consortium states that "All data that can be shared with the public should be opened for public dissemination. Data should be published in compliance with applicable laws and regulations, and only after addressing issues of security and privacy." [8]

[7] Proposed Canadian Government Action Plan On Geospatial Data Policy, Canadian Council on Geomatics (CCOG) Annual Meeting Fredericton, New Brunswick 23 October 2001

[8] Publishing Open Government Data W3C Working Draft 8 September 2009 http://www.w3.org/TR/gov-data/

As the last portions of the statements above indicate, along with the move to make data readily accessible there is the recognition that not all data should be unconditionally released. In most organizations' statements supporting the dissemination of geospatial data there is an accompanying reference to the limited need to restrict the distribution of sensitive data. The emphasis is on **limited,** with the resulting issue being not whether geospatial data should be disseminated, but what safeguards are required to protect the inappropriate release of sensitive data.

However, even with the policies, principles and mandates of organizations to share information, barriers still remain. In a survey of Canadian geographic information decision makers conducted in 2006 for GeoConnections, the top issues identified for why geospatial information is not shared included: privacy and confidentiality issues; licensing and ownership issues, and liability issues. The same survey found that removing such barriers to sharing data were felt to be the most important to mitigate.[9] For example, in the 2008 Aboriginal Community Land and Resource Management[10] report, Traditional Ecological Knowledge (TEK), harvest areas and cultural information are considered confidential and an intellectual property right of the community. In many cases the raw digital cultural data are never copied, made public or leave the community. The report recognizes that this results in "a quandary in public planning processes where cultural values need to be shared and weighed equally with economic and environmental interests."

In a 2006 workshop facilitated by GeoConnections, participants engaged in land management and sustainable development in Canada identified data issues, including the need to devise and expand ways to collect and effectively distribute information found in diverse formats, the need to develop data-sharing agreements, the need to facilitate open access, and to coordinate activities to fill critical gaps.[11] Addressing how to share data of a sensitive nature was determined to be an area for further investigation and guidance.

2.2 Factors Influencing Sensitivity

The concept of sensitivity changes with context (time and recent events), an organization's regulatory environment (legislation, policy, competition, etc.), jurisdictions and the personal views of data contributors/stewards/owners/custodians/consumers and in actuality, there is considerable intertwining of these elements. Anyone who is assessing a dataset to determine whether it should be considered sensitive should be aware of these elements.

Context

The context in which one perceives what is sensitive geospatial data and what is not is influenced by time and recent events. The most obvious example of the impact of a recent event and the change over time on the concept of sensitive geospatial data is in the

[9] Environics Research Group. 2006. Survey of Geographic Information Decision Makers. Prepared for GeoConnections, Natural Resources Canada.
[10] Aboriginal Community Land and Resource Management: Geospatial Data Needs Assessment and Data Identification and Analysis, Makivik Corporation, GeoConnections, November 2008
[11] GeoConnections, Natural Resources Canada. 2006. Geospatial Information Needs for Integrated Land/Marine Management (IL/MM) — Workshop Report. http://policyresearch .gc.ca/doclib/SD/SR_SD_GeoConnexions_200610_e.pdf

aftermath of 9/11. The immediate reaction in the US was to focus on the potential use of geospatial information in the planning of terrorist attacks and how this could be prevented. As a result numerous government agencies took steps to protect what they considered to be sensitive data. For instance, high resolution imagery showing military installations or critical infrastructure had these sensitive areas degraded and in many cases datasets were removed from web sites. Other types of datasets that were either removed or the published product modified to remove the sensitive information included energy infrastructure, logging roads, reservoirs, dams, water intakes, databases of water, air, toxics and radiation, and many more.[12]

Subsequent research raised the question as to whether all these data were truly sensitive. A review of the RAND report Mapping the Risks, by Jason Bates[13] indicated that "RAND identified 629 federal databases as likely to contain geospatial information about critical sites and found only four contained information that was not available anywhere else." Sensitive information does not include the fact there is the existence of a facility at a particular place or the general layout of a facility. Care should be taken not to automatically assume that the high cost or accuracy of data means that the data have high value to an adversary.[14]

In line with these observations, organizations have recently released information that was previously classified as sensitive because it was determined that the data was available from multiple other sources. Given the multitude of sources for so much geospatial data there is very little data that is actually unique and therefore the ability to safeguard it by an individual organization is eliminated.

Over time the focus on sensitive data has extended beyond the Public Safety and Security realm. In a discussion paper the Spatial Information Council of Australia and New Zealand (formerly known as the Australia New Zealand Land Information Council (ANZLIC)) [15] extended the sensitive geospatial data concept to include datasets such as "tracks in forestry areas, location of critical infrastructure, defence establishments, detailed bathymetry of harbour approaches, culturally sensitive sites and location of endangered species as geospatial datasets that need to be withheld from public access." The paper indicates there are situations where withholding data degrades decision-making processes, such as in emergency planning and response, and environmental management, especially in time-critical situations. While it is recognised that some data "cannot be made public because of its sensitivity, the data should still form part of datasets managed by nominated authorities. Authorised users can be given access to it for appropriate purposes, while ensuring privacy, national security and other sensitivities are not compromised."

The Best Practice is that **what is considered sensitive today may not be sensitive tomorrow and vice versa and while one can not account for context while assessing the sensitivity of their dataset it should lead an organization to review their datasets on a periodic basis to determine whether the context has changed over time.**

[12] Mapping Secure Boundaries for Data, Pinkster, L., GeoTimes, April, 2003.
[13] Guidelines Needed for Geospatial Data on Internet, J. Bates, June 2004
[14] Making Decisions About 'Sensitive' Geospatial Data - EIIP Virtual Forum Presentation, Domaratz, M., National Geospatial Programs Office U.S. Geological Survey, Nov. 2005
[15] Access to Sensitive Spatial Data, Discussion Paper, ANZLIC, July 2004

Organization's Regulatory Environment

The governance environment in which an organization operates is dictated by the complex set of legislation, policies, mandates, guidelines, agreements and standards by which it abides. The most powerful of these elements is the legislation governing an organization.

Without exception the most far reaching set of legislation concerning sensitive data are the privacy legislation, including the federal *Privacy Act*, the private sector equivalent *Personal Information Protection and Electronic Documents Act* and their provincial and territorial counterparts. These privacy laws and policies regulate the collection, use and disclosure of personal information by government and govern the manner in which personal information is managed by the private sector.[16]

In relation to personal information, it is the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others. Confidentiality is a third-party obligation to protect the personal information with which it is entrusted. It is a duty of care to maintain the secrecy of information, and not misuse or wrongfully disclose. Security (in terms of these Best Practices security is generally referred to as safeguarding) is the process or manner of assessing the threats and risks posed to information and taking the appropriate steps to protect the information against unauthorized access, use, intrusion, loss or destruction.

There is often confusion about the differences between privacy, confidentiality and security. More specifically, confidentiality and security are often confused with "privacy protection". So the distinctions are significant: privacy, a fundamental right; confidentiality, an obligation to protect information; and, security (safeguarding), the process of protection.[17]

Within the Canadian federal government the Treasury Board of Canada Secretariat requires that all databases be subjected to a Privacy Impact Assessment prior to being developed and the data collected. This process ensures that the sensitivity of the data is well understood within the context of the *Privacy Act* and that appropriate safeguards are taken to protect the sensitivity of the data.

To demonstrate how privacy can be impacted by geospatial data, the Best Practices Guide Spatial Information — Privacy Issues[18] states that there are two fundamental risks to privacy associated with improvements to the access and usability of public sector spatial information.

First, there is the risk that personal information collected in land dealings, property transactions, and land regulation and administration can be used for purposes that are unrelated to the purpose for which it was originally provided. Examples include:

- Using name and contact information for direct marketing;
- Searching for and locating individuals either for malicious purposes or out of simple curiosity; and

[16] Treasury Board Privacy Impact Assessment Policy, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450
[17] Health Canada Privacy Impact Assessment (PIA) Tool Kit – Nov. 2006
[18] Best Practice Guideline Spatial Information—Privacy Issues, ANZLIC Council, Feb. 2004

- Compiling profiles or dossiers by combining the information with personal information from other sources in order to make decisions about the person's access to services, suitability for employment or eligibility for other opportunities.

This risk has always existed. Technological developments, and especially the provision of this information online, have increased it considerably.

Second, there is the risk that spatial information containing no personal information can be manipulated and combined with other information to reveal details about an identifiable individual. Examples include:

- Person location tracking using mobile communication media; and
- Data matching using the person's address as a common identifier.

In support of open government and transparency there is the federal *Access to Information Act* and its provincial equivalents. The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government.

These acts identify, in varying levels of specificity, what type of information can be with held from release to the public, but they also require an organization to identify why any information can not be released.

Apart from privacy and access to information legislation there are numerous other acts that impact what an organization may consider to be sensitive data. Other examples of relevant Canadian legislation include the federal *Species At Risk Act* (SARA), Ontario's *Endangered Species Act* (note other provinces have similar acts), the *Canadian Environmental Assessment Act* (CEAA), provincial clean water acts, as well as federal, provincial and territorial archaeological sites regulations.

The species at risk acts generally have three main goals:

- to prevent endangered or threatened species from becoming extinct or extirpated;
- to help in the recovery of endangered, threatened and extirpated species; and
- to manage species of special concern to help prevent them from becoming endangered or threatened.

Once a species is listed under the *SARA*, it becomes illegal to kill, harass, capture or harm it in any way. Critical habitats are also protected from destruction.

The debates organizations have with regard to releasing sensitive biological or cultural data is whether the release the data would be beneficial to the resource or not as the acts are not specific as to how the data should be treated. On the one hand, by releasing the location of sensitive resources it could lead to destruction of the resource or habitat, trespassing on private property and/or impact property values. The resource destruction and trespassing could be the result of either intentional (e.g. poaching) or unintentional

(e.g. overzealous ecotourism) activities. Property values could be impacted if rare species are on the property as future development would be restricted. In some cases property owners have been known to destroy rare habitat to protect their property values and in other cases landowners refuse access to conduct biological surveys so that rare species are not identified on their property.

On the other hand, releasing the location of rare species or resources could provide protection through the public awareness and presence reducing the opportunity for intentional or unintentional destruction.

Organizations such as NatureServe, the provincial Conservation Data Centers, archaeological organizations and the Canadian Wildlife Service have had to address these issues.

In addition to legislation there are policies, guidelines, standards and agreements that bind an organization to a particular behaviour. For instance organizations that are members of the Global Biodiversity Information Facility (GBIF) should incorporate the Guide to Best Practices for Generalizing Sensitive Species Occurrence Data[19] when assessing their datasets. As Canada is a member of the GBIF, anyone assessing any biodiversity related data should be familiar with this guideline.

Within the Canadian federal government, agencies that are collecting information from the public must obtain "informed consent". They must inform those from whom they are collecting data of the purpose for the data collection and how it will be used. In turn, despite the potential value of this data to other users, the data can not be shared with any other organization (or even with other units within the organization) for use for anything other than supporting its stated purpose.

The resulting guideline is that **in order for someone to determine whether any data they are assessing is sensitive they need to understand the various regulations governing their organization. This requires a concerted education process for the Data Custodian to ensure they fully understand the implications and in many cases contradictions, of their regulatory environment.**

Appendix B provides a limited list of relevant legislation, regulations and policies that anyone establishing a sensitivity assessment process should consider.

Jurisdictions

It is important for those dealing with assessing the sensitivity of data that the interpretation of sensitivity varies between jurisdictions.

Drawing upon privacy legislation for example, while most jurisdictions have some form of privacy legislation, the interpretation varies from jurisdiction to jurisdiction. For instance, the Canadian Privacy Commissioner has placed a much more restrictive interpretation on how georeferencing addresses impacts privacy than does the Australian Commonwealth Privacy Commissioner. Currently in Canada federal agencies can not share addresses as it is too easy to compile data based on an address and create a dataset that violates a

[19] Guide to Best Practices for Generalizing Sensitive Species Occurrence Data, Chapman, A. and Grafton, O., GBIF, 2008

person's privacy. The Australian interpretation is that an address in and of itself does not violate privacy, it is the downstream users that append information that have to manage the privacy issues. As a result Australia has a shared national address database amongst its various federal and state departments, Canada does not.

An example more directly related to the environment is that the abundance of a species can vary quite drastically over its range. The result is that a species that is abundant in one jurisdiction may be rare or endangered in another jurisdiction. Researchers could find themselves with very detailed species location data in one area and very generalized information in another area. These differences could greatly impact their analysis techniques and research approach. More importantly, the resulting product may not be appropriate if the analyst did not recognize the differences in the resolution of the data.

As a Best Practice **those that are assessing datasets for sensitivity should be aware of how other jurisdictions, and more particularly adjacent jurisdictions, view the sensitivity of the same information.** While this knowledge does not change the regulatory environment under which the assessment is being made, it should lead to discussions between the jurisdictions as to how best to share data that would contain the knowledge that would be of benefit to both jurisdictions or other external users.

In fact, there is "the need to work with "neighbors" to avoid circumstances in which different organizations make contradictory decisions."[20] While from ANZLIC's perspective, 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. [21]

Competition

An issue of significance to the private sector is the release of information by government that could put them at a competitive disadvantage.

This has been widely discussed within the critical infrastructure and emergency management arena for many years. In the 2005 GITA paper, Identifying Critical Infrastructure, it states that in the United States:

> Traditionally the private sector has had concerns with sharing data with public agencies, namely because the data may become subject to the Freedom of Information Act (FOIA) and thus available to competitors. It can be argued that private critical infrastructure data is not subject to FOIA because an exemption protects private companies against disclosures of trade secrets and confidential business information.
>
> Address information, land base mapping and associated orthophotography may not contain sensitive critical infrastructure data, but they are decidedly competitive assets to a private company. If this noncritical data is shared

[20] Making Decisions About 'Sensitive' Geospatial Data - EIIP Virtual Forum Presentation, Domaratz, M., National Geospatial Programs Office U.S. Geological Survey, Nov. 2005
[21] Access to Sensitive Spatial Data, Discussion Paper, ANZLIC Council, July 2004

> with the government, it is possible to become subject to FOIA–a concern to infrastructure owners. To obviate the problem, many infrastructure owners are using data license agreements that allow sharing and updating of land base mapping information that prevent the data from entering the public domain.[22]"

Other areas of competitive geospatial information include themes as varied as detailed forest inventories, exploration areas and unsettled land claim information.

Another area of concern is the inappropriate release of land use management plans, particularly those that impose land use restrictions, such as establishing a new national park. If such information is released without sufficient understanding of what the data represents then misinterpretation could have significant impacts. For instance if a land use/zoning master plan dataset is released that is not clearly defined as candidate areas rather than final selection areas, the value of the candidate land that does not make the final selection could be negatively impacted.

