Champaign County GIS Consortium (CCGISC)

DIGITAL DATA POLICY

All digital data policies shall be governed by and consistent with the Intergovernmental Agreement Providing for the Creation of the Champaign County Geographic Information System Consortium (IGA), as amended.

The Champaign County GIS Consortium (CCGISC) groups digital data into four (4) general categories – Custodial, Repository, Production, and Hosted. All digital data, regardless of category, is stored on CCGISC servers. The data is regularly backed-up and pushed off site by the County Information Technology (IT) department.

1. CUSTODIAL DATA

a. Custodial Data shall be defined as data CCGISC creates, maintains, and distributes using accepted CCGISC standards and practices.

b. Custodial Data includes all data listed on the Digital Data Category List *(Appendix A)* under the column heading "Custodial Data".

c. The list of Custodial Data shall be maintained by the CCGISC staff. Changes to the list shall be periodically reviewed and approved by the CCGISC Policy Committee.

2. REPOSITORY DATA

a. Repository Data shall be defined as data created and maintained from external sources that CCGISC distributes to member agencies using accepted CCGISC standards and practices.

b. Repository Data includes all data listed on the Digital Data Category List *(Appendix A)* under the heading "Repository Data".

c. The list of Repository Data shall be maintained by the CCGISC staff. Changes to the list shall be periodically reviewed and approved by the CCGISC Policy Committee.

d. Repository Data shall only be distributed to non-members upon a written request from the originating agency to the CCGISC Director.

3. PRODUCTION DATA

a. Production Data shall be defined as data CCGISC creates and maintains using accepted CCGISC standards and practices but does **not** directly distribute. Production Data is the source data used to create Custodial Data.

b. Production Data includes all data listed on the Digital Data Category List (Appendix A) under the heading "Production Data".

4. HOSTED DATA

a. Hosted Data shall be defined as data CCGISC hosts on its servers for member or non-member agencies per a contractual agreement.

b. Ownership of Hosted Data resides with the contracted agency; distribution to others is limited to contractual stipulations.

c. Hosted Data includes all data listed on the Digital Data Category List (Appendix A) under the heading "Hosted Data".

5. MEMBER AGENT

a. A member agency consultant shall be considered a "Member Agent" when the criteria as listed below are met.

   i. An active legally binding contractual agreement exists between the CCGISC member agency and the third-party consultant.

   ii. An active Intergovernmental Agreement for Services exists between CCGISC and the CCGISC member agency.

   iii. An active Memorandum of Understanding exists between CCGISC and the third-party consultant.

6. DATA VERIFICATION RESPONSIBILITY

a. Questions pertaining to the accuracy of custodial or repository data shall be directed to the entity that is identified by name in the "Verification Responsibility" column heading of Appendix A. For repository data, verification responsibility shall be the entity that responsible for the creation of the data. For custodial data, verification responsibility shall be the entity that is initially directed all questions related to data accuracy and creation.

7. DATA DISTRIBUTION OR DISCLOSURE TO CONSORTIUM MEMBERS

a. Custodial and repository data shall be made available at no cost to the CCGISC members.

b. Custodial data shall be made available to University of Illinois at Urbana-Champaign faculty, staff, and students through the University of Illinois's Webstore upon the acceptance of the University of Illinois Click-through Data Release Agreement found at Appendix B.

c. Data access and availability shall meet accepted CCGISC standards and practices.

d. Upon termination from the CCGISC and pursuant to the terms and conditions of the IGA a complete copy of custodial data will be provided to the terminating member. All rights of ownership for the provided data shall remain with the CCGISC and membership rights, including the right to redistribute the data, are forfeited upon termination.

8. DATA DISTRIBUTION OR DISCLOSURE TO MEMBER AGENTS

a. Custodial data shall be made available at no cost to the Member Agent per the CCGISC Rules of Engagement at Appendix L.

b. Data access and availability shall meet accepted CCGISC standards and practices.

c. Access to CCGISC data shall be terminated by the Member Agency and/or CCGISC once a third-party consultant no longer serves as a Member Agent.

d. The Consortium Director may temporarily modify, restrict, or suspend a Member Agent's data access at any time, at the sole discretion of the Consortium Director, as necessary to preserve the security and integrity of CCGISC data and infrastructure. In the event of any such action, the Consortium Director shall advise the Member Agent and the member agency as soon as feasible as to the basis for said action and any steps necessary to resolve the issue. The Consortium Director shall then inform the Policy Committee, no later than the next regularly scheduled Policy Committee meeting, of the basis for said action and any steps taken or still necessary to resolve the issue.

9. DATA DISTRIBUTION OR DISCLOSURE TO NON-MEMBERS, INCLUDING POLICIES TO PROTECT THE PRIVACY OF INDIVIDUALS

a. CCGISC custodial data shall be made available at no cost to non-members only 1) under specific agreement approved by the GIS Policy Committee or 2) pursuant to the execution of the Digital Data Release Agreement for ***Consultants*** found at Appendix C. A Digital Data Release Agreement must be initiated and approved by a CCGISC member and shall be prepared and processed by the CCGISC staff only. Additional data may be requested and provided under a previously executed Digital Data Release Agreement if the data being requested is for use with a project as described on an existing Digital Data Release Agreement.

b. Custodial data may be made available at cost to non-members in accordance with Section 8 only upon execution of an appropriate Digital Data License Agreement - the ***standard*** digital data license agreement found at Appendix D or the digital data license agreement for ***derived products*** found at Appendix E. All Digital Data License Agreements shall be prepared and processed by the CCGISC staff only. All requests by non-members to purchase CCGISC data shall be forwarded to a CCGISC staff member.

c. Records of data disclosure to non-members shall be maintained by the CCGISC staff. These records are available for internal review only by the CCGISC and may be released to local law enforcement officials upon their written request, or as otherwise required by law.

d. All data disclosures to non-members shall protect the privacy of individuals consistent with the Intergovernmental Agreement Providing for the Creation of the Champaign County Geographic Information System Consortium.

