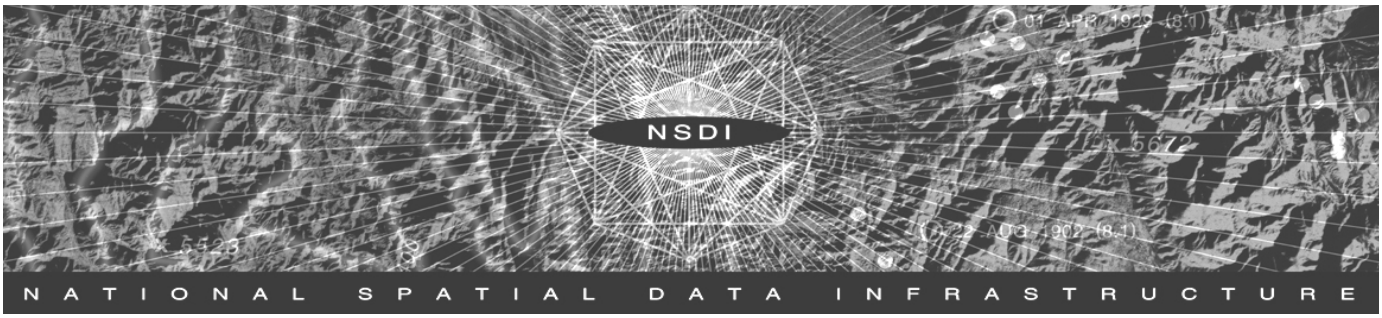


Final **June 2005**

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

What is the purpose of the guidelines?

Many public, private, and non-profit organizations originate and publicly disseminate geospatial data. Dissemination is essential to the missions of many organizations and the majority of these data are appropriate for public release. However, a small portion of these data could pose risks to security and may therefore require safeguarding. Although there is not much publicly available geospatial information that is sensitive (Baker and others, 2004, page 123), managers of geospatial information have safeguarded information using different decision procedures and criteria.

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. If safeguarding is justified, the guidelines help organizations select appropriate risk-based safeguards that provide access to geospatial data and still protect sensitive information content.

The guidelines do not grant any new authority and are to be carried out within existing authorities available to organizations. They apply to geospatial data irrespective of the means of data access or delivery method, or the format.

How are the guidelines organized?

The guidelines provide a procedure consisting of a sequence of decisions (see Figure 1) that an originating organization should make about geospatial data. Each decision is accompanied by related instructions and discussion.

The decision sequence is organized using the following rationale:

I. Do the geospatial data originate in the organization? If not, the organization is instructed to follow the instructions related to safeguarding that accompany the data.

II. If the geospatial data originate in the organization, do the data need to be safeguarded? This decision is based on three factors:

- Risk to security: Are the data useful for selecting one or more specific potential targets, and/or for planning and executing an attack on a potential target?
- Uniqueness of information: If the data contain information that pose a security risk, is this sensitive information difficult to observe and not available from open sources?
- Net benefit of disseminating data: If the sensitive information poses a risk to security and is unique to the geospatial data, do the security costs of disseminating the data outweigh the societal benefits of data dissemination?

Safeguarding is justified only for data that contain sensitive information, that are the unique source of the sensitive information, and for which the security risk outweighs the societal benefit of dissemination.