As a Best Practice **the Data Custodian of the data must understand any confidentiality associated with the data whether it is explicitly stated in an agreement or implicit in the economic implications of the information.**

Roles and Responsibilities

Despite the regulatory environment and the other elements discussed above, the views of the individuals involved will always come into play in assessing sensitivity.

A question that often arises is who owns the data – is it the individual who collects the data or the organization funding the collection or the organization that is the custodian of the data? While for the most part it is quite clear as to the owner of the data, which is generally the organization funding the data collection, there are situations where individuals may have, or claim, ownership of the data. These situations generally occur in a research environment.

In a research setting (government as well as academic) where researchers have the requirement to "publish or perish", researchers are often reluctant to share data prior to publication. In many cases they hold on to the data for years and may not even release the raw data once the paper has been published. The claimed sensitivity of the data is often used as the reason for not sharing the data. If the data is owned by the organization then steps could be taken to enable the sharing of the data without endangering the ability of the researcher to publish.

Even in situations where ownership of the data clearly resides with the organization, individuals may develop a sense of ownership of the data and may be reluctant to share out of stubbornness or as some may rightly or wrongly claim, the end users do not know how to use the data and may misuse it.

For these reasons it is essential to understand and establish the roles and responsibilities of those that participate in the collection, validation, maintenance, dissemination and

[22] Identifying Sensitive Critical Infrastructure Data, Jones, B., GITA, 2005

utilization of the data, as well as the assessment of sensitivity. For the purposes of these Best Practices the roles are as follows:

- **Data Steward** – is the role that is considered the **Data Owner** of a geospatial dataset/product and is responsible for creating or maintaining (up-dating, editing) the dataset/product including defining any techniques to desensitize copies of the source data for dissemination purposes;
- **Data Custodian** - is the role that is responsible for safeguarding corporate data. This function includes managing geospatial data to ensure it is accessible by the user community, appropriate security and dissemination restrictions are in place, meets data structure and quality standards, is properly managed with regard to accepting new datasets or revisions of existing content, protection, back-up, recovery and archiving. It is this role, in collaboration with the Data Steward and Data Contributor that is responsible for ensuring the data's sensitivity is properly assessed and documented and when necessary, assessing any Data Consumer data requests;
- **Data Contributor** – is the role that collects and submits portions of, or individual records of a dataset. They abide by the standards and processes set out by the Data Steward and contribute their data through the Data Steward; and
- **Data Consumer** – is the role that requests access to the data on a one time or ongoing basis. They are obligated to abide by any agreements, licenses or restrictions attached to the data.

As a Best Practice **it is incumbent upon an Organization to have well established definitions of roles and responsibilities so that personal views can be eliminated from the assessment process**.

Risk Management

Ultimately the issue is the balancing of the objectives of making geospatial data as readily available as possible versus the need to safeguard sensitive data. In order to manage this balancing of objectives the questions that must be addressed are:

- What is considered sensitive geospatial data?
- How does one determine whether a dataset is sensitive?
- What are the options for sharing sensitive data with confidence that it does not violate regulatory obligations and that it will be properly safeguarded by the Data Consumer? and
- What are the implications if the data is inappropriately disseminated or miss-used?

The nature of the mechanisms by which data is shared is based on the perceived impact of releasing the data such as the risk of the data being used inappropriately, or of an unauthorised release of the data, or of an infringement on privacy. There are two aspects to the risk. One is the potential violation of the regulatory governance of the organization and any resulting legal or disciplinary fall out and the second affects the underlying credibility of the organization and more specifically the program associated with the data. In some cases the long term viability of the dataset may be jeopardized if Data

Contributors decide to no longer continue providing the source data. For instance, if sensitive species data is no longer reported by concerned Data Contributors, the source database will degrade over time as trends and population counts can no longer be assessed.

Both types of **risk are best mitigated by applying standards and processes, at least within an organization, by which environmental geospatial data can be consistently assessed as to its sensitivity**. In order to demonstrate consistency and transparency the literature suggests that all assessments **should be documented** and made available, primarily through catalogued metadata. By making the results available, potential users of the data can at least determine that it exists and then take the steps to determine how and/or if they can access it in some controlled manner.

It is the understanding of these factors influencing the concept of sensitivity as it applies to a specific organization and dataset and adopting the suggested Best Practices that will ensure a consistent review process that will mitigate the risk factors.

2.3 Definition of Sensitive Environmental Geospatial Data

The first significant question to be answered is "What is sensitive geospatial data?" and how does a Data Custodian determine whether data can and should be considered "sensitive"?

What defines data as sensitive is related to legislation, regulations and policies governing an organization as well as standards adopted by the organization.

With the focus of these Best Practices are on the E&SD community, the emphasis is on **sensitive environmental geospatial** data as a subcategory of the larger subject of **sensitive geospatial** data. These Best Practices consider environmental geospatial data to be thematic data that could be used for analysis in areas such as environmental impact assessments, land use planning, land management, sustainable development, resource management, airshed management, etc.

Due to the diverse factors influencing sensitivity these Best Practices propose a categorization of sensitivity that will assist a Data Custodian in understanding which aspect of sensitivity may apply to the dataset they are assessing. In addition, each organization has to establish its own criteria for each category that further allows the Data Custodian to determine whether the dataset can be classified as sensitive and justify why or why not. This has to be done on an organization by organization basis because each organization operates under it own specific regulatory environment.

It is prudent that each organization develop and document its own environmental geospatial data sensitivity criteria independent of any specific dataset, in advance of any assessments, and have them vetted by an authorized organizational representative (legal or policy). This step is critical in establishing the mechanism for assessing whether a dataset is sensitive and provides a documented baseline for justifying the classifying of a dataset as sensitive if challenged at a later date.

Understanding these concepts will also assist in defining the metrics for establishing what is to be considered sensitive data.

2.3.1 Categories of Sensitivity

While there is considerable documentation on sensitive environmental areas, research has indicated that there is no clear definition of "sensitive environmental" geospatial data. The research has also shown that there is a diverse set of data that is considered **sensitive environmental geospatial** data and that categorizing these data could assist organizations in understanding the nature of the sensitivity within their data holdings.

Based on an assessment of the research conducted for this project, data can generally be categorized as **sensitive geospatial** data if it meets any of the following criteria:

1. *Legislation/Policies/Permits* – the data that is identified by legislation as requiring safeguarding. The most prominent legislation is the *Privacy Act* – an individual can be identified, either directly by georeferenced information (such as the geo-coordinates of an address) or indirectly through the amalgamation of geospatial data and related attributes;
2. *Confidentiality* – the data is confidential to an organization or its use can be economically detrimental to a commercial interest;
3. *Natural Resource Protection* – the use of the information can result in the degradation of an environmentally significant site or resource;
4. *Cultural Protection* – the use of the information can result in the degradation of an culturally significant site or resource; or
5. *Safety and Security* – the information can be used to endanger public health and safety.

The issue with **sensitive geospatial** data is, by releasing specific geospatial data beyond the control of the Data Custodian, there is a potential for one of the above principles to be violated if appropriate safeguarding is not maintained. For example, in the case of Cultural Protection, there is a concern that archaeological sites could be disturbed if their locations are published with enough detail to allow people to find the site. In fact, even archaeologists have to apply for a permit to look at, walk on or dig at a site.

2.3.2 Standardizing Approaches to Defining Sensitive Data

Numerous authors and agencies have identified the need for organizations to establish frameworks for identifying sensitive data and determining how or whether to share it. E.M. Power wrote in Acting Responsibly with Geospatial Data[23] that "Organizations must recognize that geospatial data can be created to contain highly sensitive data and that responsible handling of such data will not detract from a firm's commercial opportunities-in fact, it could help it avert severe reputation damage. Originating organizations will find that as the data they handle become increasingly sensitive, the procedures for deciding whether to withhold or change such data before their release must be well-established and periodically revised to ensure that organizations handle such data responsibly." In the RAND report Mapping the Risks Assessing the Homeland Security Implications of Publicly

[23] Acting Responsibly with Geospatial Data, IEEE volume 3 issue 6, E.M. Power, November 2005

Available Geospatial Information[24], "they developed a framework of three-steps – usefulness, uniqueness, and benefits and costs – for assessing the implications of making such information available".

The article Guidelines Needed for Geospatial Data on Internet quotes the Co-chair of the US Federal Geographic Data Committee (FGDC) Homeland Security Working Group, "If we can help people think through whether the information is sensitive and unique, it can help with the tough question of whether access should be restricted… We want people using the same metrics to see if their data is sensitive". [25]

Organizations have addressed this call by developing guidelines and best practices. In 2005 the FGDC released the Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns[26]. The document provides a thorough risk analysis for all government agencies to use in deciding whether or not to publish geographic data on the Internet. The focus of this document and much of the US activities is related to national security. The guidelines are to assist agencies in setting local policy regarding access to geospatial data that may appear sensitive.

The Australian and New Zealand Information Council have published several documents in the past decade discussing aspects of assessing sensitivity (ANZLIC Spatial Information Privacy Best Practices Guideline (2004), Guidelines for Custodians (1998), Guiding Principles for Spatial Data Access and Pricing Policy (2001) and, Access to Sensitive Spatial Data – discussion paper (2004)). The 2004 ANZLIC discussion paper[27] stated that 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. Access arrangements should recognize confidentiality, privacy, security and intellectual property rights. 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.

The following are examples of a variety of frameworks that have been applied to various aspects of sensitive geospatial data.

Example Framework 1:

In 2008 the Global Biodiversity Information Facility (GBIF) published their best practices for generalizing sensitive species occurrence data.[28] The guide is intended for institutions, data providers and GBIF nodes to use in the development of their own in-house guidelines.

The guide defines four steps in assessing sensitivity by determining:

[24] Mapping the Risks Assessing the Homeland Security of Publically Available Geospatial Information, Baker, J., Lachman, B., Frelinger, D., O'Connell, K., Hou, A., Tseng, M., Orletsky, D. and Yost, C., , RAND Corporation, 2004.
[25] Guidelines Needed for Geospatial Data on Internet, J. Bates, June 2004
[26] Guidelines for Providing Appropriate Access to Geospatial Data In Response to Security Concerns, Federal Geographic Data Committee, June 2005
[27] Access to Sensitive Spatial Data, Discussion Paper, ANZLIC Council, July 2004
[28] Guide to Best Practices for Generalizing Sensitive Species Occurrence Data, Chapman, A. and Grafton, O., GBIF, 2008

1. Risk of Harm – an assessment of whether the taxon is subject to harmful human activity;
2. Impact of Harm – an assessment of the sensitivity of the taxon to the harmful human activity;
3. Sensitivity of Data – an assessment on whether the release of data will increase harm; and
4. Decision on Release & Category of sensitivity – a balanced decision regarding the release of the data and determination of the category of sensitivity, and thus the level of generalization, of the data for release.

In support of step 4 above, the guide identifies techniques for restricting or generalizing disseminated textual (e.g. remove attributes, provide higher taxon name, insert standard statements) and spatial (e.g. link to an administrative/ecological unit, georeferenced to a rounded degree, the more sensitive the higher the rounding) information. The guide defines the need to document the method and level of generalization applied so that Data Consumers are aware of what was done and how reliable the released dataset is.

Example Framework 2:

The Ontario government has identified three levels of sensitivity that are applied across all of their datasets. Using the Ontario Ministry of Natural Resources (OMNR) as an example[29]:

1. High sensitivity is used for information or material assets that are extremely sensitive and are intended for use by named individuals (positions) only. This category refers to information that could have negative impacts on human life or health, if released. Currently there are no geospatial data classes that fit into this category within OMNR.
2. Medium sensitivity is used for information or material assets that are sensitive within the Ontario Public Service, are intended for use only by specified groups of employees and approved agents of the Crown. In the context of OMNR data, this refers to information where the entire data type has been flagged in the database as sensitive, this would include all species at risk as identified under the Endangered Species Act.
3. Low sensitivity classification is applied to sensitive features within a data type that are not normally sensitive. An example would be specific occurrences of Pileated Woodpecker nests. In most parts of the province, these would not be tagged as sensitive, however, there are locations where these are deemed to be a greater concern, and are therefore, tagged as sensitive by the local data maintainer.

Example Framework 3:

The Government of Canada has introduced its policy and guidelines for Privacy Impact Assessments[30] that all federal government departments and agencies must follow. The purpose of the assessment is to ensure all government programs and databases have been adequately assessed for privacy in terms of data collection process, database design, data

[29] Guide Survey, GeoConnections, 2009
[30] Privacy Impact Assessment – http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450

validation and QA, database implementation, maintenance and on going operations. The assessment includes documenting business processes (using charts or descriptions), documenting data flows (using diagrams, tables and charts to illustrate), analyze privacy (using a Privacy Analysis Questionnaire along with supporting references and documents), develop a risk management plan (use a table identifying risk, context of the risk, likelihood of it happening, impact significance and mitigation options) and developing a final report.

The significance of the Privacy Impact Assessment is that by doing the assessment up front issues are identified early and steps can easily be taken to modify processes and database design to eliminate or more easily manage the privacy/sensitivity issues before the process has been implemented.

Example Framework 4:

As evidenced by the Aboriginal Community Land and Resource Management review and the First Nations Regional and Inuit Longitudinal Health Survey (RHS), First Nations have taken considerable interest and active ownership of information concerning their communities, particularly in terms of health, culture and environment. In response to the RHS, the First Nations Centre developed the Ownership, Control, Access and Possession[31] (OCAP) principles. The OCAP principles apply to all research, data or information initiatives that involve First Nations. The principles represent a comprehensive framework developed by First Nations to bring self-determination into the realm of research and information management. Of specific relevance to this project is the Data-Sharing Protocol[32] between the First Nations and research partners. It establishes ownership of the data, including how and under what conditions the data may be shared. The protocol also sets out the principles and obligations that partners must adhere to when they collect, use, store and disclose individual or aggregate information.

A key aspect of these example frameworks is the documenting of the sensitive data is to be safeguarded. Originating organizations that restrict data should have written policies that identify what are the data that can be accessed, used, and/or redistributed, the conditions under which these actions may occur, and the organizations that are permitted to access, use and redistribute the data. Include these terms and conditions with the transfer instrument to ensure that the Data Consumer is aware of any restrictions. Care should be taken to ensure that the release of data does not enable others to force additional dissemination of the data under freedom of information laws.[33]

2.4 Potentially Sensitive Environmental Geospatial Data

This section provides some examples of what may be considered sensitive environmental geospatial data. These examples are provided within the context of the five proposed categories of sensitivity. As stated, these Best Practices consider environmental geospatial

[31] Ownership, Control, Access and Possession Sanctioned by the Fist Nations Information Governance Committee, First Nations Centre, National Aboriginal Health Organization, 2007 - http://www.naho.ca/english/pub_research.php

[32] Considerations and Templates for Ethical Research Practices, First Nations Centre, National Aboriginal Health Organization, 2007 - http://www.naho.ca/english/pub_research.php

[33] Mapping the Risks Assessing the Homeland Security of Publically Available Geospatial Information, Baker, J., Lachman, B., Frelinger, D., O'Connell, K., Hou, A., Tseng, M., Orletsky, D. and Yost, C., , RAND Corporation, 2004.

data to be thematic data that could be used for analysis in areas such as environmental impact assessments, land use planning, land management, sustainable development, resource management, airshed management, etc. The sensitivity may reside in the location of the data element or the attribution of the element, both need to be considered.