10. DATA SALES

a. Data may be available for purchase only upon approval of the CCGISC Policy Committee. Only data for which a cost has been determined and approved by the CCGISC Policy Committee shall be available to purchase.

b. A data order form and price list *(Appendix F)* shall be maintained by the CCGISC staff. The list shall be reviewed and approved by the CCGISC Policy Committee. A copy of the list shall be available at no charge to any member agency or member of the public.

c. Records of all data purchases shall be maintained by the CCGISC staff. These records are available for internal review only by the CCGISC and may be released to local law enforcement officials upon their written request, or as otherwise required by law.

d. Prior to the release of data, all data purchases shall require 1) a completed Digital Data License Agreement that is approved by CCGISC staff and 2) full payment to CCGISC staff. CCGISC staff may determine, at its discretion, to release data with a corresponding invoice prior to the receipt of payment only to local customers that have

previously demonstrated a consistent record of providing full payment in a timely manner.

11. DATA LICENSING

a. All data sold through the CCGISC shall be accompanied by a Digital Data License Agreement.

b. All Digital Data License Agreements shall contain provisions which are designed to protect the CCGISC and its members through clear limitation of liability, as well as provisions which state that there is warranty of the provided data for any purpose, protect of property rights, and include remedies for violations of the Digital Data License Agreements.

c. It shall be standard practice for Digital Data License Agreements to contain provisions that restrict the reproduction or redistribution of products derived from CCGISC data purchases outside of the Licensee's organization without permission of the CCGISC. Permission which allows for the reproduction and redistribution of CCGISC data through a derived product may be provided to the Licensee, at the discretion of the CCGISC Director, only upon execution of the Digital Data License Agreement for derived products (Appendix E).

d. A Digital Data License Agreement shall be required for each unique data purchase unless the purchasing entity has current Agency Digital Data License Agreement (Appendix G) on file.

e. An Agency Digital Data License Agreement may be entered into by CCGISC and local agencies who request multiple data purchases during a calendar year. Agency licenses shall be valid for one calendar year. For Agencies holding a valid agency license, the requirement to provide a completed license agreement with each unique purchase shall be waived.

12. FREEDOM OF INFORMATION REQUESTS

a. All Freedom of Information Requests for GIS data shall be addressed in accordance with the opinion of the Champaign County State's Attorney (Appendix H), as may be supplemented by further legal advice specific to each request.

b. Freedom of Information Requests for repository data will be referred to the agency from which the requested data originated. Freedom of Information Requests for hosted data will be referred to the agency that retains data ownership.

13. DATA SECURITY

a. The CCGISC Director in conjunction with any CCGISC member may determine that the distribution of custodial data to a non-member poses a security risk. This determination shall be made utilizing the FGDC guidelines found at Appendix I and shall be identified with the name of the member agency/agencies responsible for classifying the data as a security risk in the "Security Risk" column heading of Appendix A. Should the CCGISC member(s) and the CCGISC Director be unable to agree, the determination to classify data as a security risk will be made by a majority vote of the CCGISC Policy Committee. Security risk data will not be available for purchase from the CCGISC. CCGISC may provide security risk data to a non-member through a Digital Data Release Agreement only upon written agreement from the agency or agencies responsible for classifying the data as a security risk.

b. Any data classified as a security risk by the University of Illinois will not be supplied to University of Illinois students, faculty or staff unless approved by the Office of Campus Emergency Planning (OCEP) following the procedures outlined in Appendix J.

c. All access to data through the Internet or an Intranet shall be through a secure connection or service following accepted CCGISC standards.

14. DATA ARCHIVES & BACKUPS

a. Archive copies shall be maintained for all custodial, production, and hosted data. All digital data, including archived data, shall be backed up daily to an offsite facility.

15. DIGITAL DATA ACCESS AND DISTRIBUTION

a. CCGISC members and/or Member Agents, on behalf of a member agency, may make CCGISC custodial data available for public viewing and printing only, but shall not do so in any manner that would allow the service and/or data to be downloaded or consumed for use outside of the member agency organization or otherwise defeat, frustrate, or circumvent any aspect of CCGISC policy or the CCGISC Intergovernmental Agreement. Any data housed on the CCGISC servers - custodial, repository, production, hosted or otherwise - may not be published from the CCGISC servers in a manner which would allow the service to be directly consumed outside of the member agency organization or otherwise defeat, frustrate, or circumvent any aspect of CCGISC policy or the CCGISC Intergovernmental Agreement.

b. CCGISC members and/or Member Agents are required to follow specific guidelines and requirements for digital data access and distribution found in the CCGISC Rules of Engagement at Appendix L.

16. DISCLAIMERS

a. If it is the intent and/or requirement of a member agency or Member Agent, on behalf of the member agency, to include a disclaimer on a document that contains CCGISC custodial data, the document disclaimer found in Appendix K shall be used. It is suggested viewers of a web-based map or application that contains custodial data published by a member agency or Member Agent on behalf of a member agency, first view and acknowledge the map application disclaimer found in Appendix K.