III. If the data need to be safeguarded, what safeguards are justified? The guidelines offer two options:

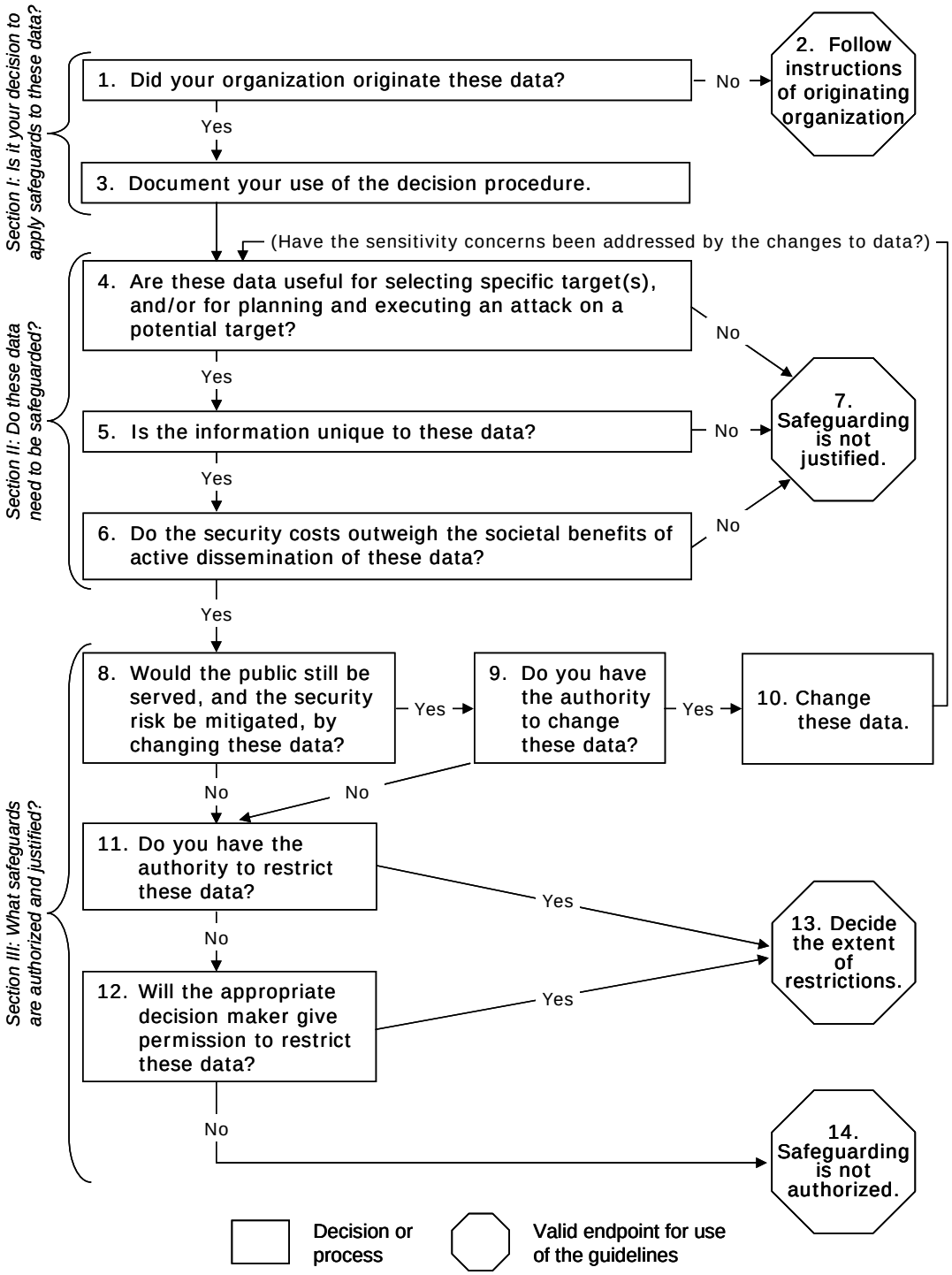
- Change the data: Change the data to remove or modify the sensitive information and then make the changed data available without further safeguards. Organizations are advised to review the changed data to ensure that the change(s) dealt effectively with the security concern.

FEDERAL GEOGRAPHIC DATA COMMITTEE
U.S. GEOLOGICAL SURVEY, 590 NATIONAL CENTER
RESTON, VIRGINIA 20192
Http://www.fgdc.gov
PHONE: 703-648-5514
FAX: 703-648-5755
EMAIL: fgdc@fgdc.gov

- Restrict the data: Establish restrictions, commensurate with the assessed risk, on access to, use of, or redistribution of the data.

In both cases, organizations are advised to ensure that they have the authority to safeguard the data. If they do not have the authority, they may seek it from an appropriate decision maker. The decision maker may provide the authority to safeguard the data, overrule the conclusion that the data require safeguarding, or find that there are no legal means to safeguard the data.

Figure 1. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns



Why were the guidelines developed?

Geospatial data play a vital role in the United States. They underpin one-half of the Nation's domestic economic activities (National Academy of Public Administration, 1998, page 11), aid our international competitiveness, support a large array of Federal, state, local, and tribal government activities, and serve the general public.

In the United States many public and private organizations and individuals originate geospatial data and make them available to the public. Because of this condition centralized control of information is not viable and decision making about the sensitivity and safeguarding of geospatial data will be decentralized.

Although there is not much publicly available geospatial information that is sensitive, organizations have safeguarded geospatial information based on the use of differing procedures and criteria. Some organizations have curtailed access without assessing the risk to security, the significance of consequences associated with improper use of the data, or the public benefits for which the data were originally made available. Contradictory decisions and actions by different organizations easily can negate each organization's actions.

Guidelines for identifying sensitive data, determining risks associated with them, and assessing their benefits help the geospatial data community in several ways. They help organizations take appropriate actions by evaluating the sensitive content in the context of other available information, the benefits lost by restricting data access, and the options for safeguarding data. Use of guidelines can frame discussions about the importance of making data publicly accessible and encourage the development of consensus decisions. Use of a common, standardized approach to the identification of geospatial data that have sensitive content and to the appropriate safeguarding of such information will increase the consistency among individual organization's actions. The guidelines help organizations decide on reasonable access to sensitive data and avoid unnecessary safeguards that unduly restrict public access to geospatial data.

On what premises are the guidelines based?

The guidelines strike a balance among these principles:

- Provide appropriate safeguarding for information that could potentially be used to inflict significant harmful consequences to public safety or security of property.
- Provide for the free flow of information between the government and the public essential to a democratic society. This flow of information enables both informed public participation in decision-making and private reuse of government information. It is also essential to minimizing the burden of government paperwork on the public, minimizing the cost of government information activities, and maximizing the usefulness of government information.
- Recognize that geospatial data often have value to organizations other than the organization that originates the data. The fundamental tenet of the National Spatial Data Infrastructure to "build once and share or use many times" should be supported to the maximum feasible extent.
- Continue the benefits that accessible geospatial data provide to the Nation's economic and scientific enterprises.
- Provide and continue public access to information needed to implement and enforce laws and regulations for the protection of public health and safety and the environment, land management, and other public purposes.
- Enable the sharing of information among organizations as needed to allow them to accomplish their missions and goals.
- Promote the economical management and maintenance of government information and avoid duplication.

