May 3, 2004

Instructions to Reviewers of "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns"

The Homeland Security Working Group of the Federal Geographic Data Committee invites your comments on the attached "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns".

You may provide comments:

- By electronic mail to guidelines@fgdc.gov. Please provide comments in the body of the electronic mail message, or as an attachment to the message in either Microsoft Word format or Rich Text Format.
- By regular or overnight mail to FGDC HSWG Guidelines Review, 511 National Center, 12201 Sunrise Valley Drive, Reston, Virginia 20192. Please send one paper copy of the comments and a digital copy on 3.5-inch diskette in Microsoft Word format or Rich Text Format.

All comments concerning these proposed guidelines must be received on or before June 2, 2004.

Suggestions to Reviewers

The working group seeks comments on those aspects of the guidelines that are useful, need improvement, or should be reconsidered. Ideas about approaches that will encourage the adoption and use of the guidelines also are invited.

The following suggestions are offered to help ensure that we understand your main points:

- Organization of comments: Organize your comments in the order in which the topics occur in the guidelines and use the headings formatted with **bold text** in the guidelines to identify the topics to which your comments apply. This approach ensures that we will understand the topics in the guidelines to which your comments apply.
- Types of comments: We invite you to identify:
  - Items that are useful: Often when people comment on a document, they focus only on the items they think should be changed. This approach leaves open the possibility that other people's comments may result in changes to an item you thought was a good idea. Please help us by identifying those items you support.
  - Items that need improvement: For items for which the guidelines have a useful idea, but take the idea too far, not far enough, or in the wrong direction, please identify the item, your concern, and your thoughts of how the item can be improved.
  - Items that need to be reconsidered: For items you think are in error, please identify the item, your concern, and why you believe the item is an error. Please provide your thoughts about other ways to consider the item.
  - Items missed: We invite new items that could strengthen the guidelines.

- Implementation ideas: We invite ideas for encouraging the adoption and use of the guidelines.

- Additional materials: If needed to help explain your comments, please feel free to include other materials with your comments. If the materials are available through the Internet, consider only providing the web address to the materials.

- Classified, sensitive, or information otherwise restricted: Please DO NOT send information or materials you consider to be classified, sensitive, confidential, proprietary, subject to privacy concerns, or otherwise restricted.

- Tell us about you: Please include your name, title, organization, mailing address, electronic mail address, and telephone number. We will use this information to identify sources of comments, and to contact you if we do not understand your comments or need more information. If you are responding on behalf of a group, please identify the group. Please also consider providing information about how the guidelines will affect your activities so that we better understand the context for your comments.

What the Working Group Will Do with the Comments

The working group will use the comments to improve the guidelines and to plan ways to encourage their adoption. We may share the comments with other organizations and individuals as part of these activities.

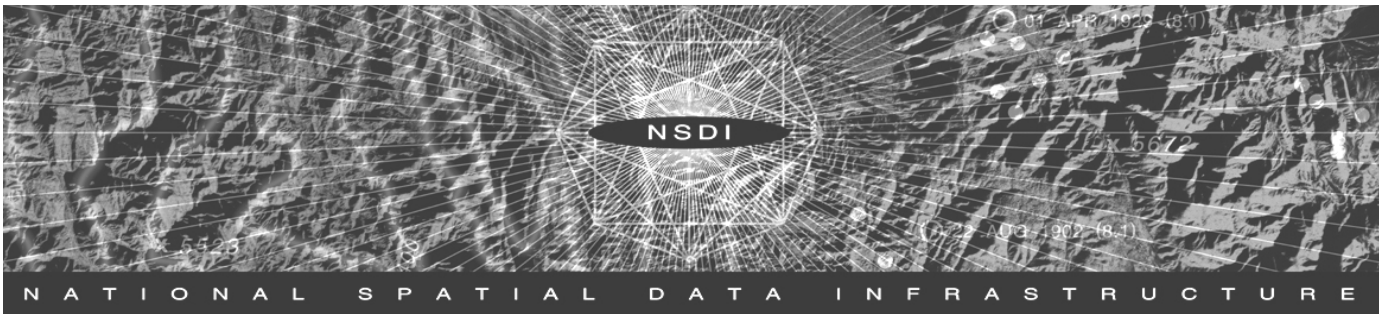
We will summarize major or recurring themes from the comments and the working group's responses, and post the information through the working group's home page at http://www.fgdc.gov/fgdc/homeland/index.html

What Will Happen to the Guidelines after the Comment Period?