Appendices
CCGISC Digital Data Policy

Digital Data Category List

CUSTODIAL DATA	**Verification Responsibility**
Enterprise Geodatabases	
CCGISV *(all data except as listed under Repository Data)*	CCGISC
CCGISR	CCGISC
ccgiscHistoric	CCGISC
REPOSITORY DATA	**Verification Responsibility**
Enterprise Geodatabases	
CCGISV	
ConservationReserveProgram	USDA/CCSWCD
DrainageDistricts	USDA/CCSWCD
WoodedAreas	USDA/CCSWCD
DFIRM feature dataset	FEMA
Soils	USDA/CCSWCD
OutsideAgencies feature dataset	Various *(MTD, ISGS, UIUC, COC, Urbana, USGS)*
UCSD feature dataset	UCSD
ParksRecreation feature dataset	RPC
CensusData	US Census Bureau
PRODUCTION DATA	**Verification Responsibility**
Enterprise Geodatabases	
ccgiscParcelFabric	CCGISC
ccgiscProduction	CCGISC
SanitarySewer	CCGISC
ccgiscWork	CCGISC
AddressDatabase	CCGISC/Addressing Jurisdictions

HOSTED DATA	**Ownership**	
Enterprise Geodatabases		
IDOT	IDOT	
Douglas	Douglas County	
Mahomet	Village of Mahomet	
Piatt	Piatt County	
Piattr	Piatt County	
Urbana	City of Urbana	
UrbanaProjects	City of Urbana	
Lucity	City of Urbana	
SECURITY RISK	**Security Risk Agency**	**Verification Responsibility**
Enterprise Geodatabases		
CCGISV		
EMA feature dataset	County	EMA
SanitarySewer feature dataset	University	CCGISC
StormmSewer feature dataset	University	CCGISC

UNIVERSITY OF ILLINOIS CLICK-THROUGH DATA RELEASE AGREEMENT

This License Agreement ("Agreement") is made and entered into by and between the Champaign County Geographic Information System Consortium ("CCGISC") and any University of Illinois at Urbana-Champaign enrolled student or University of Illinois at Urbana-Champaign faculty or staff member on behalf of an Academic or Administrative Department with a valid Net ID ("User") who completes the registration process and downloads the CCGISC GIS data vector layers and/or raster imagery ("Data"). CCGISC and User are collectively referred to as the "parties".

1. ***Service Terms and Limitations***

   a. *Description.* The Data is proprietary to CCGISC. User's access to the Data is licensed and not sold.

   b. *Format.* All vector Data is provided in a digital format within an ESRI file geodatabase. All raster data is provided in a compressed image format. The type of compressed image format varies with acquisition year.

   c. *Equipment.* User shall be solely responsible for all equipment and software necessary to download, access, view, and utilize the Data.

2. ***Limitations and Prohibited Uses***

   a. *Credits.* Source to list: ***Champaign County GIS Consortium***
   Any hard copy, digital or web-based documents/maps that are distributed outside of the User or the User's department, either by permission of CCGISC or in a "view-only" capacity, utilizing any of the Data, modified or otherwise, shall clearly indicate CCGISC as the data source. If the User has modified or supplemented the Data in any way, the User is obligated to describe the types of modifications or supplementation they have performed within the publication. The User specifically agrees to not misrepresent any Data, nor to expressly or impliedly state any changes made in the Data have been approved by CCGISC unless prior written approval by CCGISC has been obtained.

   b. *Protection of Proprietary Rights.* Reproduction, resale, or redistribution of digital Data by the User for use by others or outside of the User's department, in whole or in part, is expressly forbidden. Notwithstanding the above prohibition, digital Data may be distributed in a **"view–only"** capacity on hardcopy, through digital documents or web-based maps if appropriately credited as set forth above. Reproduction or redistribution of digital Data products derived from the provided digital Data for use outside of the User's department is expressly forbidden without prior permission in writing from CCGISC.

3. ***Disclaimer of Warranties***

   The Data is provided "as is". There is no guarantee or warranty concerning the accuracy, adequacy, completeness, legality, reliability or usefulness of information contained in the Data. This disclaimer applies to both isolated and aggregate uses of the Data. **No warranty is made, either expressed or implied, as to any other matter whatsoever, including, without limitation, the condition of the product, merchantability, freedom from contamination by computer viruses and non-infringement of proprietary rights or its fitness for any particular purpose.** The burden for determining fitness for

use lies entirely with the User. Changes may be periodically made to the Data herein; these changes may or may not be incorporated in any new version of the publication. Data may become out of date. It is recommended that careful attention be paid to the contents of the Data. Should the User find any errors or omissions, please report them to CCGISC.

4. Limitation of Liability

Neither CCGISC, nor any of the agencies who are part of CCGISC, shall be held liable for any improper or incorrect use of the Data and assumes no responsibility for anyone's use of the Data. In no event shall CCGISC, or any of the agencies who are part of the CCGISC have any liability whatsoever resulting from the use of the Data by the User for payment of any consequential, incidental, indirect, special, or tort damages of any kind, including, but not limited to, any loss of profits, data or use; procurement of substitute goods or services or business interruption however, caused and on any theory of liability, whether in contract strict liability or tort (including negligence or otherwise) arising in any way out of use of or reliance on the Data or arising out of the delivery, installation, operation, or user support relating to the same even if advised of the possibility of such damage. This limitation of liability applies to any damages or injury, including but not limited to those caused by any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, theft destruction or unauthorized access to, alteration of, or use of Data whether for breach of contract, tortious behavior, negligence or under any other cause of action.

5. Remedy for Violation

In the event the User exceeds the scope of this Agreement or in any other manner violates the terms and conditions hereof, CCGISC shall have the right to enjoin such activities as violate the terms this Agreement and may seek any other allowable remedies, including the right to obtain its reasonable costs and attorney fees as awarded by a court of competent jurisdiction in connection therewith.

6. User Representation and Information

User represents and warrants to CCGISC that: (a) User is over the age of eighteen (18) and has the power and authority to enter into and perform the User obligations under this Agreement; (b) all the information provided by User to CCGISC is truthful, accurate and complete; (c) User shall comply with all terms and conditions of this Agreement, including, without limitation, the provisions set forth at Section 5; and (e) User has provided and will provide accurate and complete registration information, including, without limitation, User's legal name, University of Illinois NET ID, e-mail address and telephone number.