These principles are drawn from relevant policies, including Federal and state laws and related implementation instructions regarding freedom of information and public records; information management; the public's right to participate in government policy development and decision making; the public's right to review information used in government decision making; the public's "right to know"; protection of sensitive information for national security and homeland security reasons; prohibition of transactions with persons who commit, threaten to commit, or support terrorism; and government depository libraries. Appendix 1 contains a sample list of these policies. Analyses from the RAND Corporation report "Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information" (Baker and others, 2004) were considered in developing the guidelines. Work by the

National States Geographic Information Council (National States Geographic Information Council, 2002) provided the basis for the decision-making approach used in the guidelines.

To whom are the guidelines directed?

The guidelines are directed at organizations that originate geospatial data and are interested in disseminating data publicly, but are concerned that such actions may pose a risk to security. Persons using the guidelines should be knowledgeable about their organization's authorities, policies, and decision making processes related to data access; the potential security risks posed by dissemination of the geospatial data; the benefits that users receive from the organization's data and the impacts of changes to data access on these users; and the ability to evaluate the information content and utility of geospatial data and compare them to other sources of information. Decisions must also be made with full knowledge and participation on the part of the executive management of the organization.

If the originating organization is uncertain about the potential security consequences of disseminating geospatial data, it should seek advice from others including legal counsel, security organizations, and facility operators. Law enforcement and emergency management agencies experienced in homeland security matters are sources of advice on the likelihood of an attack scenario and the potential consequences of such an event. Remember, however, that such advice may tend to overestimate the security risks posed by geospatial data and is unlikely to include consideration of the broad range of alternate information sources available from the geospatial and other communities. For those reasons, care should be taken to familiarize advisors with the current state of geospatial data uses and availability so that the originating organization receives practical and useful advice. That said, the responsibility for making decisions about safeguarding ultimately rests with the originating organization.

Assessments of risks and costs must also be balanced with a full understanding of the benefits of data dissemination. Originating organizations should seek advice from the known or potential users regarding the benefits of the information. Keep in mind that benefits are often highly decentralized. Benefits to geospatial data users outside the originating organization (secondary users) can be greater than those to users within the originating organization (primary users). Outside (secondary) users may receive data directly from originating organizations or indirectly through intermediaries such as libraries or companies that repackage or add value to data.

What terms are used in the guidelines?

authority – permission; the power to act that is officially or formally granted.

change – to make different in some particular aspect; to undergo a loss or modification. For the guidelines, the idea of "changing" geospatial data (see Steps 8 through 10) includes removing sensitive information and reducing the sensitivity by generalizing the data (that is, reducing the level of detail).

choke point – a strategic narrow route providing passage through or to another region; a strategic point in a transportation, transmission, or communication route which limits movement of traffic, commodities, or information to areas and regions beyond it.

disinformation – misinformation that is deliberately disseminated in order to influence or confuse adversaries.

geospatial data – data that identify the geographic location and characteristics (attributes) of natural or constructed features and boundaries on the earth. These data may be derived from, among other things, remote sensing, mapping, and surveying technologies.

metadata – data about data; data that describe the content, quality, condition, and other characteristics of data.

open-source information – publicly available information (that is, information that any member of the public could lawfully obtain by request or observation), as well as other unclassified information that has limited public distribution or access (including information from companies, academia, and other sources). Access to such information may or may not require payment. Examples of open-source information include all types of media, government reports and other documents, scientific research and reports, commercial vendors of information, and the Internet.

opportunity cost – the benefit foregone from not using a good or resource (geospatial data in the case of the guidelines) in its best use.

originating organization – an organization or individual that develops or sponsors the development of geospatial data.

redact – to prepare for publication or presentation by removing information and indicating that it was removed.

restrict – to limit access to, use of, or redistribution of data.

safeguard – an activity intended to protect by preventing something from happening; a process, procedure, technique, or feature intended to mitigate the effects of risk. As a verb, to provide a safeguard for.

What concerns are not addressed by the guidelines?

Internal procedures for protecting data: The guidelines assume that organizations already have procedures for handling sensitive data internally. These procedures would include the handling of data by the organization's agents, such as contractors.

Ability to implement the guidelines: The guidelines assume that organizations have executive and management officials who have the authority to take the actions recommended in the guidelines, mechanisms to coordinate with other organizations so as to jointly act in safeguarding data identified as being sensitive, and methods to coordinate outside requests for data among appropriate parties within the organization. The guidelines do not address internal procedures needed to carry out the guidelines, the costs of implementing the guidelines, or ways to fund such costs.

Enforcement of restrictions on "downstream" users: The legitimate sharing of sensitive data raises questions about chains of control and the ability to enforce an originator's restrictions and any subsequent changes thereto on "downstream" users. Other than urging them to respect the restrictions assigned by originating organizations, the guidelines do not directly identify the responsibilities of organizations that receive or add value to data, or of intermediaries such as libraries, distributors, and other information brokers.