The following list of examples is by no means exhaustive, nor necessarily considered sensitive in all jurisdictions, however it does provide an indication of the type of information one should consider as potentially sensitive:

Legislation/Policies/Permits

- Person's name: privacy legislation;
- Address: privacy legislation;
- Birth Date: privacy legislation;
- Data from biological collection forms/permits:
    - Collector's number;
    - Taxonomic name;
    - Habitat;
- Data from archaeological collection forms/permits:
    - Collector's number;
    - Collectors Name;
    - Method of determination;
    - Textual location descriptions;

Confidentiality

- Land holder information: can be used for commercial advantage;
- Property values: can be used for commercial advantage;
- Mineral assessment tracts: misrepresentation of this information can result in misleading or misinterpreted land use planning assessments;
- Fisheries information: misrepresentation of this information can result in misleading or inaccurate interpretations (particularly in environmental assessments of an area or project);
- Trails: off-road trails that have been GPS'ed can be sensitive information as increased use of certain trails can result in liability issues (forestry, mining roads, etc.);
- Forest inventories: can be used for commercial advantage;
- Contaminated sites: liability issues for reporting organization;
- Point source air emissions: provided in confidence by organizations;
- Oil, gas and mining exploration sites: can be used for commercial advantage;
- Unsettled Land Claims: surveyed and un-surveyed First Nation settlement lands are extremely sensitive topics and can have direct bearing on land use planning, mineral exploration, tourism, outfitting and other industries/fields of interest;
- Environmental incidents: could result in legal action;
- Logistical information supporting research: puts equipment at risk of vandalism or theft;
    - Location of field equipment and sensors;
    - Location of fuel caches;

Resource Protection

- Sensitive habitats: places individuals, populations or residences of a species at risk to disturbances, disruption of conservation efforts, destruction of habitat;
- Rare and endangered species locations: places individuals, populations or residences of a species at risk to disturbances, disruption of conservation efforts, destruction of habitat
- Habitats of species of economic value: places individuals, populations or residences of a species at risk to over exploitation, trespassing;
- Fossil Sites: providing coordinates to fossil locations could result in the commercialization &/or destruction of the resource, trespassing issues;
- Trails (lines): off-road trails that have been GPS'ed can be sensitive information as increased use of certain trails can result in environmental degradation (erosion, etc.;)

Cultural Protection

- Archaeology site locations: places sites at risk of disturbance, destruction of historical record and theft of artefacts, trespassing;
- Ceremonial and Sacred Sites: Aboriginal community owned data;
- Cultural Typonomy: Aboriginal community owned data;
- Occupancy Areas: Aboriginal community owned data;
- Travel and Trade Routes: Aboriginal owned data and places area at risk to over exploitation; and
- Use and Harvesting Areas: Aboriginal owned data and places area at risk to over exploitation.

A particularly large body of sensitive data resides in First Nations cultural data. As pointed out in the Aboriginal Community Land and Resource Management report, community owned data, for example Traditional Ecological Knowledge (TEK) and land use and occupancy data are highly confidential and it is not shared or is shared only within a small group of users within a community. These data account for 18% of all thematic data used by First Nations geomatics analysis and were ranked as highly sensitive. [34]

Safety and Security

- Wellhead and intake protection zones;
- Contaminated sites; and
- Potential pipeline/railroad/electrical infrastructure (lines): potential infrastructure plans can impact local communities and cause political and environmental issues.

[34] Aboriginal Community Land and Resource Management: Geospatial Data Needs Assessment and Data Identification and Analysis, Makivik Corporation, GeoConnections, November 2008

3 Framework for Defining Sensitive Geospatial Data

This section puts forward a framework that an organization may use as a guideline for establishing and documenting the details of their own procedures and protocols.

3.1 Principles Related to Sensitivity Assessment

The following principles provide direction and reasoning for the decision making process presented in Section 3.2 and are drawn from the Best Practices identified in Section 2.0.

Basic Principles

The basic principles to be applied to assessing sensitive environmental geospatial datasets are:

Principle 1: Share the Data

Commitment to encouraging access to spatial data and unless the dataset is classified as sensitive it will be provided free of restrictions. The generally accepted fundamental principle in sharing geospatial information generated with public funds is:

> Digital geospatial data that are collected by any level of government should be made as readily available electronically to the public as possible by improving access mechanisms and processes, unless there are privacy, security or competitive reasons not to do so.[35]

This principle is recognized in the general statutory and administrative frameworks for the dissemination of government information. It ensures that without an acceptable reason (privacy, security, competitiveness) a Data Custodian can not arbitrarily decide not to share the data. In fact, the emphasis is when in doubt, share openly.

Principle 2: Data Uniqueness

Information can not be considered sensitive if it is readily available through other sources or if it is not unique. This principle is based on the fact that if data is readily accessible then there is little point in expending the effort and cost of safeguarding the data when the information is already in the public arena.

Principle 3: Standardize the Approach

Standardize metrics for assessing sensitivity based on the organization's regulatory environment, conduct assessments early in the data design process and review on a periodic basis.

[35] Proposed Canadian Government Action Plan On Geospatial Data Policy, Canadian Council on Geomatics (CCOG) Annual Meeting Fredericton, New Brunswick 23 October 2001

In this era of openness and transparency in government it is essential that any decisions to safeguard data are justified and supported by a process that is consistent and repeatable, while accommodating all relevant legislation, regulation, policies and standards governing an organization. Establish the process independent of any specific dataset so that the framework is not limited when additional datasets come along. Execute the process early in the conceptualization and creation of a dataset so that sensitivity issues can be effectively incorporated. And review the framework periodically as the governing conditions often change over time.

Principle 4: The Data Custodian Decides

In order to ensure that sensitive data is not inadvertently shared without safeguards, it is the responsibility of the Data Custodian to determine whether the resulting data is to be classified as sensitive under the legislative and policy framework governing their organization.

This principle is based on the fact that if the Data Custodian does not determine a dataset's sensitivity, then once it is released for dissemination it is no longer controlled. As soon as the data leaves the hands of the Data Custodian without any associated safeguards it is too late to then determine if the data is sensitive and to recall the data.

An issue with this principle is that in some cases, based on the governance framework of the Data Custodian, or the miss-application of the governance, the data may not be classified as sensitive, however a Data Consumer of the data may have to treat it as sensitive based on their governance framework. This is most likely to happen with privacy issues related to the data. In these cases the recipient should inform the data source's Data Custodian of the situation.[36]

Principle 5: Define the Conditions Under Which Sensitive Data Can Be Shared

Define conditions under which sensitive data can be shared and/or define means to remove the sensitive element from information in order to support open access and apply consistently.

There are situations where an organization can not share its sensitive data under any circumstances, there are situations where the detailed sensitive data can be shared with a restricted Data Consumer group and there are situations where the sensitivity can be removed from the data while retaining the value of the information and allowing for open access. As with the assessment process, the conditions under which sensitive data would be shared must be justified and supported by a process that is consistent and repeatable.

Principle 6: Retain the Original Data

The Data Custodian must always retain an unaltered, original version of the dataset.

While it seems obvious it is imperative that any technique applied to the dataset to create an output product that has the sensitivity removed, is performed on a copy of the source dataset.

36 Guide Development Consultation Workshop, GeoConnections, 2009

Principle 7: Document and Publish

Document and publish the process, criteria, metadata and resulting decisions.

The significance of documentation can not be over stressed. The information has to be not only documented but available to Data Contributors, Stewards, Custodians and Consumers. It is particularly important for Data Contributors and Consumers to understand what data exists, why it is considered sensitive, how it is safeguarded, who to contact for access and what changes have been made to the data in any resulting output product.

Principle 8: Respecting the Restrictions Attached to a Dataset is Essential

Data Consumers of sensitive environmental geospatial datasets must honour the restrictions accompanying the information in the form of an agreement, license and/or metadata.

It is incumbent upon the Data Consumer to respect the defined restrictions placed on the data. The sharing of sensitive data is only permissible in an environment of trust. If the trust is abused then the Data Custodian must take steps to cease dissemination to either the offending party or potentially to all requestors.

3.2 Assessing Sensitive Environmental Geospatial Data

As indicated in Section 2.3.2, there are several frameworks for assessing the sensitivity of an organization's data. If your organization's sensitive geospatial data issues relate specifically to biodiversity, species at risk, First Nation data and / or privacy, one of the above approaches may be most appropriate. However, where requirements may be more generic, the following framework is presented as an example for assessing the sensitivity of an environmental geospatial dataset . It has been adopted from the US Federal Geographic Data Committee document Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns[37]. As the FGDC guidelines are primarily concerned with Security and Public Safety, the framework has been modified for the purposes of these Best Practices to accommodate environmental geospatial data.

Whether applying the guidelines below or utilizing your organization's own procedures it is essential that steps be taken early in the data collection and management processes to ensure that any resulting requirements for safeguarding the data are put in place from the outset and that sensitive environmental data is not inadvertently or inappropriately disseminated. In situations where there are multiple organizations involved in the creation of the data the FGDC guidelines state that it may be prudent to implement safeguards while the data are being developed in an organization's offices, in the field, or in a contractor's facilities before the originating organization formally takes possession of the data.

[37] Guidelines for Providing Appropriate Access to Geospatial Data in response t Security Concerns, Federal Geographic Data Committee, U.S. Geological Survey, June 2005
http://www.fgdc.gov/policyandplanning/Access Guidelines.pdf

Before starting the process there are a few elements that need to be considered and addressed in order to provide guidelines to the process. These elements include:

- Legislative considerations;
- Level at which data is being assessed;
- Geographic homogeneity of data being assessed; and
- Frequency of review.

There are two aspects of legislative consideration to be addressed. The first is the need for the Data Custodian to be familiar with the relevant legislation pertaining to their organization in order to adequately determine and consistently understand the potential sensitivity of a dataset. The other aspect is for a Data Consumer to determine their obligations in a situation where they receive data that by their Data Custodian's assessment is considered sensitive, but the source Data Custodian did not treat it as such. In this situation the originating Data Custodian may not be aware of the legislative requirements or in their jurisdiction the content is not considered sensitive.

As all data is not created equally, even within a dataset, the Data Custodian must determine at the outset whether the dataset is to be assessed as a whole or on a record by record basis. There are situations where some records in a dataset would contain sensitive data and others would not. What is your organization's policy in these situations?

The third element relates to the recognition of the geographic homogeneity of a dataset being assessed. For instance a species that may be classified as rare in one geographic region may be considered common in another. What is your organization's policy in these situations?

There is a need for a periodic review by your organization of the assessment process as a whole to ensure it still meets the objectives and requirements of current legislation and policies. For instance while the definition of Rare may be constant within the Rare Species Act, the list of rare species on the list changes. The Data Custodian must be cognisant of these changes and more importantly the frequency at which they might change.

With these elements well understood by the Data Custodian, they are ready to begin.

Sensitive Environmental Geospatial Decision Framework

The decision framework is provided in the form of a decision tree (see Figure 3.1). Note that the procedure has been followed correctly only when you reach one of the following: Step 2, Step 6, Step 11, or Step 12.

As you follow the decision procedure, organize and document your decisions. The documentation should include the identification of the geospatial data, the potential sensitivity concerns, findings determined by use of the guidelines, the actions taken, and (if needed) the authority or case law that supports the actions taken. This information should be available to organizations that receive the data.

Note that legislation or organizational policy may take precedence over any one of the steps so it is essential that the Assessor be aware of relevant legislation and policies (see Appendix B for a list of some relevant legislation).

The high level decisions are:

- Is your organization responsible for assessing sensitivity of a dataset;
- If yes, is the data "sensitive" environmental geospatial data; and
- If yes, what safeguards are authorized and justified.

Section I: Is your Organization responsible for assessing the sensitivity of the data?

Step 1 – Did your organization originate these data?

If the answer to the question is no go to Step 2. If the answer is yes go to Step 3.

Step 2 – Follow instructions of the originating organization.

When you reach this step your use of the decision procedure is complete.

As a recipient of data your organization must honour any instructions that accompany or are associated with the data. If there are no instructions or instruments associated with the use of the data, you may presume that no restrictions apply to the data.

Instructions, terms, and conditions may be found in the accompanying metadata and/or in licenses, signed agreements (including non-disclosure agreements), or other instruments that accompany the data or permit you access to the data. Your organization is responsible for knowing and honouring any restrictions that accompany the data.

Section II: Is this data "sensitive" environmental geospatial data?

This section provides guidelines to decide if the geospatial data need meets the "Sensitive" environmental geospatial data criteria.

Step 3 – Does the data meet any of the five "sensitive environmental" geospatial data criteria?

The criteria are:

1. Legislation/Policies/Permits;
2. Confidentiality;
3. Natural Resource Protection;
4. Cultural Protection; or
5. Safety and Security.