FORM FIELDS

University of Illinois NET ID
User First Name
User Last Name
User e-mail address
University Affiliation Type (check box or down)
    Student
    Faculty
    Staff
- If student chosen prompt them to enter department of major (undeclared is acceptable)
- If Faculty or Staff chosen prompt them to enter Academic or Administrative Department

ACCEPTANCE AREA

7. ***BY CLICKING THE ACCEPT BUTTON, ACCESSING, USING OR DOWNLOADING ANY PART OF THE DATA, THE USER EXPRESSLY AGREES TO AND CONSENTS TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT. IF THE USER DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THE BUTTON INDICATING "DO NOT ACCEPT" MUST BE SELECTED, THIS TRANSACTION WILL PROMPTLY BE CANCELED AND USER MAY NOT ACCESS, DOWNLOAD OR USE ANY PART OF THE DATA.***

I agree to the terms of this Agreement and agree not to redistribute the provided data.

ACCEPT

I do not agree to the terms of the Agreement

DO NOT ACCEPT

CCGISC Information:

Champaign County GIS Consortium
1776 East Washington Street
Urbana, Illinois 61802
Phone (217) 819-3555 Fax (217) 384-3896
http://www.ccgisc.org

Digital Data Release Agreement

Champaign County GIS Consortium
1776 East Washington Street
Urbana, Illinois 61802
Phone (217) 819-3555
http://www.ccgisc.org

LICENSE AGREEMENT FOR USE of CHAMPAIGN COUNTY GIS CONSORTIUM DATA BY CONSULTANTS ON A MEMBER AGENCY PROJECT

DATA DISTRIBUTION

Data distribution shall be requested from the Champaign County GIS Consortium (CCGISC). All Digital data is provided for distribution by E-MAIL or via the Champaign County GIS Consortium (CCGISC) download site unless other media is agreed upon.

NO WARRANTY

The data files are provided "as is". There is no guarantee or warranty concerning the accuracy of information contained in the data. **No warranty is made, either expressed or implied, as to any other matter whatsoever, including, without limitation, the condition of the product, or its fitness for any particular purpose.** The burden for determining fitness for use lies entirely with the user.

LIMITATION OF LIABILITY

In no event shall any of the agencies who are part of the CCGISC have any liability whatsoever resulting from the use of CCGISC Data by the Consultant with whom CCGISC has entered into this License Agreement for payment of any consequential, incidental, indirect, special, or tort damages of any kind, including, but not limited to, any loss of profits arising out of use of or reliance on the data or arising out of the delivery, installation, operation, or user support relating to the same.

PROTECTION OF PROPRIETARY RIGHTS

Reproduction or redistribution of the data or products derived there from outside the Consultant's organization or entity is expressly forbidden. The data shall only be used by the Consultant only on the specified project for the unit of local government. The Consultant may not further reproduce or redistribute the data beyond the scope of the specified project. Upon project completion all files containing any source data or products derived there from shall be returned by the Consultant to CCGISC. None of the data shall be electronically duplicated by the Consultant by any means for use by others, in whole or in part, without express written permission of the CCGISC. Resale of the data by the Consultant is prohibited.

CREDITS

Source to list: ***Champaign County GIS Consortium***

Any hard copies made by the Consultant utilizing any of the data shall clearly indicate the source. The Consultant specifically agrees not to misrepresent any data, nor to express or imply any changes made in the data have been approved unless actual prior approval by CCGISC has been obtained.

REMEDY FOR VIOLATION

In the event the Consultant exceeds the scope of this License Agreement or in any other manner violates the terms and conditions hereof, CCGISC shall have the right to enjoin such activities as violate the terms this agreement and may seek any other allowable remedies, including the right to obtain its reasonable costs and attorney fees in connection therewith.

The digital data is authorized to:

BUSINESS | ADDRESS

PHONE | CITY, STATE, ZIP

pursuant to the terms and conditions listed in this LICENSE AGREEMENT. The data is provided for use in completing the following project:

PROJECT

DATA REQUESTED

for the: GIS CONSORTIUM MEMBER AGENCY | MEMBER REPRESENTATIVE NAME

MEMBER REPRESENTATIVE PHONE and EMAIL ADDRESS

The Consultant hereby agrees to the terms and conditions in the attached LICENSE AGREEMENT and agrees to abide by same.

Printed Name | Title

Signature | Date

E-mail

COMPLETE AND E-MAIL TO:
ccgisc@co.champaign.il.us

Any questions, please call the GIS Consortium office at
Phone (217) 819-3555

Digital Data License Agreement

Standard

Champaign County GIS Consortium
1776 E Washington Street
Urbana, IL 61802
Phone (217) 819-3555
http://www.ccgisc.org

By agreeing to the terms, the user acknowledges and accepts the terms and conditions of this License Agreement.

This Agreement provides the Licensee the ability to utilize purchased Champaign County Geographic Information System Consortium ("CCGISC") data obtained through an Annual Download Subscription Purchase **OR** a One-time Data Purchase according to the terms and conditions of this Agreement. The Annual Download Subscription Purchase provides the Licensee the ability to download the GIS data layers listed in Appendix A from a download window on the CCGISC Interactive Public Web Site ("CCIPW") at www.maps.ccgisc.org, in exchange for a fee of $250.00. The One-time Data Purchase provides the Licensee a single copy of the GIS data in exchange for the cost of requested data layers as found on Data Request Form.

Terms and Conditions

DATA ACCESS TERMS

Annual Download Subscription Purchase

Access to the download site shall be enabled upon receipt of payment. Access credentials in form of a username and password will be provided to the Licensee upon receipt of payment or an account can be set-up through the CCGISC Map Store - www.ccgisc.org/MapStore.aspx. Distribution of the credentials outside the Licensee's organization or entity is expressly forbidden. Access shall be terminated by CCGISC one year from the date of the receipt of payment.

One-time Data Purchase

Upon receipt of payment, one-time data purchases shall be distributed by CCGISC to the Licensee by email or through the Internet from a provided URL link unless another media is agreed upon.