Review of decisions in response to changing environments: Decisions made about the sensitivity of geospatial data and the safeguards that are appropriate for sensitive data will inevitably change over time. Reasons include better understanding of security risks, changes in the value of geospatial data through time, and changes in competing means of gathering information. Reviews of decisions can result in a decrease, an increase, or no change in access. Altering the access to geospatial data affects not only the originating organization, but also "downstream" organizations.

Decisions about the sensitivity of derived geospatial data: Derived geospatial data, which are developed by combining or querying one or more data sets, present special challenges, especially if the source data are sensitive. Such derived works may or may not be sensitive. In addition to using the guidelines to evaluate the derived data set, organizations that develop derived data sets should contact the originators of sensitive source data to determine whether the derived data are also sensitive.

Appeals of an originating organization's decisions: Organizations should only use the guidelines to make decisions that are permitted by existing authorities. Appeals about such decisions are therefore made using procedures available under the authority cited by the originating organization.

Under what authority are the guidelines issued?

The Federal Geographic Data Committee issues the guidelines under the authority provided by U.S. Office of Management and Budget Circular A-16 to establish procedures necessary and sufficient to carry out interagency coordination and to implement the National Spatial Data Infrastructure.

When will the guidelines be reviewed, and when will they expire?

The Federal Geographic Data Committee will review these guidelines no later than five years after the date of approval. Factors to be considered include changes in security risks and the business practices of the geospatial data community, and an assessment of the degree to which the guidelines have accomplished their purpose.

The guidelines expire when superseded or when withdrawn by the Federal Geographic Data Committee.

Decision Procedure

The decision procedure is provided in the form of a decision tree (see Figure 1) and the following related instructions and discussion.

Note that the procedure has been followed correctly only when you reach one of the following: Step 2, Step 7, Step 13, or Step 14.

Section I: Is it your decision to apply safeguards to these 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.

Discussion: If your organization did not originate the geospatial data you should not make decisions about safeguarding the data.

Step 2 – Follow instructions of the originating organization.

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

Discussion: You should honor any instructions that accompany the data. If no instructions accompany 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. You are responsible for knowing and honoring restrictions that accompany the data.

Step 3 – Document your use of the decision procedure.

As you follow the decision procedure, organize and document your decisions. The documentation should include the identification of the geospatial data, the potential security 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. Appendix 2 identifies elements in the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in the metadata. Go to Step 4.

Discussion: Organizations will find it useful to document their actions so that they are positioned to review the consistency of their decisions, recall their reasoning when reviewing a decision, and explain a decision if challenged. Organizations also should describe decisions and actions to organizations that receive the data.

Section II: Do these data need to be safeguarded?

Overview: This section provides guidelines to decide if the geospatial data need safeguards.

Step 4 – Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

Does knowledge of the location and purpose of a feature, as described by the data, have the potential to significantly compromise the security of persons, property, or systems? For example, do the data:

- Provide accurate coordinates for facilities that are not otherwise available and not visible from public locations?
- Provide insights on choke points, which, if used to plan an attack, would increase its effectiveness?
- Aid the choice of a particular mode of attack by helping an adversary analyze a feature to find the best way to cause catastrophic failure?
- Provide relevant current (real-time, near real-time, or very recent) security-related data that are not otherwise available?

Do the data identify specific features that render a potential target more vulnerable to attack? For example, do the data:

- Identify internal features that are critical to the operation of a facility such as spent fuel storage at a nuclear reactor or the location of unsecured valve bodies on a major pipeline?
- Provide details on facility layout and vulnerabilities such as the location of security personnel or storage areas for hazardous materials?
- Provide insights into operational practices such as shift changes or patrol areas for security personnel or the times that sensitive operations are performed?
- Provide relevant current (real-time, near real-time, or very recent) vulnerability-related data that are not otherwise available?

If the answer to BOTH parts of the question is no, then safeguarding is not justified and you should go to Step 7. If the answer to EITHER part is yes, go to Step 5.

Discussion: In effect, this step performs a "user needs assessment" in which the "user" is an adversary. You are asked to evaluate two aspects of the data. First, do the data provide information about the location and nature of facilities or features that would allow an adversary to select critical targets? Second, do the data provide information that is helpful in executing an attack and/or maximizing the resulting damage because they offer intimate knowledge of a facility, its characteristics, or its operations?

Sensitive information does not include the fact of existence of a facility at a particular place or the general layout of a facility. Concern centers on data that provide very specific and timely information. Such security-related data include information about the relative importance of a feature to a larger system or other systems; the timing of activities; communication capabilities; detailed business and industrial processes; architectural and engineering plans; previously identified vulnerabilities and relationships to, or interdependencies with, larger or other systems; measures and plans for securing and protecting facilities; and measures and plans for responding to attacks or damage. In many cases, the attribute component of geospatial data is more likely to be sensitive than is the location component.

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. Depending on the mode or intended outcome of an attack or on what other information is available, relatively low cost, low accuracy, or historical data may be satisfactory for an adversary's purpose.