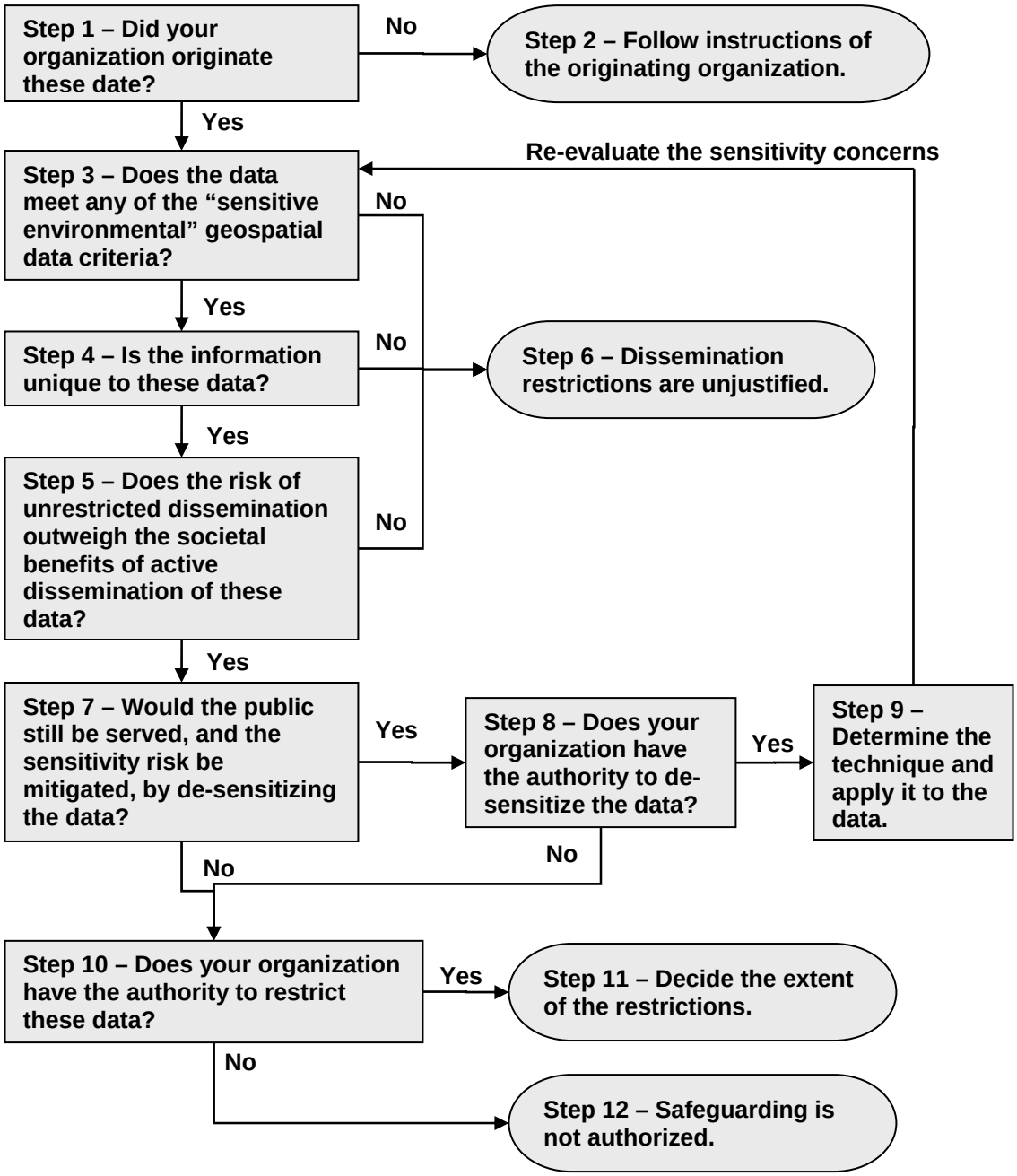

Figure 3-1: Sensitivity Assessment Procedure

For a definition of the criteria and examples refer back to Section 2.3 and for examples of potentially sensitive data refer to Section 2.4.

If the answer is no, then safeguarding is not justified and you should go to Step 6. If the answer is yes to any one of the criteria, go to Step 4.

Step 4 – Is the information unique to these data?

Is the information that appears to be sensitive based on the evaluation in Step 3:

- Difficult to observe?
- Not found in other open-source geospatial data (for example, is the feature not found elsewhere in other digital or hard copy maps)?
- Not found in other open-source publications (for example, telephone books and Internet directories) libraries, archives, or other information repositories?

If the sensitive information is readily observable or available from open sources safeguarding is not justified and you go to Step 6. If the geospatial data under evaluation provides unique information that cannot be obtained from observation or open sources, you go to Step 5.

It is in this step that the Assessor's knowledge of current legislation and policies may also come into play. In some situations the data may be readily available in open-source publications but legislation still considers the data sensitive. For instance while an organization's dataset may contain names and addresses that are available from a phone book, it is still considered private information by the federal Privacy Act and must be treated as such.

Step 5 – Does the risk of unrestricted dissemination outweigh the societal benefits of active dissemination of these data?

In particular could the release of the sensitive information cause risks such as:

- The identification of an individual;
- Negative financial impact on an enterprise;
- Destruction of rare of endangered habitat;
- Destruction of cultural heritage;

If so, do the anticipated risks outweigh the anticipated societal benefits of active data dissemination such as:

- Business or personal productivity resulting from continued or increasing use of the geospatial data?
- Continued or increasing effectiveness of land management, sustainable development or the regulatory functions of government?
- Continued or increasing support of legal rights (for example, "right to know") and public involvement in decision-making?
- Continued or increasing support to those who depend on public information in absence of an alternate data source of equal quality at the same cost?

After such consideration go to Step 6 if you believe that the benefit of providing open access to the data outweighs the potential sensitivity costs, or to Step 7 if the sensitivity costs outweigh the value of providing open access.

Step 6 – Safeguarding is not justified.

When you reach this step your use of the guidelines is complete. Retain your documentation of the decision for future use. Provide information about the evaluation in the metadata and/or in licenses, signed agreements (including non-disclosure agreements), or other instruments that accompany the data or permit you access to the data.

Section III: What safeguards are authorized and justified?

If you reach this section, you have concluded that your geospatial data has sensitive information content that, in its present form, should be safeguarded.

This section provides guidance on appropriate choices for safeguarding data. It encourages maximum possible access to data, and so emphasizes use of the minimum safeguards required to prevent unauthorized access. It also challenges the originating organization to be sure that it has the authority to undertake the planned safeguards.

Step 7 – Would the public still be served, and the sensitivity risk be mitigated, by de-sensitizing these data?

If you believe that the sensitive information in the geospatial data can be presented in an alternate manner to minimize the sensitivity of the original data, and that the resulting altered product will still have value, go to Step 8. If the data cannot be presented in an alternate product to make the sensitivity risk acceptable, go to Step 10.

This decision starts with your organization determining whether it has the authority to create a new product from the source data. The idea of altering the presentation of the source geospatial data in a new product includes removal of sensitive information (e.g. attributes) and/or reducing the sensitivity of information by simplification, classification, aggregation, statistical summarization, or other information reduction methods.

Step 8 – Does your organization have the authority to de-sensitize these data?

If the authority to change data exists go to Step 9. If such authority does not exist that course of action is closed and you go to Step 10.

Step 9 – Determine the technique and apply it to these data.

Apply changes that create a new data product to remove or mitigate the sensitivity posed by the information. Such changes should be documented in the metadata.

When the changes are complete, ensure that the changes actually have mitigated the risk by reviewing the new data product using the criteria in Section II beginning with Step 3. The changed data are cleared for dissemination when Step 6 is reached.

An originating organization that generate new data products to remove sensitivity should have written procedures describing the types of changes allowed (refer to Section 4.2) and the conditions under which they are permitted. The originating organization should document, or at least characterize, the changes in the metadata and/or in any licenses, agreements (including nondisclosure agreements), or other instruments that accompany the data.

Such documentation should cite the authority or other basis that permits changing of the data.

It is essential to recognize that the source data is not altered in anyway and is safeguarded by the originating organization. It is the altered product that is re-assessed for sensitivity.

Step 10 – Does your organization have the authority to restrict these data?

If the authority to restrict the data does not exist, you may elect to appeal to an executive manager and/or legal counsel authorized to grant the required permission or if the authorized executive manager and/or legal counsel grants permission to restrict the data go to Step 11. If your organization does not have the authority to restrict data go to Step 12.

Step 11 – Decide the extent of restrictions.

The originating organization decides the conditions under which the geospatial data can be accessed, used, and/or redistributed, if any.

When you complete this step, your use of the guidelines is complete. Retain documentation of your decision for future use. Restrictions should be documented in the metadata. Provide information about the evaluation using metadata and/or licenses, signed agreements (including non-disclosure agreements), or other instruments that accompany the data to organizations that receive the data or permit you access to the data.

Step 12 – Safeguarding is not authorized.

When you reach this step your use of the guidelines is complete. Retain documentation of your decision for future use. Provide information about the evaluation using metadata and/or licenses, signed agreements (including non-disclosure agreements), or other instruments that accompany the data to organizations that receive the data or permit you access to the data.

3.3 Impact Assessment Outcomes

Once the assessment is completed the Assessor has reached the determination that:

- The organization did not generate the data and must abide by any restrictions placed on the data by the originator of the content; or
- There is no justification to safeguard the data and it may be distributed as non-sensitive data under the policies of the organization; or
- There is justification to safeguard the data, however, the data can be de-sensitized thereby allowing it to be distributed as non-sensitive data under the policies of the organization (refer to Section 4.2 for examples); or

- There is justification to safeguard the data, however, it may be distributed to a restricted group under defined restrictions (refer to Section 4.1 for examples of instruments that can be used to apply the restrictions); or

- There is justification to safeguard the data and it may not be distributed outside of a defined group within the organization.

Any restriction placed on the data as a result of arriving at Step 9 or 11 must be commensurate with the risk of dissemination.

Once the sensitive data is defined and the regulatory environment understood, then it can be determined how to best share the data. The following section discusses mechanisms and resources for sharing sensitive data.

4 Mechanisms for Sharing Sensitive Data

This section speaks to an Organization's obligation to protect sensitive data within their hands and identifies various mechanisms that can be used to support the distribution of sensitive environmental geospatial information to qualified users once the sensitivity of the data is understood and the risk in dissemination is fully assessed.

Options and solutions to sharing sensitive geospatial information are available through the use of technology, geographic processing or presentation techniques (generalization, aggregation, buffering, scale ranges etc), institutional policies or processes, or licensing practices. Those sharing or accessing geospatial data may use a combination of mechanisms to ensure data is shared and used responsibly. In considering sensitive information, protecting and clarifying rights to information is a principle concern. The scope of this may include consideration of confidentiality agreements, appropriate licensing, ways and means of protecting sensitive information, protection of intellectual property, considerations of downstream and upstream uses, and digital rights management.

The mechanisms available to the Data Custodian and Data Steward include:

- Instruments such as Agreements and Licences;
- De-sensitizing the geospatial data by creating a new data product that has the sensitive aspects removed or altered;
- Assessing the requestor's need-to-know and capacity to safeguard the data;
- Metadata defining safeguards to be applied to the data; and
- Training of data owners and users to ensure data is appropriately handled and a trusted relationship is ensured.

In practice a combination of these mechanisms are generally used to ensure the overall safeguarding of the shared sensitive data is maintained.

The physical means of safeguarding the data and supporting the dissemination of the data through the use of passwords, data encryption, etc. is beyond the scope of these Best Practices. For more information on this aspect of safeguarding data refer to your organization's Information Technology standards. However, the following potential resources may provide guidance:

- A Developers' Guide to the CGDI: Developing and publishing geographic information, data and associated services, GeoConnections 2007, http://www.geoconnections.net/publications/Technical_Manual/2007/CGDI_devguide_2007.pdf. Chapter 11 of this publication discusses aspects of providing access to Services and Data products through the CGDI. This includes Web Security options within the CGDI, such as Communication Security (Authentication, Authorization, Integrity) and GeoSpatial Data Rights Management (GeoDRM);

- Geospatial eXtensible Access Control Markup Language (GeoXACML), Open Geospatial Consortium, Standards, (http://www.opengeospatial.org/standards/geoxacml);

- Securing Publicly Available Information (Office of Critical Infrastructure Protection and Emergency Preparedness) http://www.publicsafety.gc.ca/prg/em/ccirc/2002/in02-005-eng.aspx; and

- Geospatial Digital Rights Management Reference Model (GeoDRM RM), Open Geospatial Consortium http://www.opengeospatial.org/standards/as/geodrmrm

4.1 Overview of Instruments Types

Instruments include agreements and licenses that are formalized between a Data Custodian and a Data Consumer of geospatial data and sets out the terms and conditions for safeguarding of the data. The following information has been drawn from the GeoConnections Dissemination of Geographic Data Best Practices Guide[38] which describes the instruments in detail and has templates for the different instruments in its appendices. The objective of this section is to give the reader an indication of what the instruments are, the situation under which they would be used and the protection they are intended to provide.

4.1.1 Agreements

Federal government departments and agencies routinely enter into arrangements between themselves governing collaboration on matters of mutual concern or interest. Such arrangements are described in informal agreements, known as "gentlemen's agreements", "handshake agreements", and memoranda of understanding ("MOUs") or memoranda of agreement ("MOAs"). The terms MOUs and MOAs are used interchangeably in the Government of Canada context. For the sake of simplicity, the latter term (MOA) is used in these Best Practices.

"MOA" is the general term used to refer to an agreement that is not intended to have any legal effect. It is the preferred vehicle to evidence arrangements between federal departments and agencies to exchange information, cooperate or coordinate programs to optimize the benefits from each department's efforts.

A MOA, as opposed to a legally binding agreement (such as a licence) only describes general cooperation procedures. As such, MOAs should be used to evidence data sharing arrangements between federal departments and agencies. Basic elements of MOAs pertaining to the sharing of government geographic data include the following:

> **Responsibilities** - identifies the roles and responsibilities of the federal departments or agencies. It should clearly set out the actions the parties have agreed to take.

[38] The Dissemination of Government Geographic Data in Canada: Guide to Best Practices, GeoConnections, version 2, 2008 http://www.geoconnections.org/publications/Best_practices_guide/Guide_to_Best_Practices_Summer_2008_Final_EN.pdf

Intellectual Property Rights - confirms the custodial responsibilities of the federal departments or agencies in the data they exchange under the aegis of the MOA, and provides for the allocation of intellectual property rights and the custodial responsibilities in products developed by one of the participating departments or agencies as a result of its use, analysis or interpretation of the other's data.

Permitted Uses - lists what a department or agency is authorized to do with the other's data.

Restrictions On Use - lists any restrictions on uses that may be made of the data exchanged pursuant to the MOA (for example, restrictions on further distribution).

4.1.2 Licences

Licences are used by Federal departments/agencies when entering into data use arrangements with other levels of government or non-governmental organizations. Such arrangements should be evidenced by a legally binding licence agreement.

The key characteristics of the licence agreements that have been developed in support of the four (4) distribution models which are:

- **Unrestricted Use** - promotes wide use and re-use of the licensed geographic data, with few restrictions on how the data may be used and allows for further distribution;
- **End-Use** - provides for a more restricted grant of rights, with no rights to redistribute. The end-use model is appropriate in instances where the producer of the geographic data wishes to grant access to its data while retaining control over the number of users and the manner in which it is used and where there are confidentiality and security concerns;
- **Reseller** - appropriate where the stated dissemination objective of the producer of the geographic data is to enhance dissemination opportunities and to promote wide use of its data through established distribution channels. the reseller does not, as a matter of practice, deploy significant intellectual effort in transforming the geographic data; and
- **Value-Added Reseller** - allows the value-added reseller to develop and distribute products and services that incorporate the licensed geographic data, thus enhancing its market penetration, user uptake and revenue generation potential.

Only the End-Use Restricted Licence Agreement (No-Fee and the Fee-Based) are applicable to the distribution of the sensitive environmental geospatial datasets as all other licenses allow un-restricted use and dissemination.