The revised guidelines will be submitted to the Steering Committee of the Federal Geographic Data Committee for adoption.

Thank You for Your Help

Thank you in advance for your comments and suggestions. With your help, we can ensure that the guidelines will support interagency coordination and the implementation of the National Spatial Data Infrastructure through appropriate access to sensitive geospatial data and maintaining public access to data that are not sensitive.



Public Review Version **May 3, 2004**

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 distribute geospatial data. The vast majority of these data are appropriate for public dissemination and dissemination is essential to the purpose of many organizations. However, a small portion of these data could pose risks to security and may therefore require additional safeguards. Although there is not much publicly-available information that is sensitive, managers of geospatial information at federal, state, and local levels have restricted access to information using different criteria.

The guidelines provide procedures to:

1. Identify sensitive information content of geospatial data sets that pose a risk to security.
2. Review decisions about sensitive information content during reassessments of restrictions on geospatial data sets.

Additionally, the guidelines provide a method for balancing security costs and the benefits of dissemination. If protection is warranted, the guidelines help organizations select appropriate risk-based restrictions that provide access to data sets and still protect sensitive information content.

The guidelines are to be carried out within authorities available to organizations; they do not grant any new authority.

How are the guidelines organized?

The guidelines are organized as a series of decisions (see Figure 1) that an originating organization makes about a data set. Each decision is accompanied by related instructions and discussion.

The decisions are organized using the following rationale:

I. Do the data originate in the organization? If not, the organization is instructed to follow the guidance it received with the data set.

II. Organize documentation on your use of the guidelines, including the identification of the data set, the potential concern, findings determined by use of the guidelines, the action to be taken, and (if needed) the authority for taking the action.

III. If the data originate in the organization, do the data warrant restriction? 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 pose a risk to security, is the sensitive information unique to the data set?
- Net benefit of disseminating data: If the sensitive information poses a risk to security and is unique to the data set, do the security costs of disseminating the data outweigh the associated societal benefits of dissemination?

Data that do not pose a risk or are not unique, or for which dissemination is a net benefit, do not warrant restriction so no additional consideration is necessary.