Examples:

- Regarding knowledge that aids selection of a target: Does an attribute table provide a detailed inventory of hazardous material in a facility? Very current information (for example, a daily inventory) would be of much greater concern than would be summary information (for example, a yearly average).
- Regarding specific features that render a potential target vulnerable: Do the data locate and identify operational procedures at facilities, floor plans showing exact storage locations, or information about the security measures in place at a facility?

Step 5 – Is the information unique to these data?

In particular is the information that appears to be sensitive based on the evaluation in Step 4:

- 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)?
- Not available from open-source engineering or technical sources?
- Not available from open-source 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 7. If the geospatial data under evaluation provide unique information that cannot be obtained from observation or open sources, you go to Step 6.

Discussion: This step addresses the likelihood that actions you take to safeguard information will be effective. If information encoded by data that appears to be sensitive (based on the evaluation in Step 4) is readily available from observation or open sources, efforts to safeguard the information are unlikely to reduce vulnerabilities or be effective.

Remember that the goal is to identify information that is unique, not just geospatial data that are unique. Your data may be the only "geospatial" source of an item of information, but other publications and media may disclose the same information.

Consider relevant historical data in addition to contemporary data. A facility constructed thirty years ago not only is described in new data, but also in data, maps, imagery, and other sources compiled and disseminated during the previous thirty years.

Decisions to safeguard data are only effective when all parties that have similar information choose the same action. In the case of organizations that originate similar information through independent actions, consultation among the organizations about appropriate safeguarding would increase the effectiveness their actions.

Examples:

- Data that show the layout of a publicly observable facility (for example, a bridge, radio tower, water tower, or national monument) may be considered sensitive upon initial evaluation. However, experts generally agree that adversaries visit their intended targets in person and they would, therefore, be able to easily observe the layout.
- A government agency may initially think that the location of a police station should be withheld from an Internet mapping system. However, the locations of such facilities must be widely known for them to effectively serve the public. They can be easily found by looking in telephone directories or by driving past the site.

Step 6 – Do the security costs outweigh the societal benefits of active dissemination of these data?

In particular would the sensitive information cause security costs such as:

- A significant increase in the likelihood of an attack?
- A significant decrease in the difficulty of executing an attack?
- A significant increase in the damage caused by an attack?

If so, do the anticipated security costs 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 public health and safety 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 7 if you believe that the benefit of providing open access to the data outweighs the potential security costs, or to Step 8 if the security costs outweigh the value of providing open access.

Discussion: Originating organizations should make every effort to learn about the laws and regulations that affect dissemination of their data and should carefully consider the magnitude of the security risk incurred versus the benefits that accrue from the dissemination of any particular data. The benefits should be evaluated using quantitative and qualitative measures. Included among the societal benefits should be opportunity costs caused by the reduced availability of data resulting from safeguarding.

A great deal of our Nation's success can be attributed to its openness. Access to information has always been readily available to the American public and they recognize that some risk is acceptable. Many laws have been enacted that require public disclosure of seemingly sensitive information. However, some data can be misused with potentially disastrous consequences. Safeguarding of such data therefore warrants consideration.

Examples:

- Geospatial data for hazardous material facilities may be available to the public in response to "right to know" laws. Geospatial data that record the fact that one facility stores 50,000 pounds of a hazardous chemical while another stores only 20 pounds may help an adversary select as a target the facility that stores the larger amount. On the other hand, a citizen may be more concerned about living next to 50,000 pounds of the chemical than 20 pounds, and so the amount would be important information required to comply with "right to know" laws. Is it necessary to provide the detailed attribute information to comply with "right to know" legislation for such facilities, or does informing the public of the presence of the hazardous chemical, but not the quantity, provide sufficient information?
- Geospatial data may locate and identify operational procedures at facilities, floor plans showing precise storage locations, or information about the security measures for a facility. Does the public have the right to access the floor plan of a facility that shows the location and nature of its security systems or the exact storage areas for hazardous materials? Or should this information be restricted to the fire and law enforcement agencies that would respond in the event of an emergency?

Step 7 – 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. As noted in Step 3, the documentation should include the identification of the geospatial data, the potential security concerns, findings determined by use of the guidelines, the actions taken, and (if needed) the authority or case law that supports the actions taken. Appendix 2 identifies elements in the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in metadata.

Discussion: Safeguarding is justified only for data that contain sensitive information, that are the unique source of this sensitive information, and for which the security risk outweighs the societal benefit of dissemination. If you reach this step you have decided that your geospatial data fail one of these criteria and so safeguarding is not justified.

Section III: What safeguards are authorized and justified?

Overview: 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 access by a potential adversary. It also challenges the originating organization to be sure that it has the authority to undertake the planned safeguards.

Note that the need to safeguard data should be anticipated as early as possible in a project. In the case of projects undertaken by multiple participants, discussions and decisions should involve all participants. To ensure the effective safeguarding 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.

Step 8 – Would the public still be served, and the security risk be mitigated, by changing these data?

If you believe that the sensitive information in the geospatial data can be changed to minimize the security risk, and that the changed data still will have public value, go to Step 9. If the data cannot be changed to make the security risk acceptable, go to Step 11.

Discussion: The first type of safeguard is to change the geospatial data. You may find that the geospatial data contain sensitive information that needs to be safeguarded, but that by changing the data they would still useful and could be made publicly accessible.