The following table highlights the features of the various License Models available at the federal level.

	Primary Dissemination Objectives	Restrictions on Use of the Data	Downstream Data Distribution	Value-Added/ Derived Products Development	Positive Aspects - - - - - Negative Aspects
No-Fee Unrestricted Use Web-Wrap Licence Agreement	Promote the widest public use and private benefit of the data, at no cost to the Licensee Promote wide recognition of government as source of the data Solicit interest in other gvt datasets	No restrictions	Permitted Licensees' licences with 3rd parties must contain same terms as those contained in Canada's licence agreement with Licensee	Permitted Right to create and market Value-Added Products (products developed by Licensee by deriving, developing, adapting, incorporating, etc. or simply using the data)	**POSITIVE** Ease of administration Strong public support Good public relations - - - - - **NEGATIVE** Reduced control over the use of the data Reduced control over the number and/or type of users
Fee-Based Unrestricted Use Licence Agreement	Promote the widest public use and private benefit of the data, on a fee Basis Promote wide recognition of government as source of the data Solicit interest in other gvt datasets	No restrictions	Permitted Licensee's licences with 3rd parties must contain same terms as those contained in Canada's licence agreement with Licensee.	Permitted Right to create and market Value-Added Products (products developed by Licensee by deriving, developing, adapting, incorporating, etc. or simply using the data)	**POSITIVE** Ease of administration Strong public support Good public relations Predictable impact on cost recovery - - - - - **NEGATIVE** Reduced control over the use of the data Reduced control over the number and/or type of users
No-Fee End-Use Restricted Licence Agreement	Promote use of data, at no cost to the Licensee, while retaining control on the number and/or type of users Promote wide recognition of gvt as source of the data	No redistribution of the data Rights to the data restricted to Licensee's own internal use	Prohibited	Permitted Right to create Derived Products (products developed by Licensee that interpret the data, <u>but do not incorporate it</u>)	**POSITIVE** Effective control of number/type of users ---------- **NEGATIVE** Potential inhibitor of wider use of data
Fee-Based End-Use Restricted Licence Agreement	Promote use of data while retaining control on the number and/or type of users, on a fee basis Promote wide recognition of gvt as source of the data	No redistribution of the data Rights to the data restricted to Licensee's own internal use	Prohibited	Permitted Right to create Derived Products (products developed by Licensee that interpret the data, <u>but do not incorporate it</u>)	**POSITIVE** Effective control of number/type of users Predictable impact on cost recovery - - - - - **NEGATIVE** Admin. Overhead Potential inhibitor of wider use of data
Reseller Agreement	Promote wider use of data through access to established distribution channels Promote wide	No modification or alteration to the data allowed, except to perform minimal utility reformatting, for convenience of client delivery	Permitted, on an end use basis only. Reseller's licences with 3rd parties must be on an end-use basis and contain prescribed	Prohibited	**POSITIVE** Access to reseller's distribution channels Greater potential for cost recovery Predictable impact on cost recovery

	Primary Dissemination Objectives	Restrictions on Use of the Data	Downstream Data Distribution	Value-Added/ Derived Products Development	Positive Aspects - - - - - Negative Aspects
	recognition of government as source of the data	only	terms set out in Canada's agreement with Reseller		- - - - **NEGATIVE** Admin. Overhead Reduced control over use of data Reduced control over the number and/or type of users
Value-Added Reseller Agreement	Promote wider use of data through value added products Promote wide recognition of government as source of the data Promote innovation	No restrictions	Permitted, on an endues basis only Reseller's licences with 3rd parties must be on an end-use basis and contain prescribed terms set out in Canada's agreement with Reseller.	Permitted Includes the right to create VAR Products (products developed by the VAR reseller by deriving, developing, adapting, incorporating, etc. or simply using the data)	**POSITIVE** Greater potential for cost recovery Predictable impact on cost recovery Promotes innovation - - - - **NEGATIVE** Admin. Overhead Reduced control over use of data Reduced control over the number and/or type of users

4.1.3 Data Access Requests

As pointed out, once the data has been released by the source organization the ability to safeguard the data is now dependent upon the policies, procedures and security mechanisms of the recipient organization. All the agreements and security mechanisms put in place do not replace the basic need for the Data Custodian to trust that the Data Consumer will respect the sensitivity of the data and treat it accordingly. To develop this trust and manage risk, determining whether to release sensitive data to an organization often requires the Data Consumer to complete a formal data request process. The Data Custodian generally wants to determine whether the Data Consumer has a need-to-know right to the details of the sensitive data, that the data will be used appropriately and that it will be safeguarded. The request process asks questions regarding the Data Consumer's organization, the program/project the data is being used for, how the data is to be used, who will have access to it, what security mechanisms will be applied to the data and what are the policies and training requirements of the requesting organization.

For this reason many organizations require the Data Consumer to submit a formal application for access to the data. The types of questions may include elements of the following:

- Name, address, organization, department, contact information of the applicant;
- Professional status (Biologist, Forester, Archaeologist, Engineer, etc.) and member number of the applicant;
- Description of program/project utilizing the data;
- Specifics of the data requested (dataset, data attributes, areal extent);

- How is the information to be used;
- Who will have access to the data;
- Who is ultimately responsible for the safeguarding of the data in compliance with any agreements and metadata related to the data;
- For the organization accountable for the request, what safeguarding policies, training and mechanisms are in place; and
- Has the organization requested data in the past.

This approach is commonly adopted by those managing archaeological and rare species data, as well as in areas such as non-sensitive environmental research data and public health data.

As with all other processes associated with these Best Practices, the Data Custodian must **define and document the criteria by which data requests are assessed and make available the results of the assessment for all requests**. This is particularly important when a request is rejected and the Data Consumer requires an explanation.

4.2 Methods of Removing the Sensitivity of the Data

An alternative to denying access to safeguarded data is to remove the sensitivity in the data and still retain the overall knowledge of the source data in the end product.

There are three main ways of removing the sensitivity in environmental geospatial data:

- Generalize the spatial locality or georeference;
- Aggregate or statistically summarize data; and
- Modify or remove attribution.

The following are only a few examples of means of removing sensitivity from geospatial data. **Each organization has to determine the technique(s) that best satisfy their requirements to remove sensitivity and still impart valuable information for decision making processes. Which ever technique is chosen should be documented, applied consistently and recorded in the dataset's metadata.**

Any effort to remove the sensitivity of the data must be performed on a copy of the source data and not the original dataset. The original dataset should be retained and safeguarded.

In generalizing the spatial locality or georeference of a feature, the objective is to retain the fact that there is a point but to represent it in such a way that the user can not precisely locate it physically on the ground. Techniques range from:

- Randomising points within administrative polygons – this gives a vague impression of the distribution of points but the users have to recognize that the points are not precisely located but occur somewhere within the specified jurisdictional unit;
- Altering the precision of a georeferenced point - depending on the precision level chosen the user would know that the true point is within a certain radius of the

specified location. For example, based on the GBIF levels of sensitivity they stipulate:

1. Extreme Sensitivity – georeference not released or data may be related by watershed/bioregion/county, etc with no georeference coordinates;
2. High Sensitivity – Georeference rounded to 0.1 degree;
3. Medium Sensitivity - Georeference rounded to 0.01 degree;
4. Low Sensitivity - Georeference rounded to 0.001 degree;
5. Not Sensitive – Georeference unrestricted[39]; or

- Representing the point as a symbol - this uses a symbol that is large enough to obscure the accurate location of the point in which the symbol is not centred on the point but the point lies within the confines of the symbol. In this case the user knows the point lies somewhere under the symbol.

Aggregating or statistically summarizing data within an area is intended to bring multiple features together within a larger framework in order to obscure the details. Common approaches include amalgamating data higher up the chain of a hierarchy than the level at which the data was collected. For instance reporting at a Census Sub Division level rather than at a Postal Code level or at a primary watershed level rather than a tertiary watershed level. How many levels up the hierarchy the data must be amalgamated may be dictated by the sensitivity of the data.

Another approach is to report point data at a polygon level. In this case the data may be amalgamated such that the user does not even know how many points were involved in producing the content.

In the Canadian archaeological field the Borden number system is used. This is a gridded reference that identifies an area and the number of the archaeological site within the grid cell. This is the extent to which the georeferenced location of the site is made available to other researches or the public while the exact coordinates are retained in the source database.

In some cases the sensitivity does not lie in the location of the feature but in some component of the attribution of the feature. In these cases the removal or modification of the sensitive attribute may be sufficient to alter the sensitive classification of the feature. For instance, identifying a plant or animal at the order level rather than species or sub-species level could remove the sensitivity from the record.

While there are few articles or books devoted to techniques for removing sensitivity from geospatial data the concepts can be derived from reviewing various geospatial analysis techniques. Some references that might provide useful insights include:

- Geospatial Analysis A Comprehensive Guide to Principles, Techniques and Software Tools, de Smith, M., Goodchild, M. and Longley, P., Troubadour Publishing, 2007;

[39] Guide to Best Practices for Generalizing Sensitive Species Occurrence Data, Chapman, A. and Grafton, O., GBIS, 2008

- GIS, Spatial Analysis and Modeling, Maguire, M., Batty, M. and Goodchild, M., ESRI GIS Bookstore, 2005; or
- How to Lie with Maps, Monmonier, M. and Blij, H., 1996.

4.3 Metadata

Metadata is commonly known as "data about data and services"[40]. It is the data describing the context, content and structure of records and their management through time. It describes the data including details about data ownership, quality, time of collection or update, attribute information and how it can be accessed and obtained. Metadata is essential to understanding the data product, its purpose and/or limitations.

Metadata is the vital foundation for data management and for understanding, collaborating and sharing resources with others. According to the FGDC four types of information should be encoded in the metadata related to the safeguarding of the sensitive geospatial data[41]:

1. the fact that the geospatial data and metadata were reviewed using the organization's specified process;
2. decisions that were made;
3. the date of the decisions; and
4. the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.

One practice that has been used by some organizations in Canada to control access but support discovery, transparency and potential sharing of sensitive geospatial data is to provide metadata about such data through Cataloguing services and tools; but not necessarily to provide direct access to the data through open web services (for example: WMS, KML, FTP, HTTP). This allows for the discovery and knowledge of the data by potential Data Consumers, but then also requires those potential Data Consumers to engage in a process to request the data. This provides an organization acting as the Data Custodian the opportunity to assess potential end uses and users of the data; and assess against data sharing constraints and sensitivities.

4.4 Training

There are two aspects to training people in their role in the safeguarding of sensitive environmental geospatial information. Training for those producing or originating the data (Data Stewards, Contributors and Custodians). And training for those that use the data (Data Consumers). Training also serves the twin objectives of managing risk and building trust.

[40] Guide to the Canadian Geospatial Data Infrastructure, GeoConnections Technical Manual - Using Metadata to Describe You Resources
http://www.geoconnections.org/publications/Technical_Manual/html_e/appendix_2-3.html
[41] Guidelines for Providing Appropriate Access to Geospatial Data in response t Security Concerns, Federal Geographic Data Committee, U.S. Geological Survey, June 2005

Data Stewards, Contributors and Custodians are required to be trained in the method of assessing sensitivity as the process begins with them. In order to appropriately define whether the data is sensitive and how it can be treated they need to be trained in:

- the legislation, regulations, policies and agreements governing their organization;
- what constitutes sensitive data within their organization;
- the method by which data is assessed for sensitivity;
- under what conditions can sensitive data be shared by the organization; and
- the methods by which the data may be changed in order to assess whether proposed approach is viable in removing sensitivity from the data.

Appropriate training and adherence to processes will reduce the risk of sensitive data inadvertently being shared and build the credibility of the organization for the effective safeguarding of sensitive data.

Training is equally important for the Data Consumer that utilizes the content. They require training in:

- how to manage and safeguard the content that is imported into their organization;
- how to represent it in any resulting derived products; and
- To track and ensure that any restrictions and limitations that are attached to the acquired data are flowed through to any products.

This is critical as any misuse of the data can destroy the trust between organizations and likely result in more stringent restrictions being imposed on the data going forward. It also ensures the credibility of the organization against charges of miss-management of sensitive data.

4.5 Community of Practice and Networking

A final mechanism that can be used to assist an organization in determining how best to meet its obligations with regard to collecting, managing and disseminating environmentally sensitive geospatial information is to participate in a related community of practice or network. While no specific community of practice has been identified at this time, those with an interest in this subject matter should reach out to others. Those that participated in the development of these Best Practices through a workshop agreed to have their names published with the expressed interest in developing a network in this subject area (see Appendix D).

5 Conclusion

This document has identified basic principles and best practices that an organization can apply to consistently assess and document the sensitive nature of their environmental geospatial datasets and the resulting mechanisms that are appropriate for sharing their specified sensitive datasets.

At its core, the successful long term sharing of sensitive environmental geospatial information is about trust, risk management, the credibility of the participating organizations and their overriding desire to disseminate information.

As indicated in Section 2.2 there are a myriad of factors that influence an organization's definition of what constitutes sensitive environmental geospatial data. As a result there is no off the shelf framework that will allow a Data Custodian (defined role responsible for assessing sensitive data) to conduct an assessment of a dataset. Each organization has to define its own specific framework.

It is intended that these Best Practices have provided the reader with sufficient insight and links to resources to assist in defining and implementing a consistent and documented approach to managing and sharing their organization's sensitive environmental geospatial data. In undertaking such an effort it is important that the team utilize the links and references in this document to understand the context of their potentially sensitive data and to reach out to other stakeholders interested in this subject.

Finally, this document is also intended as a living document, and may be updated as related practices mature and the user-community needs evolve. Therefore any contributions, links or relevant legislation/regulations/guidelines, etc. that the reader feels would benefit this document are greatly appreciated (e-mail: info@geoconnections.org).