IV. If the data warrant restriction, what restrictions are warranted? The guidelines offer two options:

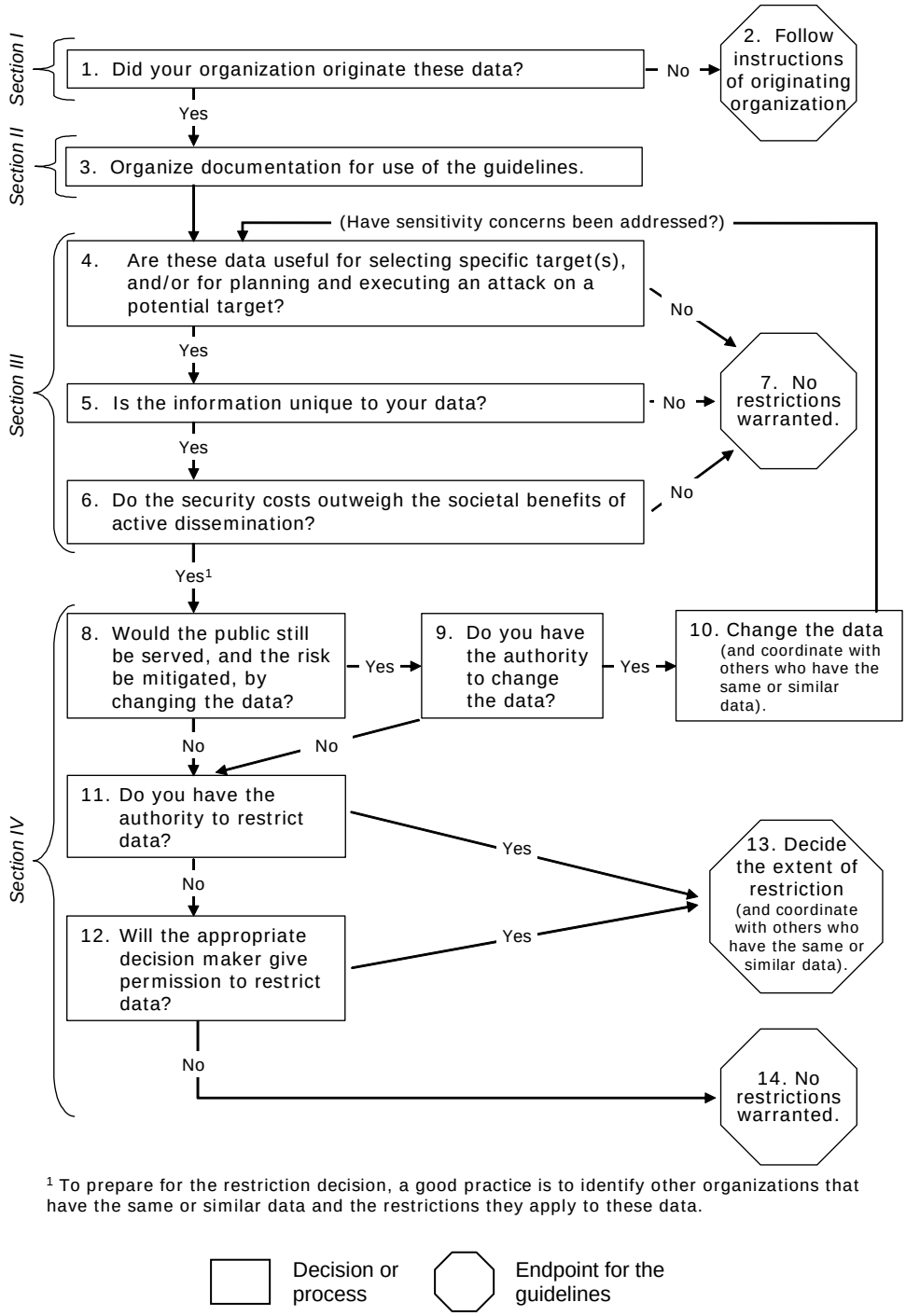
- Change the data: Change the data to remove or modify the information that causes concern, and make the changed data available without further restrictions. Organizations are advised to review

the changed data to ensure that the change dealt effectively with the concern.

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

In both cases, organizations are advised to ensure that they have the authority to restrict the data. If they do not have the authority, they might seek it from an appropriate decision maker. The decision maker can provide the authority to restrict the data or can overrule the conclusion that the data are sensitive.

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



[1] To prepare for the restriction decision, a good practice is to identify other organizations that have the same or similar data and the restrictions they apply to these data.

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, aid our international competitiveness, support a large array of Federal, state, and local government activities, and serve the general public.

Many public, private, and non-profit organizations originate and publicly distribute geospatial data sets. While the vast majority of these data are appropriate for public dissemination, a small portion of these data could pose a risk to security and may require additional safeguarding.

Although there is not much publicly-available geospatial information that is sensitive, federal, state, and local levels have restricted access to information based on differing criteria to identify sensitive data. Some organizations 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.

Guidelines for identifying sensitive data, determining risks associated with them, and assessing their benefits help the geospatial data community in several ways. Use of guidelines can frame discussions about the importance of making data publicly accessible and encourage the development of consensus decisions in the community. Because contradictory decisions and actions by different organizations can easily negate each organization's action, a common, standardized approach to identify data sets that have sensitive content and to appropriately safeguard such information will increase the effectiveness of an individual organization's actions and not unduly restrict public access.

The guidelines help organizations decide on reasonable access to sensitive data and avoid unnecessary restrictions. They do so by helping organizations identify content that might pose a risk to security. They then guide organizations to 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 restricting data.

On what premises are the guidelines based?

The guidelines strike a balance among these principles:

- Appropriately safeguard information that could potentially be used to inflict significant harmful consequences to public safety or security of property.
- Encourage the free flow of information between the government and public to enable both informed public participation in decision making and private reuse of government information.
- Recognize that geospatial data sets often have value to organizations other than the organization that originates the data, and that 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.
- Enable the continued 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 were 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. The appendix 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" (RAND Report MG-142 NGA 2004) were considered in developing the guidelines. Work by the National States Geographic Information Council 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 making the data

publicly accessible, but are concerned that such actions might pose a risk to security. In the United States, a large number of public, private, and non-profit 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 decisions about the sensitivity and restriction of data will be decentralized.