NO WARRANTY

The data files are provided "as is". There is no guarantee or warranty concerning the accuracy, adequacy, completeness, legality, reliability, or usefulness of information contained in the data. This disclaimer applies to both isolated and aggregate uses of the data. **No warranty is made, either expressed or implied, as to any other matter whatsoever, including, without limitation, the condition of the product, merchantability, freedom from contamination by computer viruses and non-infringement of proprietary rights or its fitness for any particular purpose.** The burden for determining fitness for use lies entirely with the user.

LIMITATION OF LIABILITY

Neither CCGISC, nor any of the agencies who are part of CCGISC, shall be held liable for any improper or incorrect use of the data and assumes no responsibility for anyone's use of the data. In no event shall CCGISC, or any of the agencies who are part of the CCGISC have any liability whatsoever resulting from the use of CCGISC data by the Subscriber for any consequential, incidental, indirect, special, or tort damages of any kind, including, but not limited to, any loss of profits, data or use; procurement of substitute goods or services or business interruption however, caused and on any theory of liability, whether in contract strict liability or tort (including negligence or otherwise) arising in any way out of use of or reliance on the data or arising out of the delivery, installation, operation, or user support relating to the same even if advised of the possibility of such damage. This limitation of liability applies to any damages or injury, including but not limited to those caused by any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, theft destruction or unauthorized access to, alteration of, or use of data whether for breach of contract, tortious behavior, negligence or under any other cause of action.

PROTECTION OF PROPRIETARY RIGHTS

Reproduction, resale, or redistribution of the digital data for use by others outside of the Licensee's organization or entity is expressly forbidden. Notwithstanding the above prohibition, digital data may be distributed by the Licensee in a "view–only" capacity on hardcopy, through digital documents or web-based maps if appropriately credited as set forth below. Reproduction or redistribution of digital data products derived from the provided digital data for use outside Licensee's organization is expressly forbidden without prior permission in writing from CCGISC. The data provided by CCGISC shall remain the property of CCGISC, which shall retain all rights commensurate with ownership, including the right to sell, release, license, use, or provide the data to others as it deems appropriate in its sole discretion.

DAYS AND HOURS OF OPERATION

Annual Download Subscription Purchase

Every effort will be made to ensure CCIPW and download functionality are available seven days a week, 24 hours a day, including holidays. Exceptions include periods of preventive or remedial maintenance and/or operational or security issues. CCGISC will not be liable, financially, or otherwise, for periods of inaccessibility.

One-time Data Purchase

The CCGISC offices are generally open from 8:00 am to 4:30 pm Monday through Friday, except on County holidays.

OBLIGATIONS

Annual Download Subscription Purchase

It is the responsibility of the Licensee to purchase, obtain, and install all necessary equipment, software, and services necessary to properly download the CCGISC GIS data layers from CCIPW. The Licensee is responsible for ensuring the access credentials are not distributed outside of the Licensee's organization or entity.

One-time Data Purchase

It is the responsibility of the Licensee to purchase, obtain, and install all necessary equipment, software, and services necessary to utilize the purchased GIS data layers.

CREDITS

Source to list: ***Champaign County GIS Consortium***

Any hard copy, digital or web-based documents/maps that are distributed outside of the Licensee's organization either by permission of CCGISC or in a "view-only" capacity, utilizing any of the data, modified or otherwise, shall clearly indicate CCGISC as the data source. If the Licensee has modified or supplemented the data in any way, the Licensee is obligated to describe the types of modifications or supplementation they have performed within the publication. The Licensee specifically agrees not to misrepresent any data, nor to expressly or impliedly state any changes made in the data have been approved by CCGISC unless prior written approval by CCGISC has been obtained.

TERMINATION

This Agreement may be terminated immediately by CCGISC for Licensee's failure to comply with any of the terms of this Agreement or failure to perform any of its obligations. This Agreement shall also terminate immediately if CCGISC Policy Board fails to appropriate or continue funding for services provided under this Agreement.

REMEDY FOR VIOLATION

In the event the Licensee exceeds the scope of this agreement or in any other manner violates the terms and conditions hereof, CCGISC shall have the right to enjoin such activities as violate the terms of this Agreement and may seek any other allowable remedies, including the right to obtain its reasonable costs and attorney fees in connection therewith.

The Licensee hereby agrees to the terms and conditions of this AGREEMENT and agrees to abide by the same.

_____

Licensee (Organization or Company Name; if not part of an Organization or Company print First and Last Name)

_____ _____

Phone City, State, Zip

_____

By (Printed Name)

_____

Title (if part of an organization)

_____

E-mail

_____ _____

Licensee Signature Date

Any questions, please call the GIS Consortium office at
Phone (217) 819-3555

For Internal Use Only:
Data Sales Number: _____

Supplemental Information

Inquiries regarding the Agreement should be directed to CCGISC at ccgisc@co.champaign.il.us or 217.819.3555.

Payment by Check:

Mail or email this entire agreement, signed, and dated, along with payment by check to:

Champaign County GIS Consortium
1776 E Washington Street
Urbana, IL 61802

Payment by Credit Card:

Email the entire agreement to ccgisc@co.champaign.il.us, upon receipt a PayPal invoice will be e-mailed to you.

Appendix A – Downloadable CCGISC Data Layers

Street Centerlines
Hydrology Centerlines
Stream Polygons
Lakes
Tax Parcel Points *(Assessment Data NOT included)*
Tax Parcel Polygons *(Assessment Data NOT included)*
Subdivisions
Municipal Boundaries
Municipal Annexations
Civil Townships
County Board Districts
State Representative Districts
Voting Precincts

Taxing Districts

School Districts
High School Districts
Community College Districts
Fire Districts
Library Districts
Park Districts
Public Health Districts
Cemetery Districts
UC Sanitary Districts
Mass Transit Districts
Multi Assessor Districts
Forest Preserve Districts
Township Roads and Bridges Districts

Digital Data License Agreement

Derived Products

Champaign County GIS Consortium
1776 E Washington Street
Urbana, IL 61802
Phone (217) 819-3555
http://www.ccgisc.org

By agreeing to the terms, the user acknowledges and accepts the terms and conditions of this License Agreement.