This decision starts with your organization determining whether it has the authority to change the data. The idea of changing geospatial data includes redaction or removal of sensitive information and/or reducing the sensitivity of information by simplification, classification, aggregation, statistical summarization, or other information reduction methods.

Step 9 – Do you have the authority to change these data?

If the authority to change data exists go to Step 10. If such authority does not exist that course of action is closed and you go to Step 11.

Discussion: At this step, you must decide if your organization has the authority to change the data. Laws, regulations, policies, or concerns about liability may compel the organization to maintain and release data in its original (unchanged) state. Rarely do organizations have policies that instruct them to change data provided for public use. If you are unsure of your organization's authority or policy, seek a policy decision from appropriate executive managers or legal counsel in your organization.

Step 10 – Change these data.

Apply changes that remove or mitigate the security risk posed by the sensitive information. Such changes should be documented in the metadata. As noted in Step 3, the documentation should include the identification of the geospatial data, the potential security concerns, findings determined by use of the guidelines, the actions taken, and (if needed) the authority or case law that supports the actions taken. Appendix 2 identifies elements in the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in metadata.

When the changes are complete, ensure that the changes actually have mitigated the security risk by reviewing the changed data using the criteria in Section II beginning with Step 4. The changed data are cleared for dissemination when Step 7 is reached. Note that the originating organization must also safeguard the unchanged data if they are retained.

Discussion: At this point you have determined that your organization has the authority to change the data. Change the data and document the changes using the metadata. *Do not place disinformation in geospatial data.*

An originating organization that changes data should have written procedures and policies describing the types of changes allowed 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.

Examples: The following examples are provided for illustrative purposes only:

- Very high-resolution orthophotography (with pixels smaller than one foot, for example) may provide too much detail about air handling or security systems at a sensitive facility. Possible changes that would mitigate this concern include generalizing the data to a lower resolution, eliminating pixels, or applying an algorithm that reduces the sharpness of the image over the features of concern. Of course, visible differences in the image resulting from these changes may draw attention to the sensitive areas.
- Geospatial data for hazardous material storage facilities include detailed, current, and frequently updated information about the quantity of Class A poisons or explosives that could be used to harm the public, along with information on the names, home addresses, and telephone numbers of management and security personnel. Possible changes to the data include summarizing information about the quantities and removing data fields about personnel from the version of the geospatial data provided for open access.
- The point features in geospatial data provide precise coordinates that allow "discovery" and targeting of sensitive features. Possible modifications to the data include converting the point locations to polygons of random size and shape or reducing the precision of the points by systematic or random changes to the point locations.

Step 11 – Do you 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 (go to Step 12). If your organization has the authority to restrict data go to Step 13.

Discussion: The second, and last, type of safeguard is to restrict access to, uses of, and/or redistribution of the data. At this step, you must decide if your organization has the authority to restrict the data. Some organizations have laws, regulations, policies, or concerns about liability that compel them to release data. Others have clear authority to restrict data. If you are unsure of your organization's authority or policy, seek a policy decision from appropriate executive managers or legal counsel in your organization.

Step 12 – Will the appropriate decision maker give permission to restrict these data?

If the authorized executive manager and/or legal counsel grants permission to restrict the data go to Step 13. If not, go to Step 14.

Step 13 – 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. As noted in Step 3, the documentation should include the identification of the geospatial data, the potential security concerns, findings determined by use of the guidelines, the actions taken, and (if needed) the authority or case law that supports the actions taken. Appendix 2 identifies elements in the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in the metadata.

Discussion: At this point you have determined that your organization has the authority to place limits on access to geospatial data, uses for which they can be applied, or redistribution of the data. Decide the extent of restrictions and document them in the metadata.

Originating organizations that restrict data should have written procedures and policies that identify data that can be accessed, used, and/or redistributed, the conditions

under which these actions may occur, and organizations that are permitted to access, use and redistribute data that are restricted. Care should be taken to ensure that the release of the data to selected organizations does not enable other organizations to compel the release of the data under freedom of information or public records laws.

Such procedures and policies should be reviewed to ensure that they comply with available authorities. Restrictions should be commensurate with the security risk associated with the data. Organizations should identify present and potential users who have legitimate needs for the data. These may include first responders, law enforcement agencies, and emergency managers at the local, state, tribal, and Federal levels. Other organizations and research institutions may have legitimate reasons to use the data. Their requests should be granted if they provide proper safeguards and assurance that they will prevent unauthorized access to the data. Organizations that request sensitive data should ensure that they have the authority to honor the conditions under which they would receive the data.

For data that are released the originating organization should provide documentation to the recipient describing all obligations incurred by receipt of the data. These terms and conditions and any other obligations associated with possession of the geospatial data should be included in the metadata and/or in any licenses, agreements (including non-disclosure agreements), or other instruments that accompany the data. Such documentation also should cite the authority or other basis that permits the safeguards. Data that are safeguarded should be clearly labeled. Organizations could choose to follow up with recipients to ensure that safeguards are being observed.