The guidelines acknowledge, however, circumstances for which originating organizations should consult with other organizations, such as those that hold similar data, to ensure that any protective measures are effective or to better understand any conflicting assessment of risk.

In cases when the severity of the potential consequences of releasing a geospatial data set is uncertain, originating organizations should seek advice from others including legal counsel, security organizations, and facility operators. Competent law enforcement, emergency management, and homeland security agencies are sources of advice on the likelihood of an attack scenario and the potential consequences of such an event. The detailed knowledge that operators have for their facilities also may be helpful. Remember, however, that such advice may tend to overestimate the security risks posed by a geospatial data set and is unlikely to include consideration of the broad range of alternate information sources available from the geospatial and other communities. For that reason, 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. The responsibility for making decisions rests with the originating organization, not its advisors.

Assessments of risks and costs must also be balanced with a full understanding of the benefits of active dissemination. Originating organizations should seek advice from the primary or potential (if information is not disseminated currently) users regarding the benefits of the information. Keep in mind that benefits are often highly decentralized, and benefits to secondary users can be greater than those to primary users. Secondary users receive data directly from originating organizations or primary users or indirectly through other intermediaries.

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" a data set (see Steps 8 through 10) includes removing sensitive information and reducing the sensitivity by generalizing the data (reducing the granularity of information).

data set – a collection of related data, including secondary or ancillary data, software, and documentation, that completely document and support the use of those data.

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.

open-source information – publicly-available information (that is, any member of the public could lawfully obtain the information 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 might or might 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.

originating organization – an organization that develops or sponsors the development of a data set.

redact – to prepare for publication or presentation by correcting, revising, or adapting.

What concerns are not addressed by the guidelines?

Internal procedures for protecting data: The guidelines assume that organizations 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 to restrict 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 a data set and the restrictions that are appropriate for it will inevitably change over time. Reasons include better understanding of security risks, changes in the value of data sets 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 a data set affects not only the originating organization, but also "downstream" organizations.

Decisions about the sensitivity of derived data sets: Data derived from other 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 originate derived data should contact originators of sensitive source data to determine whether the sensitivity applies to the derived data.

Appeals of an originating organization's decisions: Organizations 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 the implementation of 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 superceded or withdrawn by the Federal Geographic Data Committee.

Guidelines

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

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

Section I: Is the decision to restrict data yours to make?

Step 1 – Did your organization originate these data?

If the answer to the question is no, then your organization should not make decisions about restricting the data. Move to Step 2. If the answer is yes, move to Step 3.

Discussion: If your organization did not originate the data set in question, you should not apply the guidelines. Instead, you should honor any restrictions that accompanied the data.

Step 2 – Follow instructions of originating organization.

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

Discussion: Users are responsible for knowing and honoring restrictions that accompany the data. The originating organization should document all restrictions in the metadata and/or in any license, agreement, or other instrument that accompanies the data.

Section II: Organize documentation.

Overview: If you reach this section, you are the originating organization for the data set.

Step 3 – Organize documentation for use of the guidelines.

Document your use of the guidelines, including the identification of the data set, the potential concern, findings determined by use of the guidelines, the action taken, and (if needed) the authority or case law that supports the action taken. When prepared, proceed 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, to recall their reasoning when reviewing a decision, and to explain a decision if challenged.

Section III: Are restrictions warranted?

Overview: This section provides guidelines to decide if the data set warrants restriction.

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 (recent or real-time) 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 no restrictions are warranted for the data. Move to Step 7. If the answer to either part is yes, then move to Step 5.

Discussion: In general, this step performs a "user needs assessment" in which the "user" is an adversary. In this step, 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?

Generally, sensitive information does not include the fact of the 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 data include information about the relative importance of a feature to a larger system, the timing of activities, communication capabilities, detailed business and industrial processes, previously identified vulnerabilities, measures and plans for securing and protecting facilities, and measures and plans for responding to attacks or damage. In many cases, attribute data are more likely to be sensitive than are geospatial data.

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 other information available, relatively low cost or low accuracy 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 your data?

In particular is the sensitive information about the feature:

- 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 clearly is available from open sources the data set under evaluation does not warrant restriction. Move to Step 7. If the data set under evaluation provides unique information that cannot be obtained from other open sources, then move to Step 6.

Discussion: If you originate data that appear to be sensitive based on the evaluation in Step 4, you should carefully consider whether the information provided by the data is readily available from other open sources.