This agreement between the Champaign County Geographic Information System Consortium ("CCGISC") and the Licensee provides the Licensee the ability to utilize purchased CCGISC data obtained through an Annual Download Subscription Purchase **OR** a One-time Data Purchase for derived products according to the terms and conditions of this Agreement. The Annual Download Subscription Purchase provides the Licensee the ability to download the GIS data layers listed in Appendix A from a download window on the CCGISC Interactive Public Web Site ("CCIPW") at www.maps.ccgisc.org, in exchange for a fee of $250.00. The One-time Data Purchase provides the Licensee a single copy of the GIS data in exchange for the cost of requested data layers as found on Data Request Form.

Terms and Conditions

DATA ACCESS TERMS

Annual Download Subscription Purchase
Access to the download site shall be enabled upon receipt of payment. Access credentials in form of a username and password will be provided to the Licensee upon receipt of payment or an account can be set-up through the CCGISC Map Store - www.ccgisc.org/MapStore.aspx. Distribution of the credentials outside the Licensee's organization or entity is expressly forbidden. Access shall be terminated by CCGISC one year from the date of the receipt of payment.

One-time Data Purchase
Upon receipt of payment, one-time data purchases shall be distributed by CCGISC to the Licensee by email or through the Internet from a provided URL link unless another media is agreed upon.

NO WARRANTY
The data files are provided "as is". There is no guarantee or warranty concerning the accuracy, adequacy, completeness, legality, reliability, or usefulness of information contained in the data. This disclaimer applies to both isolated and aggregate uses of the data. **No warranty is made, either expressed or implied, as to any other matter whatsoever, including, without limitation, the condition of the product, merchantability, freedom from contamination by computer viruses and non-infringement of proprietary rights or its fitness for any particular purpose.** The burden for determining fitness for use lies entirely with the user.

LIMITATION OF LIABILITY

Neither CCGISC, nor any of the agencies who are part of CCGISC, shall be held liable for any improper or incorrect use of the data and assumes no responsibility for anyone's use of the data. In no event shall CCGISC, or any of the agencies who are part of the CCGISC have any liability whatsoever resulting from the use of CCGISC data by the Subscriber for any consequential, incidental, indirect, special, or tort damages of any kind, including, but not limited to, any loss of profits, data or use; procurement of substitute goods or services or business interruption however, caused and on any theory of liability, whether in contract strict liability or tort (including negligence or otherwise) arising in any way out of use of or reliance on the data or arising out of the delivery, installation, operation, or user support relating to the same even if advised of the possibility of such damage. This limitation of liability applies to any damages or injury, including but not limited to those caused by any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, theft destruction or unauthorized access to, alteration of, or use of data whether for breach of contract, tortious behavior, negligence or under any other cause of action.

PROTECTION OF PROPRIETARY RIGHTS BY LICENSEES

Reproduction, resale, or redistribution of the digital data for use by others outside of the Licensee's organization or entity shall be strictly limited as detailed in the Data Usage Provision included as Appendix B, and for subcontractors of the Licensee involved as detailed in the Data Usage Provision included as Appendix B. Except as detailed in Appendix B, data obtained by the Licensee from the CCGISC may be reproduced by the Licensee for backup purposes only. None of the data shall be electronically duplicated by the Licensee by any means other than as detailed in the Data Usage Provision, attached as Appendix B, for use by others, in whole or in part, without express written permission of the CCGISC. Resale of the original data by the Licensee is prohibited.

DAYS AND HOURS OF OPERATION

Annual Download Subscription Purchase

Every effort will be made to ensure CCIPW and download functionality are available seven days a week, 24 hours a day, including holidays. Exceptions include periods of preventive or remedial maintenance and/or operational or security issues. CCGISC will not be liable, financially, or otherwise, for periods of inaccessibility.

One-time Data Purchase

The CCGISC offices are generally open from 8:00 am to 4:30pm Monday through Friday, except on County holidays.

OBLIGATIONS

Annual Download Subscription Purchase

It is the responsibility of the Licensee to purchase, obtain, and install all necessary equipment, software, and services necessary to properly download the CCGISC GIS data layers from CCIPW. The Licensee is responsible for ensuring the access credentials are not distributed outside of the Licensee's organization or entity.

One-time Data Purchase

It is the responsibility of the Licensee to purchase, obtain, and install all necessary equipment, software, and services necessary to utilize the purchased GIS data layers.

CREDITS

The Licensee specifically agrees not to misrepresent any data, nor to express or imply any changes made in the data have been approved by CCGISC unless actual prior approval by CCGISC has been obtained.

TERMINATION

This Agreement may be terminated immediately by CCGISC for Licensee's failure to comply with any of the terms of this Agreement or failure to perform any of its obligations. This Agreement shall also terminate immediately if CCGISC Policy Board fails to appropriate or continue funding for services provided under this Agreement.

REMEDY FOR VIOLATION

In the event the Licensee exceeds the scope of this License Agreement or in any other manner violates the terms and conditions hereof, the CCGISC shall have the right to enjoin such activities as violate the terms of this Agreement and may seek any other allowable remedies, including the right to obtain its reasonable costs and attorney fees in connection therewith.

The Licensee hereby agrees to the terms and conditions of this AGREEMENT and agrees to abide by the same.

Licensee (Organization or Company Name; if not part of an Organization or Company print first and last name)

Phone City, State, Zip

By: (Printed Name)

Title (if part of an organization)

E-mail

Subscriber or Licensee Signature Date

GIS Director Signature Date

Any questions, please call the GIS Consortium office at Phone (217) 819-3555

For Internal Use Only:
Data Sales Number: _____

Supplemental Information

Inquiries regarding the Agreement should be directed to CCGISC at ccgisc@co.champaign.il.us or 217.819.3555.