Appendix A – Terms & Acronyms

Term	Definition
Data Contributor	Is the role that is responsible for collecting and submitting portions of, or individual records of a dataset. They abide by the standards and processes set out by the Data Steward and contribute their data through the Data Steward.
Data Consumer	Is the role that requests access to the data on a one time or ongoing basis. They are obligated to abide by any agreements, licenses or restrictions attached to the data.
Data Custodian	Is the role responsible for safeguarding corporate data. This function includes managing geospatial data to ensure it is accessible by the user community, appropriate security and dissemination restrictions are in place, meets data structure and quality standards, is properly managed with regard to accepting new datasets or revisions of existing content, protection, back-up, recovery and archiving.
Data Steward	Is the role that is considered the owner of a geospatial dataset/product and is responsible for creating and/or maintaining (up-dating, editing) the dataset/product. This function includes defining what needs to be collected, the level of detail required of the data, and manages the data collection and maintenance processes.
Framework data	Framework data is the set of continuous and fully integrated geospatial data that provide context and reference information for Canada. Framework data are expected to be widely used and generally applicable, either underpinning or enabling geospatial applications.
Geomatics	The science and technology of gathering, analyzing, interpreting, distributing and using geospatial data. Geomatics encompasses a broad range of disciplines including surveying, global positioning systems, mapping, remote sensing and cartography.
Georeference	The assignment of coordinates of an absolute geographic reference system to a geographic feature. In remote sensing it is a process of taking an image and assigning it geographic coordinates.
Geospatial	Referring to location relative to the Earth's surface. "Geospatial" is more precise in many GIS contexts than "geographic," because geospatial information is often used in ways that do not involve a graphic representation, or map, of the information.
Geospatial Data	Data or Information that are geospatial provides the location and representation of phenomena in relation to the surface of the Earth. For example, data with explicit geographic positioning information included, such as a road network from a GIS, or a georeferenced satellite image. Geospatial data may include

Term	Definition
	attribute data that describes the features found in the dataset.
Metadata	Information about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data are formatted. Metadata is essential for understanding information stored in data warehouses.
Orthophotography	An **orthophoto** or **orthophotograph** is an aerial photograph geometrically corrected ("orthorectified") such that the scale is uniform: the photo has the same lack of distortion as a map. Unlike an uncorrected aerial photograph, an orthophotograph can be used to measure true distances, because it is an accurate representation of the earth's surface, having been adjusted for topographic relief, lens distortion, and camera tilt.
Sensitive	For this Guide sensitive refers to all geospatial data that may be considered restricted for purposes of dissemination and therefore requires some form of safeguarding.
Taxon	Taxon, (pl. taxa), n. A taxonomic unit, whether named or not: i.e. a population, or group of populations of organisms which are usually inferred to be phylogenetically related and which have characters in common which differentiate (q.v.) the unit (e.g. a geographic population, a genus, a family, an order) from other such units. A taxon encompasses all included taxa of lower rank (q.v.) and individual organisms.

Acronym	Definition
ANZLIC	Australia New Zealand Land Information Council
CGDI	Canadian Geospatial Data Infrastructure
E&SD	Environmental and Sustainable Development
FGDC	Federal Geographic Data Committee
GBIF	Global Biodiversity Information Facility
GeoXAMCL	Geospatial eXtensible Access Control Markup Language
GIS	Geographic Information System
GML	Geographic Markup Language
GPS	Global Positioning System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NGO	Non-Governmental Organization
NRCan	Natural Resources Canada
OGC	Open Geospatial Consortium

Acronym	Definition
OMNR	Ontario Ministry of Natural Resources
RHS	First Nations Regional and Inuit Longitudinal Health Survey
TEK	Traditional Ecological Knowledge
WFS	Web Feature Service
WMS	Web Map Service
XML	Extensible Markup Language

Appendix B – Summary of Relevant Legislation, Regulations and Policies

The following table provides a list of several Canadian acts, regulations and policies. This list is by no means exhaustive and should be added to as new documents become available and in fact any contributions to GeoConnections would be greatly appreciated. Each document has an associated link (if available) and a brief description to give a high level view of what the document entails.

The table is divided into:

Legislation – Federal, Provincial/Territorial

Regulations - Federal, Provincial/Territorial

Policies - Federal, Provincial/Territorial

Guidelines/Frameworks - Federal, Provincial/Territorial

Title – Web Link		Objective
> Legislation - Federal		
Access to Information Act – http://laws.justice.gc.ca/en/showtdm/cs/A-1	Federal	The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government.
Canadian Environmental Assessment Act – http://laws.justice.gc.ca/en/C-15.2/	Federal	The purpose of the Act is to: • ensure that projects are considered in a careful and precautionary manner before federal authorities take action in connection with them, in order to ensure that such projects do not cause significant adverse environmental effects; • encourage responsible authorities to take actions that promote sustainable development and thereby achieve or maintain a healthy environment and a healthy economy; • ensure that responsible authorities carry out their responsibilities in a coordinated manner with a view to eliminating unnecessary duplication in the environmental assessment process; • promote cooperation and coordinated action between federal and provincial governments with respect to environmental assessment processes for projects; • promote communication and cooperation between responsible authorities and Aboriginal peoples with respect to environmental assessment; • ensure that projects that are to be carried out in Canada or on federal lands do not cause significant adverse environmental effects outside the jurisdictions in which the projects are carried out; and • ensure that there be opportunities for timely and meaningful public participation throughout the environmental assessment process.

Title – Web Link		Objective
Copyright Act - http://laws.justice.gc.ca/en/C-42/	Federal	Stipulates that copyright to any work (term which encompasses original geographic datasets) prepared: • by employees of the government in the course of their employment; or • under the direction or control of the government belongs to the government, subject to an agreement with the author to the contrary. The government, as owner of the copyright in the work, has the exclusive right to use the work in any manner
Emergency Management Act http://www.publicsafety.gc.ca/media/nr/2007/bk20070807-eng.aspx	Federal	The Emergency Management Act (EMA) sets out clear roles and responsibilities for all federal ministers across the full spectrum of emergency management. This includes prevention/mitigation, preparedness, response and recovery, and critical infrastructure protection.
Personal Information Protection and Electronic Documents Act (PIPEDA) – http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod2/mod2-3-eng.asp	Federal	*PIPEDA* is based on balancing an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes. The Act also established the Privacy Commissioner of Canada as the ombudsman for privacy complaints.
Privacy Act – http://laws.justice.gc.ca/en/showtdm/cs/P-21	Federal	This Act regulates how federal government institutions collect, use and disclose personal information. It also provides individuals with a right of access to information held about them by the federal government, and a right to request correction of any erroneous information. Under the Privacy Act, the Privacy Commissioner of Canada has powers to audit federal government institutions to ensure their compliance with the act, and is obliged to investigate complaints by individuals about breaches of the act. Some of the key components of the *Privacy Act* include: • A listing of various types of personal information; • How to submit a formal request; • How to change personal information if you feel it is untrue or misleading; • How personal information is safeguarded by the Government of Canada; • How the Government of Canada can disclose personal information • Turnaround times on requests. • The Act also provides key privacy definitions
Species at Risk Act – http://www.sararegistry.gc.ca/approach/act/sara_e.pdf	Federal	The Species at Risk Act (SARA) is a federal law with three main goals: • to prevent endangered or threatened species from becoming extinct or extirpated; • to help in the recovery of endangered, threatened and extirpated species; and • to manage species of special concern to help prevent them from becoming endangered or threatened. Once a species is listed under the *Species at Risk Act*, it becomes illegal to kill, harass, capture or harm it in any way. Critical habitats are also protected from destruction.

Title – Web Link		Objective
> Legislation – Provincial / Territorial		
> > Alberta		
Freedom of Information and Protection of Privacy Act (FOIP) – http://foip.alberta.ca/	Provincial	The purposes of this Act are: • to allow any person a right of access to the records in the custody or under the control of a public body subject to limited and specific exceptions as set out in this Act, • to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information and to control the disclosure by a public body of that information, • to allow individuals, subject to limited and specific exceptions as set out in this Act, a right of access to personal information about themselves that is held by a public body, • to allow individuals a right to request corrections to personal information about themselves that is held by a public body, and • to provide for independent reviews of decisions made by public bodies under this Act and the resolution of complaints under this Act.
> > British Columbia		
Freedom of Information and Protection of Privacy Act (FOIPP) – http://www.cio.gov.bc.ca/services/privacy/	Provincial	The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by: giving the public a right of access to records, • giving individuals a right of access to, and a right to request correction of, personal information about themselves, • specifying limited exceptions to the rights of access, • preventing the unauthorized collection, use or disclosure of personal information by public bodies, and • providing for an independent review of decisions made under this Act.
> > Manitoba		
Freedom of Information and Protection of Privacy Act (FIPPA) – http://gov.mb.ca/chc/fippa/index.html	Provincial	The purposes of this Act are: • to allow any person a right of access to records in the custody or under the control of public bodies, subject to the limited and specific exceptions set out in this Act; • to allow individuals a right of access to records containing personal information about themselves in the custody or under the control of public bodies, subject to the limited and specific exceptions set out in this Act; • to allow individuals a right to request corrections to records containing personal information about themselves in the custody or under the control of public bodies; • to control the manner in which public bodies may collect personal information from individuals and to protect individuals against unauthorized use or disclosure of personal information by public bodies; and • to provide for an independent review of the decisions of public bodies under this Act.
Mines and Minerals Act – http://web2.gov.mb.ca/laws/statutes/ccsm/m162e.php#2	Provincial	The object and purpose of this Act is to provide for, encourage, promote and facilitate exploration, development and production of minerals and mineral product in Manitoba, consistent with the principles of sustainable development.
> > New Brunswick		
Protection of Personal Information Act http://www.gnb.ca/0062/PDF-acts/p-19-1.pdf	Provincial	A public body is responsible for personal information under its control. The chief executive officer of a public body, and his or her designates, are accountable for the public body's compliance with principles related to: • Identifying Purposes; • Consent; • Limiting Collection; • Limiting Use, Disclosure and Retention; • Accuracy; • Safeguards;

Title – Web Link		Objective
		• Openness; • Individual Access; and • Challenging Compliance.
Protected Natural Areas Act – http://www.gnb.ca/0062/acts/acts/p-19-01.htm	Provincial	The purpose of this Act is to protect the biological diversity of fauna and flora within the Province and the relationship between such fauna and flora and the environment by protecting, conserving and managing lands that • are representative of ecosystems or natural landscapes within the Province, • contain unique or unusual assemblages of fauna or flora, • contain, in its natural habitat, native fauna or flora that is rare or endangered, • contain ecologically sensitive fauna, flora or habitats, • contain unique or rare examples of botanical, zoological, pedological or geological phenomena, or • contain ecosystems that have been altered by humans and that offer opportunities for the study of the recovery of the ecosystems from such alteration, While providing opportunities for public access to those lands or portions of those lands for outdoor recreational activities, educational activities and scientific research that have minimal environmental impact.
Clean Water Act – http://www.gnb.ca/0062/PDF-acts/c-06-1.pdf	Provincial	The purpose of this Act is to protect the quality of water and covers: • Application of the Act; • Action by the Minister – orders, liability, remedial action by the Minister; • Recovery of costs; and • Restoration of land, premises and personal property.
> > Newfoundland and Labrador		
Access to Information and Protection of Privacy Act (ATIPPA) – http://www.assembly.nl.ca/legislation/sr/statutes/a01-1.htm	Provincial	The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by • giving the public a right of access to records; • giving individuals a right of access to, and a right to request correction of, personal information about themselves; • specifying limited exceptions to the right of access; • preventing the unauthorized collection, use or disclosure of personal information by public bodies; and • providing for an independent review of decisions made by public bodies under this Act.
> > Northwest Territories		
Access to Information and Protection of Privacy Act – http://www.justice.gov.nt.ca/PDF/ACTS/Access_to_Information.pdf	Provincial	The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by: • giving the public a right of access to records held by public bodies; • giving individuals a right of access to, and a right to request correction of, personal information about themselves held by public bodies; • specifying limited exceptions to the rights of access; • preventing the unauthorized collection, use or disclosure of personal information by public bodies; and • providing for an independent review of decisions made under this Act.

Title – Web Link		Objective
> > Nova Scotia		
Freedom of Information and Protection of Privacy (FOIPOP) – http://www.gov.ns.ca/legislature/legc/statutes/freedom.htm	Provincial	Pursuant to the Acts, all public bodies, municipalities and local public bodies are obliged to adopt a policy of accountability, openness and transparency and to provide a right of access to information with limited exceptions. They are also obliged to ensure the protection of individuals' personal privacy. ...the legislation in Nova Scotia is deliberately more generous to its citizens and is intended to give the public greater access to information that might otherwise be contemplated in the other provinces and territories in Canada. Nova Scotia's lawmakers clearly intended to provide for the disclosure of all government information (subject to certain limited and specific exemptions) in order to facilitate informed public participation in policy formulation; ensure fairness in government decision making; and permit the airing and reconciliation of divergent views. No other province or territory has gone so far in expressing such objectives.
> > Nunavut		
Access to Information and Protection of Privacy Act – http://www.justice.gov.nt.ca/PDF/ACTS/Access_to_Information.pdf	Provincial	Same as Northwest Territories
> > Ontario		
Freedom of Information and Protection of Privacy Act (FIPPA) – http://www.accessandprivacy.gov.on.ca/english/act/index.html	Provincial	The purposes of this Act are, • to provide a right of access to information under the control of institutions in accordance with the principles that, o information should be available to the public, o necessary exemptions from the right of access should be limited and specific, and o decisions on the disclosure of government information should be reviewed independently of government; and • to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information. R.S.O. 1990, c. F.31, s. 1.
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) – http://www.accessandprivacy.gov.on.ca/english/act/index.html	Provincial	The purposes of this Act are, • to provide a right of access to information under the control of institutions in accordance with the principles that, o information should be available to the public, o necessary exemptions from the right of access should be limited and specific, and o decisions on the disclosure of information should be reviewed independently of the institution controlling the information; and • to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information. R.S.O. 1990, c. M.56, s. 1.
Clean Water Act – http://www.ene.gov.on.ca/en/water/cleanwater/index.php	Provincial	The Clean Water Act requires local multi-stakeholder source protection committees to prepare science based assessment reports for designated watershed areas.

Title – Web Link		Objective
> > Prince Edward Island		
Freedom of Information and Protection of Privacy Act – http://www.gov.pe.ca/attorneygeneral/index.php3?number=1024336&lang=E	Provincial	The purposes of this Act are • to allow any person a right of access to the records in the custody or under the control of a public body subject to limited and specific exceptions as set out in this Act; • to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information and to control the disclosure by a public body of that information; • to allow individuals, subject to limited and specific exceptions as set out in this Act, a right of access to personal information about themselves that is held by a public body; • to allow individuals a right to request corrections to personal information about themselves that is held by a public body; and • to provide for independent reviews of decisions made by public bodies under this Act
PEI Archaeological Sites Protection Act – http://www.gov.pe.ca/law/regulations/index.php3	Provincial	The Act supports: Establish policies or programs respecting (a) the protection and preservation; (b) the coordination of orderly development; (c) the study and interpretation; and (d) the promotion of appreciation, of archaeological, and paleontological, objects and sites in the province. The Government entering into any agreement respecting the coordination, preservation, study, interpretation and promotion of archaeology or palaeontology in the province, with (a) the Government of Canada or the government of another province; or (b) any person, agency or organization. The development of programs to support and encourage the conservation of archaeological sites and archaeological or paleontological objects. The Minister may establish an advisory panel to advise the Minister with respect to matters pertaining to this Act.
> > Quebec		
Content to be added as document lives	Provincial	
> > Saskatchewan		
Freedom of Information and Protection of Privacy Act – http://www.justice.gov.sk.ca/Freedom-of-Information-and-Protection-of-Privacy-Act	Provincial	The Freedom of Information and Protection of Privacy Act allows people to apply for access to information possessed or controlled by government, subject to certain exemptions. The Act also establishes privacy rules for how the government may collect and use personal information.
Local Authority Freedom of Information and Protection of Privacy Act – http://www.justice.gov.sk.ca/Local-Authority-Freedom-of-Information-and-Protection-of-Privacy-Act	Provincial	The Local Authority Freedom of Information and Protection of Privacy Act allows people, subject to certain exemptions, to apply for access to information possessed or controlled by a local authority, such as a municipality, board of education, hospital or special-care home. The Act also establishes privacy rules for how a local authority may collect and use personal information.