Remember that the goal is to identify information that is unique, not just data that are unique. Your data set might be the only "geospatial" source of a unit of information, but other publications and media might 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, and imagery collected during the previous thirty years.

Examples:

- A data file that shows the location of high-voltage overhead electric transmission lines might be considered sensitive upon initial evaluation. However, experts generally agree that adversaries visit their intended targets in person and they would, therefore, be easily able to observe the locations of these lines.
- A state or local government might 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 and they can be easily found by looking them up in telephone directories or by driving past the site.

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

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 dissemination such as:

- Business or personal productivity resulting from continued or increasing applications of geospatial data?
- Continued or increasing effectiveness of public 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, move 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 that affect distribution of their data and should carefully consider the magnitude of the risk incurred versus the benefits that accrue from the release 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 the restrictions on the data.

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, data can be misused with potentially disastrous consequences. Restriction of such data therefore warrants consideration.

Examples:

- A data set for hazardous material facilities might be available to the public in response to "right to know" laws. A data set that records the fact that one facility stores 50,000 pounds of a hazardous chemical while another stores only 20 pounds might 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?
- A data set might 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 – No restrictions warranted.

When you reach this step, your use of the guidelines is complete. Retain documentation of the decision for future use.

Section IV: What restrictions are warranted?

Overview: If you reach this section, you have concluded that public access to your data set in its present form should be restricted.

This section provides guidance on choices for restricting data from unwarranted access. It encourages maximum possible access to data, and so emphasizes use of the minimum restriction required to prevent access by an adversary. It also challenges the originating organization to be sure that it has the authority to impose the planned restriction.

Note that the need to restrict data should be anticipated as early as possible in a project. To ensure effectiveness, it may be prudent to implement restrictions before an originating organization formally takes possession of a data set, to protect field-collected information, to ensure the security of data while contractors are developing them, and to take other steps to restrict access to data while they are being developed.

The originating organization should document all restrictions in the metadata and/or in any license, agreement, or other instrument that accompanies the data. Such instructions also should include the authority or other basis for the restriction.

Decisions to restrict data are only effective when all parties that have the same or similar data choose the same

action. In the case of projects undertaken by multiple participants, such decisions should be reached early in the project. In the case of organizations that originate similar data through independent actions, consultation among the organizations about restrictions would increase the effectiveness of a restriction action.

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

If you believe that the sensitive characteristics of the data set can be changed to minimize the security risk, and that the changed data still will have public value, move to Step 9. If the data cannot be changed to make the security risks acceptable, move to Step 11.

Discussion: You might find that parts of a data set warrant restriction, but the remainder would be useful and could be made publicly accessible.

The idea of changing, or redacting, a data set includes removing sensitive information and/or reducing the sensitivity of information by simplification, classification, aggregation, statistical summarization, or other information reduction methods.

Do not place disinformation in a data set.

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

- Very high-resolution orthophotography (with pixels smaller than one foot, for example) might provide too much detail of 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 might draw attention to the area.
- A data set of hazardous material storage facilities includes 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 data set provided for open access.
- The point features in a data set 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 9 – Do you have the authority to change the data?

If the authority to change data exists, move to Step 10. If the authority does not exist this course of action is closed; move 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 might compel the organization to maintain and release data in its original (unchanged) state. Rarely do organizations have policies that instruct them to change data that are 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 the data (and coordinate the decision with others who have the same or similar data).

When the changes are complete, the guidelines direct you to review the changed data using the steps in Section III. The changed data are cleared for public access when Step 7 is reached. The originating organization also must protect the unchanged data if they are retained.

Discussion: At this point, you have determined that your organization has the authority to change the 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 any license, agreement, or other instrument that accompanies the data. Such documentation should identify the authority or other basis that permit it to change the data.

Step 11 – Do you have the authority to restrict data?

If the authority to restrict 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 authority to restrict data, go to Step 13.

Discussion: The second, and last, type of restriction is to restrict access to, uses of, and/or redistribution of data.

This decision starts with your organization determining if it 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.

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

If the authorized executive manager and/or legal counsel agree to restrict the data and grant permission to do so, go to Step 13. If they do not agree, go to Step 14.

Step 13 – Decide the extent of restriction (and coordinate the decision with others who have the same or similar data).