Payment by Check:

Mail or email this entire agreement, signed, and dated, along with payment by check to:

Champaign County GIS Consortium
1776 E Washington Street
Urbana, IL 61802

Payment by Credit Card:

Email the entire agreement to ccgisc@co.champaign.il.us, upon receipt a PayPal invoice will be e-mailed to you.

Appendix A – Downloadable CCGISC Data Layers

Street Centerlines
Hydrology Centerlines
Stream Polygons
Lakes
Tax Parcel Points *(Assessment data NOT included)*
Tax Parcel Polygons *(Assessment Data NOT included)*
Subdivisions
Municipal Boundaries
Municipal Annexations
Civil Townships
County Board Districts
State Representative Districts
Voting Precincts

Taxing Districts
School Districts
High School Districts
Community College Districts
Fire Districts
Library Districts
Park Districts
Public Health Districts
Cemetery Districts
UC Sanitary Districts
Mass Transit Districts
Multi Assessor Districts
Forest Preserve Districts
Township Roads and Bridges Districts

Appendix B – Data Usage Provisions

[To be prepared by Licensee.]

Digital Data Order Form

Customer:	
Date:	
PO #:	
Contact:	
Phone:	
Email:	

To purchase Champaign County GIS data, complete this form and return to *ccgisc@co.champaign.il.us*.

Credit card payments are processed via PayPal and subject to an approximate 3% convenience fee.

Checks payable to:

Champaign County GIS Consortium
1776 E. Washington St.
Urbana, IL 61802
Phone: 217-819-3555

Questions? Call (217) 819-3555 or email ccgisc@co.champaign.il.us

ORDER INFORMATION

GIS Data Subscription

Cost: $250.00/year
Download Format: geodatabase, shapefile, dxf, dwg, or dgn

Subscribers receive a login to the Champaign County Public Interactive Map -http://maps.ccgisc.org/public/.
The login allows ***download*** access to the following countywide data layers:

- Street Centerlines
- Hydrology Centerlines
- Stream Polygons
- Lake Polygons
- Tax Parcel Points ∗
- Tax Parcel Polygons ∗
- Subdivisions / Lots
- Civil Townships
- Municipal Boundaries
- Municipal Annexations
- County Board Districts
- State Representative Districts
- Voting Precincts
- School Districts
- High School Districts
- Community College Districts
- Forest Preserve Districts
- Fire Districts
- Library Districts
- Park Districts
- Public Health Districts
- Cemetery Districts
- UC Sanitary Districts
- Mass Transit Districts
- Multi Assessor Districts
- Township Road / Bridge Districts

∗ *Tax parcel layers only include the parcel number attribute.*

One-time Individual Order Form

All orders subject to a $11.25 set-up fee

Item:	Cost:	Qty:	Total:
Administrative, Political and Taxing District Boundaries *(entire county)*			
Administrative Boundaries – Municipal, Civil Township, UCSD	$50.00		
Administrative Boundary Annexations – Municipal, Civil Township, UCSD	$50.00		
Political Boundaries (State Representative Districts, County Board District and Precincts)	$50.00		
Taxing Districts (school districts only)	$75.00		
Taxing Districts (all taxing districts including school districts)	$125.00		
Parcel Data			
Parcel Polygons – entire county*	$100.00		
Parcel Polygons – subset ($20 minimum purchase) *	$0.01 /polygon		
Parcel Boundary Line Features – entire county	$100.00		
Subdivisions/Lots – entire county	$150.00		
∗ Tax parcel polygons only include the parcel number attribute			
Topographic Data *(2500' x 2500' tiles)*			
Contour Data	$2.50 / tile		
Planimetric Data *(provided in ESRI shape format)*			
Road Centerlines - entire County (no Addresses)	$50.00		
Road Centerlines - entire County (w/Addresses)	$250.00		
Hydro Group – entire county	$100.00		
Prints *(print orders subject to minimum $11.25 set-up charge)*			
Large Format Prints (standard maps)	$1.50 / sq ft		
Laser Prints 8.5 x 11 or 8.5 x 14	$1.00		
Laser Prints 11 x 17	$1.50		
Assessment Data *(as attributes w/parcel data – or provided as .dbf table)*			
Parcel master table	$0.05 / record		
Parcel sales table	$0.05 / record		
Parcel master table - full file (entire County)	$1,500.00		
Parcel sales table – full file (entire County)	$500.00		
Ortho-Imagery			
Uncompressed TIF Tiles			
Ortho-imagery Tiles (standard procedure is to provide as .TIF images - MrSid images may also be available - please specify preference when submitting request) 2002 Black & White 6" pixel resolution for urbanized areas, 2' countywide 2005 Color 6" pixel resolution for urbanized areas, 2' countywide 2008 Color 6" pixel resolution for urbanized areas, 2' countywide 2011 Color 6" pixel resolution coverage of Champaign, Urbana, Mahomet and Savoy—1' pixel size countywide 2014 Color 6" pixel resolution countywide 2017 Color 6" pixel resolution countywide 2020 Color 6" pixel resolution countywide See index maps showing tile coverage details	$1.25 / tile 2014 and older $2.50 / tile 2017 – present		