Title – Web Link		Objective
> > Yukon		
Access to Information & Protection of Privacy Act (ATIPP Act) – http://www.atipp.gov.yk.ca/	Provincial	The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by • giving the public a right of access to records; • giving individuals a right of access to, and a right to request correction of, personal information about themselves; • specifying limited exceptions to the rights of access; • preventing the unauthorized collection, use, or disclosure of personal information by public bodies; and • providing for an independent review of decisions made under this Act.
> Regulations > Federal		
Content to be added as document lives		
> Regulations > Provincial		
> > Northwest Territories		
Northwest Territories Archaeological Sites Regulations – http://pwnhc.learnnet.nt.ca/programs/downloads/NWTASR.E.pdf	Provincial	These Regulations apply to all lands and waters in the Northwest Territories other than • those within the boundaries of a park, as defined in the *Canada National Parks Act*; and • any lands set apart as a national historic site of Canada under section 42 of that Act.
> > Nunavut		
Nunavut Archaeological & Paleontological Sites Regulations – http://ftp.nirb.ca/REVIEWS/CURRENT_REVIEWS/06MN082-ZINIFEX_HIGH_LAKE/1-SCREENING/02-DISTRIBUTION/COMMENTS/061103-06MN082-CLEY_Comments-IMAE.pdf	Provincial	Under the Nunavut Act, the federal government can make regulations for the protection, care and preservation of paleontological sites and specimens in Nunavut. Under the Nunavut Archaeological and Paleontological Sites Regulations, it is illegal to alter or disturb any paleontological site in Nunavut unless permission is first granted through the permitting process.
> Policies > Federal		
Policy on Access to Information – http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453	Federal	The objectives of this policy are to: facilitate statutory and regulatory compliance, and to enhance effective application of the Access to Information Act and its Regulations by government institutions; and ensure consistency in practices and procedures in administering the Act and Regulations so that applicants receive assistance throughout the request process.
Policy on Privacy Protection – http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text#cha9	Federal	The objectives of this policy are to: facilitate statutory and regulatory compliance, and to enhance effective application of the Privacy Act and its Regulations by government institutions; ensure consistency in practices and procedures in administering the Act and Regulations so that applicants receive assistance in filing requests for access to personal information and ensure effective protection and management of personal information by identifying, assessing, monitoring and mitigating privacy risks in government programs and activities involving the collection, retention, use, disclosure and disposal of personal information. It replaces the *Policy on Privacy and Data Protection* dated 1993, and all mandatory policy requirements contained in Implementation Reports issued up to April 1, 2008.

Title – Web Link		Objective
Privacy Impact Assessment – http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450	Federal	The Government of Canada's new Privacy Impact Assessment Policy (PIA) enhances the government's implementation of the federal Privacy Act by providing federal departments and agencies with a consistent framework to identify and resolve privacy issues during the design or re-design of programs and services.
Critical Infrastructure Policy	Federal	Information Sharing and Protection under the Emergency Management Act
> Policies > Provincial		
Content to be added as document lives		
> Guidelines and Frameworks - Federal		
Securing Publicly Available Information (Office of Critical Infrastructure Protection and Emergency Preparedness) – http://www.publicsafety.gc.ca/prg/em/ccirc/2002/in02-005-eng.aspx	Federal	The purpose of this document is to assist security professionals in identifying risk management strategies for sensitive information that, if in the public domain, could place critical infrastructure (CI) at greater risk. Owners and operators of CI are encouraged to consider these criteria when deciding whether information should be made available to the public via the Internet or through other means.
Guide for Private Sector Entities – http://www.publicsafety.gc.ca/prg/em/cip/_fl/labelling-sensitive-cip-information-eng.pdf	Federal	Identifying and Marking Critical Infrastructure Management (CI/EM) Information Shared in Confidence with the Government of Canada
Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks (Treasury Board Secretariat) – http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp	Federal	The guidelines are intended to provide a comprehensive framework for the completion of a Privacy Impact Assessment (PIA). They convey practical advice on the application of the Government of Canada's Privacy Impact Assessment Policy.
Right of Access – Access to Information and Privacy (Treasury Board Secretariat) – http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13783	Federal	This document contains the guidelines for the Determination of Presence and the special rules relating to third party objections regarding the right of access.
Taking Privacy into Account Before Making Contracting Decisions (Treasury Board Secretariat) – http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do-eng.asp	Federal	This guidance document is intended to provide advice to federal government institutions whenever they consider contracting out activities in which personal information about Canadians is handled or accessed by private sector agencies under contract. The document was developed in response to privacy risks associated with the potential exposure of Canadians' personal information to U.S. authorities under the USA PATRIOT Act.

Title – Web Link		Objective
> Guidelines and Frameworks - Provincial		
> > Yukon		
Yukon Archaeological Sites Regulations – Guidelines to Permit Holders – http://www.tc.gov.yk.ca/pdf/PermitGuidelines08.pdf	Provincial	Archaeological sites and access to site information are protected by legislation in the Yukon. Please note that documents submitted to YESAA Designated Offices, or to the Yukon Water Board, or to Yukon land regulators in respect of land use or land disposal, are public documents. It is requested that site location and other sensitive site information not be included in public release documents.

Appendix C – Annotated Bibliography and Relevant Links

A Developers' Guide to the CGDI: Developing and publishing geographic information, data and associated services

GeoConnections 2007

The Guide to the CGDI describes the Canadian Geospatial Data Infrastructure, and explains how you can use it. If you would like to increase the accessibility and visibility of your organization's data and services within the CGDI, or build an application with CGDI-endorsed standards and specifications, the Guide to the CGDI will show you how. Chapter 11 of this publication discusses aspects of providing access to Services and Data products through the CGDI. This includes Web Security options within the CGDI, such as Communication Security (Authentication, Authorization, Integrity) and GeoSpatial Data Rights Management (GeoDRM).

http://www.geoconnections.net/publications/Technical_Manual/2007/CGDI_devguide_2007.pdf

Aboriginal Community Land and Resource Management: Geospatial Data Needs Assessment and Data Identification and Analysis:

Executive Summary
Volume 1, Aboriginal Mapping and Information Needs: Experiences from Ten Land Use Planning Processes Across Canada
Volume 2, Data Identification and Analysis

Makivik Corporation Nov 2008

Prepared for GeoConnections, this report assessed 10 Aboriginal land use plans from across Canada and documents the methodologies used in the plans and the data that were relied upon for their preparation, analysis and implementation.

Of particular relevance to sensitive geospatial are the discussions defining what data is considered confidential and sensitive and how significant this data is to the planning process.

Relevant – discusses issues with sensitivities around aboriginal land use data and planning especially Traditional Ecological Knowledge (TEK) data. Make recommendation "Government and industry should collect and share confidentiality agreements and intellectual rights agreements between communities and third parties via networks such as the Aboriginal Mapping Network".

http://www.geoconnections.org/publications/Key_documents/Executive_Summary_E.pdf
http://www.geoconnections.org/publications/Key_documents/Volume1_E.pdf
http://www.geoconnections.org/publications/Key_documents/Volume2_E.pdf

Access to Sensitive Spatial Data - Discussion Paper

ANZLIC Council July 16, 2004

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.

Geospatial Data Policy Study

Sears, G., KPMG Consulting Inc. Mar 28, 2001

KPMG report on fee and non-fee based dissemination of Geospatial data by governments. The recommendations in this report are reviewed by CCOG (see 27 below).

Geospatial Information Needs for Integrated Land/Marine Management – Workshop Report PRI Project – Sustainable Development

Policy Research Institute Jan 2006

This is a report resulting from the national workshop on integrated land/marine management held in Ottawa in January 2006 to explore in detail the role of geographic information to support an integrated approach to land, freshwater and marine management. The meeting brought together of 60 practitioners of integrated approached t land, freshwater and marine environments. They spoke to content requirements, as well as policy and technical issues. The results provided valuable input to the criteria used in moving the Integrated Land Management practice forward.

Good Practices in Regional-Scale Information Integration

Hickling, Arthurs, Low: Technology Management, Strategy and Economics Mar 2008

While there is significant opportunity for the use of CGDI to support public policy decision makers, there is limited awareness of the numerous challenges in performing regional scale information integration and the means of addressing them. The report assessed four projects to identify good practices.
The study concludes that there are a number of factors that would contribute to further deployment of CGDI: establish stable funding for regional CGDI data providers; geomatics industry adopt and enhance CGDI-endorsed standards; and communities of practice recognizing the benefits of, and implementing CGDI standards.

Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

Federal Geographic Data Committee June 2005

The guidelines provide standard procedures to:
1. Identify sensitive information content of geospatial data that pose a risk to security.
2. Review decisions about sensitive information content during reassessments of safeguards on geospatial data.
Additionally, the guidelines provide a method for balancing security risks and the benefits of geospatial data dissemination.
These guidelines form the basis for much of the policies and procedures for managing sensitive geospatial data for federal departments, state and municipal organizations in the United States.
The focus of sensitive in these guidelines is from a Public Safety and Security perspective.

Guide to Best Practices for Generalizing Sensitive Species Occurrence Data

Chapman, D. and Grafton, O. 2008

A Best Practices document from a study done in UK which is very similar to what we are doing. The same approach was taken but the main difference is that they are focused on biodiversity

information and not spatial data.

Health Canada Privacy Impact Assessment (PIA) Tool Kit

Corporate Services Branch of Health Canada — Nov 3, 2006

This document provides guidelines and templates for Health Canada staff to execute a Privacy Impact Assessment as is required under the Privacy Act. It provides a roadmap for stepping the reader through the process of deciding if a PIA is required and if so how to move forward. Report has 2 parts: PIA Process, including Health Canada PIA Roadmap, Lessons Learned to Date, and Health Canada's PIA Processes; and PIA Tools Checklist, Q&A, Template, Samples and Reference Materials.

Identifying Sensitive Critical Infrastructure Data

Jones, B., James W. Sewall Company

Using RAND report methodology (i.e. three filters for defining sensitive data), this paper "…reviews current public and private data sharing mechanisms; and explores the impact of federal acts on data access." Data focus is on critical infrastructure.

Most of paper is a summary of RAND methodology with a focus on critical infrastructure data. Points raised in paragraphs preceding Summary section with respect to the Freedom of Information Act (FOIA) may pertain to Canada as well even though our reports concern is not critical infrastructure data.

Making Decisions About 'Sensitive' Geospatial Data - EIIP Virtual Forum Presentation

Domaratz, M., National Geospatial Programs Office U.S. Geological Survey — Nov 16, 2005

This presentation is based on work of the Homeland Security Working Group of the FGDC who created a decision tree for defining sensitive data. This working group developed the guidelines to help organizations decide on reasonable access to sensitive data. The HLWG's decision tree is adapted from RAND Corporation report "Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information".

Mapping and Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information

Baker, J., Lachman, B., Frelinger, D.' O'Connell, K., Hou, A., Tseng, M., Orletsky, D., Yost, C. — 2004

Report follows Sept 11 terrorist attacks to assist data originators and users of geospatial data in determining the need for security safeguards. The analytical approach presented in this study integrates three distinct filters—usefulness, uniqueness, and societal benefits and costs—as a first-step framework for decision makers to help evaluate whether a geospatial dataset is conceivably sensitive, and whether public access should be curtailed in some way.

Provides a reasonable approach to defining sensitive geodata for protecting against terrorists acquiring data to carry out their events thus making it sensitive. Thus this report comes from predetermined perspective of the terrorist attackers needs for specific geospatial data. Practitioners may leverage this sort of decision tree but may not be able to define the intent of the proponent of the data to sculpt the decision tree for sensitive environmental sustainability and land use geospatial data.

Model Code for the Protection of Personal Information

Canadian Standards Association

Model Code for the Protection of Personal Information (Q830) sets out ten principles that balance the privacy rights of individuals and the information requirements of private organizations. The Privacy Code was developed using CSA's renowned consensus-based methods. Drawing on the experience gained through this development process, CSA has published a suite of companion resources to help an organization put the Code into practice. In Canada, the key elements of the Privacy Code are now incorporated into the *Personal Information Protection and Electronic Documents Act* (PIPEDA). All organizations that comply with the CSA standard can be confident that they meet the federal requirements of PIPEDA.

Oakland County Michigan Geospatial Data Access, Distribution and Use Policy

Oakland County, Michigan

Definition of the County's geospatial data sharing policies, with specific reference to sensitive geospatial data.

Sensitive geospatial data is defined in terms of privacy, public safety and security, legislation and does the risk of sharing out weigh the benefits.
Provides a decision tree for allowing access to geospatial data based on whether data is classified as sensitive, relationship with requestor and licensing requirements.

Ownership, Control, Access and Possession Sanctioned by the First Nations Information Governance Committee, Assembly of First Nations

First Nations Centre 2007

As a result of heightened interest in the issue of First Nations ownership of information, the OCAP principles were developed during the inception of the First Nations and Inuit Regional Longitudinal Health Survey. The OCAP principles apply to all research, data or information initiatives that involve First Nations. The principles represent a comprehensive framework developed by First Nations to bring self-determination into the realm of research and information management. OCAP applies to all research, data or information initiatives that involve First Nations, and encompasses all aspects of research (including funding and review), monitoring, statistics, cultural knowledge and so on. By insisting on the application of the OCAP principles, First Nations are asserting their authority over all research concerning their communities.

Considerations and Templates For Ethical Research Practices

First Nations Centre 2007

Provides practical guidance to communities interested in developing their own research policies and protocols. Of specific relevance to this project is the Data-Sharing Protocol between the First Nations and research partners. It establishes ownership of the data, including how and under what conditions the data may be shared. The protocol also sets out the principles and obligations that partners must adhere to when they collect, use, store and disclose individual or aggregate information.