The originating organization decides the conditions under which the data set can be released, if any. When you complete this step, your use of the guidelines is complete. Retain documentation of the decision for future use.

Discussion: Originating organizations that restrict data should have written procedures and policies that identify data that can be released, the conditions under which they can be released, and organizations to which they can be released. Such procedures and policies should be reviewed to ensure that they comply with available authorities. Restrictions should be commensurate with the sensitivity of the data.

When developing these procedures, organizations should identify others who have legitimate needs to access the data. These might include first responders, law enforcement agencies, and emergency managers at the local, state, and Federal levels. Other organizations and research institutions may have legitimate reasons to use the data and 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. Types of restrictions might include limits on access to a data set, uses for which a data set can be applied, and redistribution of a data set. These terms and conditions and any other obligations associated with the possession of the data set should be included in the metadata and/or in any license, agreement, or other instrument that accompanies the data. Such documentation also should cite the authority or other basis that permit the restriction. Restricted data should be clearly labeled. Organizations could choose to follow up with recipients to ensure that restrictions are being observed.

Example: An organization might combine restrictions to establish levels of restriction, such as a data set being:

- Generally available to members of the public with use and redistribution restrictions. Recipients might be required to identify themselves before receiving the data set.
- Available to other government agencies or non-profit 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.

The review of such a procedure would include ensuring that the release of data to selected organizations would not enable other organizations to request the data under freedom of information or public records laws.

Step 14 – No restrictions warranted.

When you reach this step, your use of the guidelines is complete. Retain documentation of the decision for future use.

Discussion: When an originating organization reaches this step, the authorized executive manager or legal counsel has decided not to give permission to restrict data.

Appendix

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 might have additional laws and other policies that control their actions.

Ashcroft, John, Attorney General, "The Freedom of Information Act": http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm

Card, Andrew, Assistant to the President and Chief of Staff, "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security": http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm

Department of Justice, "Freedom of Information Act Guide, May 2002": http://www.usdoj.gov/oip/foi-act.htm

Executive Order 12898, "Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations": http://www.archives.gov/federal_register/executive_orders/pdf/12898.pdf

Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure": http://www.fgdc.gov/publications/documents/geninfo/execord.html

Executive Order 12958, "Classified National Security Information": http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1995_register&docid=fr20ap95-135.pdf

Executive Order 13224, "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten To Commit, Or Support Terrorism": http://www.treasury.gov/offices/eotffc/ofac/sanctions/t11ter.pdf

Executive Order 13231, "Critical Infrastructure Protection in the Information Age": http://www.ciao.gov/News/EOonCriticalInfrastrutureProtection101601.html

House Subcommittee on Water Resources and the Environment, "Hearing on Terrorism: Are America's Water Resources and Environment at Risk?": http://www.house.gov/transportation/water/10-10-01/10-10-01memo.html

House Subcommittee on Water Resources and the Environment, "Hearing on Right-to-Know after September 11th": http://www.house.gov/transportation/water/11-08-01/11-08-01memo.html

"Homeland Security Act of 2002": http://thomas.loc.gov/cgi-bin/query/D?c107:6:./temp/~c107ud6JmH::

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

Maine Statutes, Title 35, Chapter 13, Section 1311-B, "Security of certain utility information": http://janus.state.me.us/legis/statutes/35-a/title35-asec1311-b.html

North Carolina General Statutes, Chapter 132, Section 1.7, "Sensitive public security information": http://www.ncleg.net/statutes/generalstatutes/html/bychapter/chapter_132.html

Office of Management and Budget Circular A-16, "Coordination of Geographic Information and Related Spatial Data Activities": http://www.whitehouse.gov/omb/circulars/a016/a016_rev.html

Office of Management and Budget Circular A-130, "Management of Federal Information Resources": http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

U.S. Code, Title 42, Chapter 116, "Emergency Planning and Community Right-to-Know": http://www.access.gpo.gov/uscode/title42/chapter116_.html

U.S. Code, Title 42, Chapter 85, Section 7412, "Hazardous Air Pollutants": http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC7412

U.S. Code, Title 43, Chapter 77, Section 6217, "Scientific Inventory of Oil and Gas Reserves": http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=632101424153+0+0+0&WAISaction=retrieve