Example: An organization may elect to establish one or more levels of restriction for geospatial data commensurate with the associated security risk, such as geospatial data being:

- Generally available to members of the public with use and redistribution restrictions. Recipients may be required to identify themselves before receiving the geospatial data.
- Available to other government agencies or non-governmental organizations (for example, the Red Cross), with use and redistribution restrictions.
- Available only to law enforcement, first responder, and emergency management agencies with use and redistribution restrictions.
- Available only to "partner" agencies from other levels of government with use and redistribution restrictions.
- Available only within your organization.

Step 14 – 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. As noted in Step 3, the documentation should include the identification of the geospatial data, the potential security concerns, findings determined by use of the guidelines, the actions taken, and (if needed) the authority or case law that supports the actions taken. Appendix 2 identifies elements in the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in the metadata.

Discussion: When an originating organization reaches this step, the authorized executive manager or legal counsel cannot give permission to safeguard data because no legal remedy exists or overruled the conclusion that the data require safeguarding.

Appendix 1: Sample Policies from Which Principles for the Guidelines Were Developed

The following list is a sample of policies from which the principles for the guidelines were developed. The list is not exhaustive. Attention was concentrated on policies that affect multiple organizations; individual organizations may have additional laws and other policies that control their actions.

Federal and State Laws

"An act to enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes (Brief title: "E-government Act of 2002")." (Public Law 107-347, 17 Dec 2002) (See especially Section 216, "Common Protocols for Geographic Information Systems"): U.S. Government Printing Office web site at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h2458enr.txt.pdf. (Accessed August 12, 2004)

"An act to establish the Department of Homeland Security, and for other purposes (Brief title: "Homeland Security Act of 2002")." (Public Law 107-296, 25 Nov 2002): U.S. Department of Homeland Security web site at http://www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf. (Accessed August 12, 2004)

"Depository Library Program," Title 44 U.S. Code, Chapter 19, 2000 ed.: U.S. Government Printing Office web site at http://www.access.gpo.gov/uscode/title44/chapter19_.html. (Accessed August 12, 2004)

"Emergency Planning and Community Right-to-Know," Title 42 U.S. Code, Chapter 116, 2000 ed.: U.S. Government Printing Office web site at http://www.access.gpo.gov/uscode/title42/chapter116_.html. (Accessed August 12, 2004)

"Hazardous Air Pollutants," Title 42 U.S. Code, Section 7412, 2000 ed.: Available through U.S. Government Printing Office web site at http://www.access.gpo.gov/uscode/title42/chapter85_subchapteri_parta_.html. (Accessed August 12, 2004)

"Records excepted from disclosure requirements; names and addresses; time limitations; destruction of records," Indiana Code 5-14-3-4, 2003 ed. (see especially section (a)(19)): Indiana General Assembly web site at http://www.in.gov/legislative/ic/code/title5/ar14/ch3.html. (Accessed August 12, 2004)

"Scientific Inventory of Oil and Gas Reserves," Title 42 U.S. Code, Section 6217, 2000 ed.: Available through U.S. Government Printing Office web site at http://www.access.gpo.gov/uscode/title42/chapter77_subchapteri_parta_.html. (Accessed August 12, 2004)

"Security of certain utility information," Maine Revised Statutes Title 35, Section 1311-B, 2003 ed.: Maine Office of the Revisor of Statutes web site at http://janus.state.me.us/legis/statutes/35-a/title35-asec1311-b.html. (Accessed August 12, 2004)

"Sensitive public security information," North Carolina General Statutes 132-1.7, 2003 ed.: North Carolina General Assembly web site http://www.ncleg.net/statutes/generalstatutes/html/bychapter/chapter_132.html. (Accessed August 12, 2004)

Policies, Hearings, and Correspondence

Ashcroft, John, "Memorandum on the Freedom of Information Act, October 12, 2001." U.S. Department of Justice web site at http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm. (Accessed August 12, 2004)

Card, Andrew. "Memorandum on Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security, March 19, 2002." U.S. Department of Justice web site at http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm. (Accessed August 12, 2004)

U.S. Department of Justice, "Freedom of Information Act Guide". Washington: May 2004. U.S. Department of Justice web site at http://www.usdoj.gov/oip/foi-act.htm. (Accessed August 12, 2004)

U.S. Executive Office of the President. "Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations" (Executive Order 12898). Washington: February 11, 1994. Available through National Archives and Records Administration web site at http://www.archives.gov/federal_register/executive_orders/1994.html. (Accessed August 12, 2004)

U.S. Executive Office of the President. "Coordinating Geographic Data Acquisition and Access: The National

Spatial Data Infrastructure" (Executive Order 12906). Washington: April 11, 1994. Available through National Archives and Records Administration web site at http://www.archives.gov/federal_register/executive_orders/1994.html. (Accessed August 12, 2004)

U.S. Executive Office of the President. "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten To Commit, Or Support Terrorism" (Executive Order 13224). Washington: September 23, 2001. U.S. Department of the Treasury web site at http://www.treasury.gov/offices/eotffc/ofac/sanctions/t11ter.pdf. (Accessed August 12, 2004)

U.S. Executive Office of the President. "Critical Infrastructure Protection in the Information Age" (Executive Order 13231). Washington: October 16, 2001. Available through National Archives and Records Administration web site at http://www.archives.gov/federal_register/executive_orders/2001_wbush.html. (Accessed August 12, 2004)