Policy Review: Blocking Public Geospatial Data Access is Not Only a Homeland Security Risk

Tombs, B. 2005

Policy review paper suggesting that societal benefits are under weighted in FGDC decision tree.
Proposed Canadian Government Action Plan On Geospatial Data Policy Phillip Nicholson Consultants, Inc. Oct 23, 2001 This CCOG report reviews the KPMG study on Canadian Government Geospatial Data Policy recommendations and suggested go-forward policy. This 2001 study was commissioned in order to provide empirical information on the impact of current government geospatial data policies on government, as well as the users and distributors of the data in the business sector and in the community at large. The report made recommendations on how Canadian government geospatial data dissemination policies and practices could be modified to facilitate business development and improved competiveness of the Canadian geomatics industry while ensuring adequate funding for infrastructure.
The Dissemination of Government Geographic Data in Canada: Guide to Best Practices GeoConnections 2008 The document describes best practices for sharing government geospatial data. It discusses the benefits of sharing, importance of metadata, licensing and agreement models, guidance on which model to use and templates of models. Two of the licensing models are particularly relevant to sensitive geospatial data.

Relevant links:

- Alberta Sustainable Resource Development data product license agreement: http://www.srd.gov.ab.ca/lands/geographicinformation/resourcedataproductcatalogue/productorderprocess.aspx
- Canadian Museum of Civilization, public component of archeological sites inventory: http://collections.civilisations.ca/sites/sitwe01e.html
- Canadian Museum of Civilization Sites Online - WMS at: http://www.civilization.ca/cmc/archeo/sites/sowms00e.shtml
- GBIF: www.gbif.org
- GBIF Data Sharing Agreement: http://data.gbif.org/tutorial/datasharingagreement
- GBIF Data Use Agreement: http://data.gbif.org/tutorial/datauseagreement
- Nature News – Data Sharing: http://www.nature.com/news/specials/datasharing/index.html
- Natural Resources Canada, GeoConnections, Using Metadata to Describe Your Resources: http://www.geoconnections.org/publications/Technical_Manual/html_e/appendix_2-3.html
- Ontario Ministry of Natural Resources, Natural Heritage Information Centre internet facing applications and tools for generalized discovery, promoting awareness and authorized access: http://nhic.mnr.gov.on.ca/nhic_.cfm and http://www.biodiversityexplorer.mnr.gov.on.ca/nhicWEB/main.jsp
- Prince of Wales Northern Heritage Centre Web site at: http://pwnhc.learnnet.nt.ca/programs/archaeology.asp

Appendix D – Project Contribution Acknowledgements

The following are acknowledged for their contributions to the development of these Best Practices.

Last Name	First Name	Organization	Position
Workshop Participants			
Anderson	**Candace**	Canadian Environmental Assessment Agency	Senior Policy Analyst
Bowles	**Ian**	Environmental Monitoring and Reporting Branch, Ontario Ministry of Natural Resources	GIS Officer - Geomatics Centre
Clark	**David**	Canadian Heritage, Parks Canada Agency	Ecological Information Specialist
Ford	**Shane**	NatureServe Canada	Coordinator - BC Conservation Data Centre
Gemza	**Andy**	Environment - Drinking Water Management Division, Ontario Ministry of Natural Resources	Program Coordinator, Information Management
Halverson	**Anne**	Science and Geographic Information Resources Division, Ontario Ministry of Natural Resources	Manager - Information Access Section
Hulsman	**Peter**	Natural Heritage Information Centre, Ontario Ministry of Natural Resources	Coordinator
Hyde	**Doug**	NatureServe Canada	Executive Director
Johanis	**Lucie**	Canadian Museum of Civilization	Sites Officer
Martin	**Ann**	Mapping Information Branch, Natural Resources Canada	Director
McLeod	**Brian**	GeoConnections, Natural Resources Canada	Infrastructure and Technology, Manager
McNichol	**Nora**	GeoConnections, Natural Resources Canada	CGDI Content Analyst
Ogston	**Ryan**	GeoConnections, Natural Resources	Geomatics Policy Advisor

Last Name	First Name	Organization	Position
		Canada	
Paynter	**Jacques**	AMEC Earth and Environmental	Study Facilitator
Prégent	**André**	GeoConnections, Natural Resources Canada	Policy Advisor
Rushforth	**Peter**	GeoConnections, Natural Resources Canada	Technical Advisor
Sayer	**Robert**	AMEC Earth and Environmental	Manager
Speers	**Larry**	Environmental Health, Agriculture and Agri-Food Canada	Research Assistant
Schwarz	**Brian**	AMEC Earth and Environmental	Senior Consultant
Trant	**Doug**	Environment Accounts and Statistics, Statistics Canada	Section Chief
Turner	**Tony**	GeoConnections, Natural Resources Canada	Environment and Sustainable Development Advisor
Van Steenburgh	**Ellen**	Environmental Monitoring and Reporting Branch, Ontario Ministry of Natural Resources	Supervisor - Business Planning and Support
Wyman	**Laine**	City of Ottawa	Program Manager - GIS

Appendix E – Project Methodology and Survey Summary Results

Methodology

The approach taken to collect data and address the issues of these Guidelines was to consult widely to determine the definition of "sensitive" environmental geospatial data, how to determine if data should be classified as "sensitive" and what are the mechanisms for sharing sensitive data and to what degree environmental geospatial data that has been determined to be sensitive can be shared.

The methods used to collect and assess information were to:

- Conduct a literature review (45 documents) of relevant documents;
- Survey stakeholders (33 responses, 30% response rate) in federal and provincial governments, Non-Governmental Organizations (NGO), industry and aboriginal organizations across the country;
- Conducted a workshop (June 8, 2009) to assess a Framework for Assessing Sensitive Environmental Geospatial Data and review mechanisms for sharing sensitive data. The workshop was attended by diverse group of 28 people from federal, provincial and municipal governments as well as NGO representation; and
- Work with selected stakeholders to critique the final document.

While the Guide's survey response was relatively small it was well targeted with the responding organizations characterized as follows:

- 100% collect/create geospatial data;
- 100% receive geospatial data from outside sources;
- 97% share geospatial data externally; and
- 93% produce or consume sensitive geospatial data.

Survey responses were received from:

- Federal Departments – 8
- Provincial Departments – 15
- Municipalities – 1
- NGOs – 4
- Private Sector – 2
- Aboriginal Organization – 2
- Academic - 1

With few exceptions every organization shared their data internally and most shared externally with other government agencies (federal, provincial, territorial and municipal), Non Governmental Agencies (NGO), planning boards, First Nations governments and academics.

The organizations and practitioners that were surveyed and consulted reflect the documents intended audience and are acknowledged for providing valuable insight contributing to these guidelines.

Survey Summary

Part C		Percentage		
		Yes	No	Not Sure
1	Is your organization a user of geospatial data?	93%	7%	0%
2	Does your organization collect/create geospatial data?	100%	0%	0%
3	Does your organization receive geospatial data from an outside source?	100%	0%	0%
4	Does your organization share its geospatial data externally?	97%	3%	0%
6	Does your organization produce or consume **sensitive geospatial** data?	93%	3%	3%
8	Does your organization have any standards, policies, principles or guidelines to ensure the effective utilization and sharing of **sensitive geospatial** data?	67%	10%	23%
9	Is the acquisition, use and/or sharing of **sensitive geospatial** data critical to meeting your business needs?	80%	13%	7%

As the responses indicate, the survey respondents' organizations geospatial activities fell within the core areas of interest for this project. Over 90% of the respondents collect/create geospatial data, receive and share geospatial data externally and deal with **sensitive** geospatial data. Not only do these organizations deal with sensitive geospatial data but it is considered crucial in conducting their business activities.

However, despite the importance of dealing with sensitive geospatial data only 67% of the respondents knew their organizations had standards, policies, principles or guidelines in place to safeguard the sensitive data and a surprising 23% were not sure.

The distribution of how organizations share their data is as follows:

- Internally – 80%
- Other Departments of the government – 63%
- Other levels of government – 70%
- Public – 77%
- Special Interests – 53%

The survey demonstrates that the vast majority of the organizations are sharing data on multiple levels with a wide variety of organizations.

Part D		1 – Strongly Disagree 5 – Strongly Agree					
		1	2	3	4	5	NA
10	The five criteria of **sensitive geospatial** data presented in the introduction are reasonable and clear.						

Part D		1 – Strongly Disagree 5 – Strongly Agree					
		1	**2**	**3**	**4**	**5**	**NA**
	Privacy	7%	3%	7%	17%	57%	10%
	Security	0%	7%	23%	13%	50%	7%
	Intellectual Property	7%	7%	17%	20%	40%	10%
	Confidentiality and Commercial Advantage	0%	13%	10%	20%	47%	10%
	Resource and Cultural Protection	3%	10%	10%	20%	53%	3%
11	Our organization's management is aware of the role and importance that **sensitive geospatial** data plays (or could play) in current or planned initiatives.	0%	7%	10%	40%	37%	7%
12	Management within our organization plays an active role in determining how **sensitive geospatial** data is acquired, used and/or shared	10%	13%	23%	20%	27%	7%
13	A clear and well articulated written policy related to acquisition, use and/or sharing of **sensitive geospatial** data has been established and communicated within our organization.	32%	16%	23%	10%	16%	3%
14	There is a need for enhanced communications aimed at increasing the level of awareness of the issues related to the acquisition, use and/or sharing of **sensitive geospatial** data.	10%	10%	13%	23%	40%	3%
15	The availability of multiple versions of **sensitive geospatial** data from similar, but different sources, maintained by various organizations is an impediment to the security of the information and needs to be addressed.	7%	17%	23%	20%	13%	20%

The survey respondents agreed with the basic distinctions between the defined categories for sensitive geospatial data. However, through the workshop review and assessment the categories have been revised to what is currently defined in Section 2.3.1.

The survey indicates that the management levels of organizations are well aware (77%) of the role and importance of sensitive geospatial data. However, the extent to which management participates in determining how sensitive data is acquired, used and/or shared drops to 47%. Further more, the communication of clear and well articulated written policies related to acquisition, use and/or sharing of **sensitive geospatial** data drops down to 26%.

The responses suggest that while there is recognition of the fact that organizations are dealing with sensitive data there is not the management level follow through to ensure that the data is treated as such. The responses also show a wide range in how organizations respond to managing the implementation of these policies from leaving it in

the hands of the technical staff to figure it out to very hands on participation and support by senior management levels within the organization.

The level of seriousness that an organization places on this issue seems to be determined by the importance the organization places on the integrity of the data and the need to have trusted interactions with data partners. It also appears that while technology is rapidly advancing allowing for greater interoperability and sharing of data, organizations have not kept up on the policy implications. Many respondents indicated that this is a recognized area for improvement.

There were several comments to the effect that some groups treat data as sensitive simply because that is how they have always treated it or individuals have been over protective of the data and have not bought into the principle that data is to be shared unless there is a justifiable reason not to.

16 - What does your organization consider to be **sensitive environmental geospatial** data and why?

The responses ranged from "Don't know" to very specific identification of data content. Examples of the types of data considered sensitive are found in Section 2.4. Why data is considered sensitive is primarily driven by definitions in legislation and agreements and cover the full gamut of sensitivity categories.

17 - What parameters and/or criteria does your organization use to identify and/or classify **sensitive environmental geospatial** data?

The responses again show a wide range of approaches to how data is recognized as sensitive. In some cases there are registers that specify what is sensitive (e.g. list of archaeological sites and species at risk), in other cases it is found within the definitions in legislation (e.g. data related to privacy), it is often defined in data sharing agreements, some organizations have guidelines and in other cases it is left to the discretion of the Custodian.

Part E		Percentage		
		Yes	No	Not Sure
19	For sharing of data, which categories typically apply to **sensitive environmental geospatial** data and why?			
	Privacy	53%	20%	27%
	Security	50%	20%	30%
	Intellectual Property	47%	27%	27%
	Confidentiality and Commercial Advantage	43%	27%	30%
	Resource and Cultural Protection	80%	10%	10%

Not surprisingly most organizations feel that the Resource and Cultural protection categories apply to their data, what is surprising is the consistency in the level of the other

four categories. It demonstrates that organizations are dealing with multiple issues when they are assessing their datasets.

20 - What are the barriers to the acquisition, use and/or sharing of **sensitive environmental geospatial** data **internally** and **externally** to your organization (corporate or government)?

A few themes emerged from the survey responses related to barriers to sharing data:

- Number one is trust. There are concerns that data may be misinterpreted or inappropriately used by either internal or external resources;
- Technical issues such as large volumes of data, inconsistent data collection methods and data standards, high speed internet access;
- Lack of clear criteria for defining sensitive data (although this is being addressed by several organizations), guidelines for assessing sensitivity and guidelines for sharing sensitive data;
- Effort/funds required to:
    - Establish agreements;
    - Responding to requests and prepare data; and
    - Put processes, standards and infrastructure in place.

21 - What is the potential for, or barriers to, sharing **sensitive environmental geospatial** data with the public?

The themes are similar to Question 20 with additional emphasis on the concern of how the public will interpret and use the data. Other issues included accuracy of data, using the lowest common denominator when sharing data from multiple jurisdictions.

Part E		Percentage				
		None	Written Agreement	MOU	Legal Contract / License	Other
22	What are some of the conditions that would be required for your organization to share **sensitive environmental geospatial** data?	4%	33%	28%	25%	11%

The responses indicate that 86% of the organizations rely on some form of instrument in order to share data. The type of instrument put in place is based on the legal relationship between the two organizations (see Section 4.1).

Several organizations indicated that they remove the sensitivity from the data in order t make it available.

23 - Within your organization, who should be responsible for defining policy and procedures regarding **sensitive environmental geospatial** data; and ensuring that these are communicated, understood, and respected?

The responses generally pointed to a specific senior organizational position that had the authority to set and enforce the policy. Many responses also pointed to committees that would have the responsibility. Only a few did not know or have an opinion.

24 - How does your organization ensure compliance with agreements when you share **sensitive environmental geospatial** data?

Overwhelmingly the responses indicated that this is not activity that is actively pursued due to the fact that:

- It is not considered an issue;
- Lack the resources to do so; or
- Do not have the mechanisms to do so.

The organizations rely on trust, peer pressure, whistle blowers, training and adherence to work contract.

Consequences range from none, to revoking further access to data to potential legal action.

25 - Does your organization modify **sensitive environmental geospatial** data before sharing it?

Less than 50% of the respondents indicated that they will alter the content in order to remove sensitivity. For those that do alter the content, most indicated that this is done to a copy of the data and that the source data remains untouched.

26 - What technologies does your organization use to safeguard **sensitive environmental geospatial** data?

Most organizations rely on restricting physical access and/or permitting access based on log in procedures (user has been validated and granted permission to access to the data) and on the overall network security architecture of the organization.

27 - What other mechanisms is your organization considering in order to share **sensitive environmental geospatial** data?

The most common mechanism being considered by organizations (6) is the use of secure web services. Other mechanisms include creating common databases across departments with associate security mechanisms, publishing all metadata including for sensitive data, controlled user access and removing the sensitive aspect of the data.