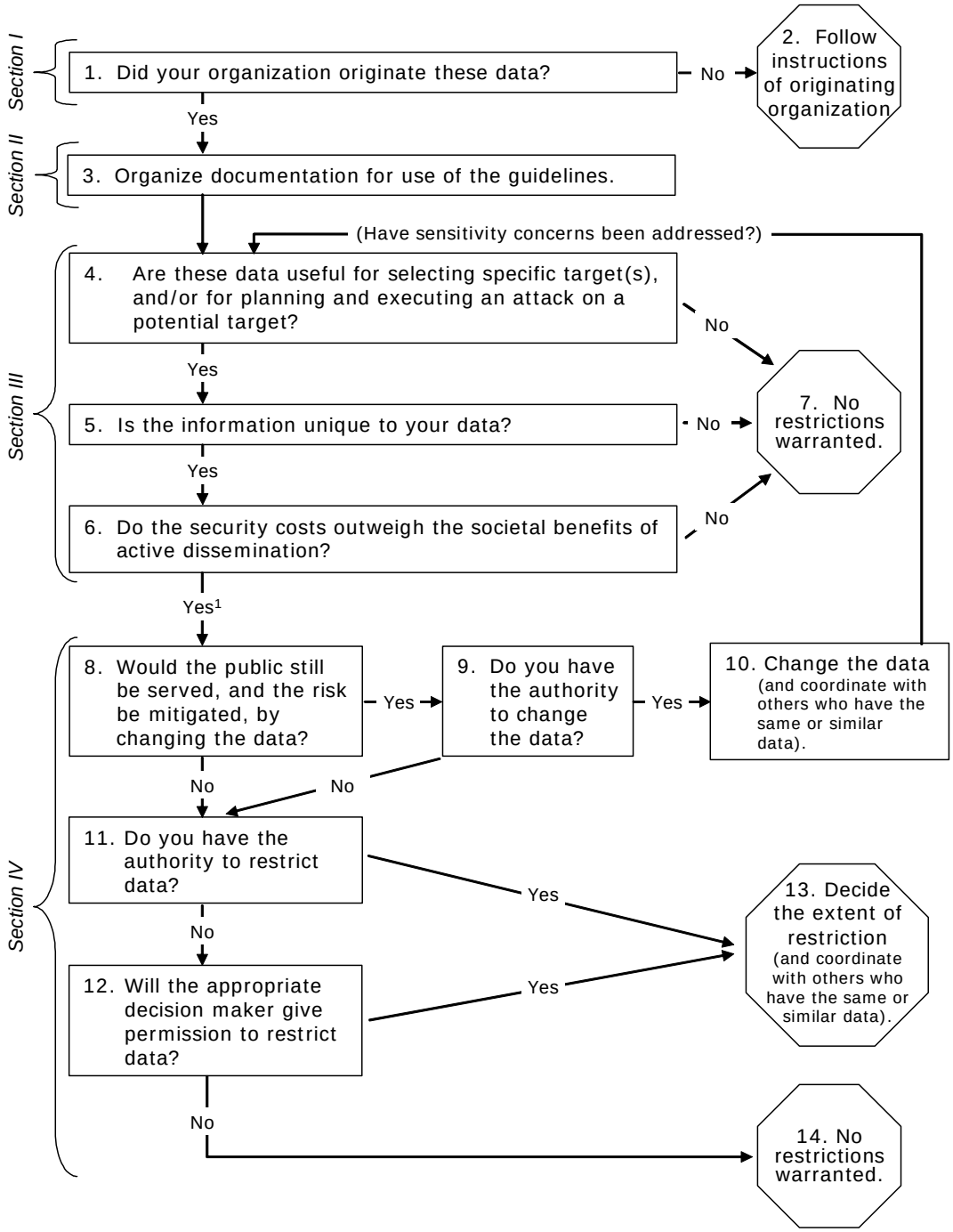
U.S. Code, Title 44, Chapter 19, "Depository Library Program": http://www.access.gpo.gov/uscode/title44/chapter19_.html

U.S. Code, Title 44, Chapter 36: "E-Government Act of 2002" (see especially section 216, "Common Protocols for Geographic Information Systems"): http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h2458enr.txt.pdf

U.S. Commercial Remote Sensing Policy: http://crsp.usgs.gov/

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.)



[1] To prepare for the restriction decision, a good practice is to identify other organizations that have the same or similar data and the restrictions they apply to these data.