U.S. Executive Office of the President. "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information" (Executive Order 13292). Washington: March 25, 2003. Available through National Archives and Records Administration web site at http://www.archives.gov/federal_register/executive_orders/2003.html. (Accessed August 12, 2004)

U.S. Executive Office of the President. Office of Management and Budget. "Management of Federal Information Resources" (Circular A-130, transmittal memorandum #4). Washington: November 28, 2000: U.S. Office of Management and Budget web site at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html. (Accessed August 12, 2004)

U.S. Executive Office of the President. Office of Management and Budget. "Coordination of Geographic Information and Related Spatial Data Activities" (Circular A-16). Washington: August 19, 2002: U.S. Office of Management and Budget web site at http://www.whitehouse.gov/omb/circulars/a016/a016_rev.html. (Accessed August 12, 2004)

U.S. Government, 2003, U.S. Commercial Remote Sensing Policy: U.S. Geological Survey web site at http://crsp.usgs.gov/. (Accessed August 12, 2004)

U.S. House. Committee on Transportation and Infrastructure, Subcommittee on Water Resources and the Environment, "Terrorism: Are America's Water Resources and Environment at Risk?" Hearing, 10 Oct 2001. U.S. House web site at http://www.house.gov/transportation/water/10-10-01/10-10-01memo.html. (Accessed August 12, 2004)

U.S. House. Committee on Transportation and Infrastructure, Subcommittee on Water Resources and the Environment, "Right-to-Know after September 11th" Hearing, 8 Nov 2001. U.S. House web site at http://www.house.gov/transportation/water/11-08-01/11-08-01memo.html. (Accessed August 12, 2004)

Appendix 2: Documenting Use of the Guidelines in Metadata Accompanying Geospatial Data

This appendix identifies data elements in the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in the metadata.

Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (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.

Provide an overview of the potential security concerns, the decisions made, the date of the decisions, and the safeguards applied using "Abstract" (element 1.2.1). Use "Supplemental Information" (element 1.2.3) to provide details about these activities. The text should document, or at least characterize, the potential security concerns, findings determined by use of the guidelines, the actions taken, the date of the decisions, and (if needed) the authority or case law that supports the actions taken. If safeguards are justified, describe them by documenting the types of changes made to the geospatial data and/or any restrictions on access, use, or dissemination. Describe any license, agreement, or other instrument that accompanies the data. Such documentation should also cite the authority for safeguarding.

To document changes made to the data, the best choices are elements available under "Data Quality Information" (element 2), which has available elements for reporting attribute accuracy, positional accuracy, logical consistency, completeness, and lineage. Report processes used to change the data under "Process Step" (element 2.5.2). If you decide not to use element 2, a less-preferred choice is to include information about changes in "Supplemental Information" (element 1.2.3).

To document the details about restrictions on access, use, or dissemination of the data:

- Report restrictions on access to the geospatial data under "Access Constraints" (element 1.7).
- Report restrictions on use or redistribution of the geospatial data under "Use Constraints" (element 1.8).

If your organization has a formal classification system you also can report the classification level of the geospatial data by category under "Security Information" (element 1.12).

Geospatial metadata can also be subject to safeguarding. To document the details of restrictions on access, use, or dissemination of the metadata:

- Report restrictions on access to the geospatial metadata under "Metadata Access Constraints" (element 7.8).
- Report restrictions on use or distribution of the geospatial metadata under "Metadata Use Constraints" (element 7.9)

If your organization has a formal classification system you also can report the classification level of metadata by category under "Metadata Security Information" (element 7.10).

References

Baker, John; Lachman, Beth; Frelinger, David; O'Connell, Kevin; Hou, Alexander; Tseng, Michael; Orletsky, David; and Yost, Charles, 2004, Mapping the risks: assessing the homeland security implications of publicly available geospatial information: Santa Monica, Ca., RAND Corporation, 195 p. (Also available through the RAND Corporation web site at http://www.rand.org/publications/MG/MG142/) (Accessed August 12, 2004)

Federal Geographic Data Committee, 1998, Content standard for digital geospatial metadata (FGDC-STD-001-1998): Reston, Va, Federal Geographic Data Committee, 78 p. (Also available through the Federal Geographic Data Committee web site at http://www.fgdc.gov/metadata/contstan.html) (Accessed August 12, 2004)

National Academy of Public Administration, 1998, Geographic information for the 21st century: building a strategy for the nation: Washington, National Academy of Public Administration, 358 p.

National States Geographic Information Council, 2002, Data access decision tree: National States Geographic Information Council web site at http://www.nsgic.org/hot_topics/security/080702_HS_Decision_Tree_CI_Data _Version7.ppt (Accessed August 12, 2004)

The following is the recommended bibliographic citation for the guidelines:

> Federal Geographic Data Committee. Homeland Security Working Group. "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns". Washington: June 2005, 16 p. Available through Federal Geographic Data Committee web site at http://www.fgdc.gov/fgdc/homeland/index.html.

Figure 1. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

(Duplicate graphic that can be detached and used separately.)