Item:	Cost:	Qty:	Total:
Ortho-Imagery			
Compressed Image Tiles *(MrSid and/or Jpeg2000)*			
2008 Color 6" pixel resolution for urbanized areas, 2' countywide 2011 Color 6" pixel resolution coverage of Champaign, Urbana, Mahomet and Savoy—1' pixel size countywide 2014 Color 6" pixel resolution countywide 2017 Color 6" pixel resolution countywide 2020 Color 6" pixel resolution countywide – **See index maps showing tile coverage details**	$0.75 / tile *2008 and 2011* $1.25 / tile *2017 and 2020*		
High Resolution Compressed Image Mosaics *(MrSid and/or Jpeg200)*			
2002 Black & White - 6" pixel resolution for urbanized areas	$440		
2005 Color - 6" pixel resolution for urbanized area	$780		
2008 Color - 6" pixel resolution for urbanized area	$850		
2011 Color - 6" pixel resolution for Champaign, Urbana, Mahomet and Savoy	$780		
2014 Color - 6" pixel resolution County-wide	$6,520		
2017 Color- 6" pixel resolution County-wide	$3,260		
2020 Color- 6" pixel resolution County-wide	$6,560		
2020 Color - 6" pixel resolution Champaign only	$500		
2020 Color - 6" pixel resolution Urbana only	$430		
2020 Color - 6" pixel resolution Savoy only	$220		
2020 Color - 6" pixel resolution Rantoul only	$360		
2020 Color - 6" pixel resolution Mahomet only	$400		
2020 Color - 6" pixel resolution University only	$220		
Low Resolution Compressed Image Mosaics *(MrSid and/or Jpeg200)*			
2002 Black & White – 2' pixel resolution County-wide *2005 Color – 2' pixel resolution County-wide* *2008 Color – 2' pixel resolution County-wide*	$200 / mosaic		
2011 Color – 2' pixel resolution County-wide	$360		
Set Up			
Set-up Fee: $45 / hour – billed in ¼ hour increments	$45.00 / hr		
	Total Amount:		

All orders subject to a $11.25 set-up fee

Digital Data License Agreement

ANNUAL

Champaign County GIS Consortium
1776 East Washington Street
Urbana, Illinois 61802
Phone (217) 819-3555
http://www.ccgisc.org

THIS AGREEMENT is between _____, herein called the "Agency", and the Champaign County GIS Consortium, herein called the "CCGISC".

The Agency desires to purchase digital data from the CCGISC on one or more occasions during the term of this Agreement. The parties therefore agree to the following terms and conditions as part of this Agreement to facilitate the Agency purchase of digital data from the CCGISC.

ALL INCLUSIVE
All data provided to the Agency by the CCGISC under this Agreement during the term specified shall be subject to this Agreement.

TERM
The term of this Agreement shall be from January 1, 20XX to December 31, 20XX.

DATA DISTRIBUTION
All Digital data provided by the CCGISC to the Agency pursuant to this Agreement shall be by email or through the Internet from a provided URL link unless another media is agreed upon.

NO WARRANTY
The data files are provided "as is". There is no guarantee or warranty concerning the accuracy, adequacy, completeness, legality, reliability, or usefulness of information contained in the data. This disclaimer applies to both isolated and aggregate uses of the data. **No warranty is made, either expressed or implied, as to any other matter whatsoever, including, without limitation, the condition of the product, merchantability, freedom from contamination by computer viruses and non-infringement of proprietary rights or its fitness for any particular purpose.** The burden for determining fitness for use lies entirely with the user.

LIMITATION OF LIABILITY

Neither CCGISC, nor any of the agencies who are part of CCGISC, shall be held liable for any improper or incorrect use of the data and assumes no responsibility for anyone's use of the data. In no event shall CCGISC, or any of the agencies who are part of the CCGISC have any liability whatsoever resulting from the use of CCGISC data by the Subscriber for any consequential, incidental, indirect, special, or tort damages of any kind, including, but not limited to, any loss of profits, data or use; procurement of substitute goods or services or business interruption however, caused and on any theory of liability, whether in contract strict liability or tort (including negligence or otherwise) arising in any way out of use of or reliance on the data or arising out of the delivery, installation, operation, or user support relating to the same even if advised of the possibility of such damage. This limitation of liability applies to any damages or injury, including but not limited to those caused by any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, theft destruction or unauthorized access to, alteration of, or use of data whether for breach of contract, tortious behavior, negligence or under any other cause of action.

PROTECTION OF PROPRIETARY RIGHTS

Reproduction, resale, or redistribution of the digital data for use by others outside of the Licensee's organization or entity is expressly forbidden. Notwithstanding the above prohibition, digital data may be distributed by the Licensee in a "view–only" capacity on hardcopy, through digital documents or web-based maps if appropriately credited as set forth below. Reproduction or redistribution of digital data products derived from the provided digital data for use outside Licensee's organization is expressly forbidden without prior permission in writing from CCGISC. The data provided by CCGISC shall remain the property of CCGISC, which shall retain all rights commensurate with ownership, including the right to sell, release, license, use, or provide the data to others as it deems appropriate in its sole discretion.

CREDITS

Source to list: ***Champaign County GIS Consortium***

Any hard copy, digital or web-based documents/maps that are distributed outside of the Licensee's organization either by permission of CCGISC or in a "view-only" capacity, utilizing any of the data, modified or otherwise, shall clearly indicate CCGISC as the data source. If the Licensee has modified or supplemented the data in any way, the Licensee is obligated to describe the types of modifications or supplementation they have performed within the publication. The Licensee specifically agrees not to misrepresent any data, nor to expressly or impliedly state any changes made in the data have been approved by CCGISC unless prior written approval by CCGISC has been obtained.

TERMINATION

This Agreement may be terminated immediately by CCGISC for Licensee's failure to comply with any of the terms of this Agreement or failure to perform any of its obligations. This Agreement shall also terminate immediately if CCGISC Policy Board fails to appropriate or continue funding for services provided under this Agreement.

REMEDY FOR VIOLATION

In the event the Licensee exceeds the scope of this agreement or in any other manner violates the terms and conditions hereof, CCGISC shall have the right to enjoin such activities as violate the terms of this Agreement and may seek any other allowable remedies, including the right to obtain its reasonable costs and attorney fees in connection therewith.

The Agency hereby agrees to the terms and conditions in the attached LICENSE AGREEMENT and agrees to abide by same.

Agency:

Printed Name:

Title:

Street Address:

Date:

E-Mail Address:

Signature

Intended use for data:

Any questions, please call the GIS Consortium office at
Phone (217) 819-3555

Julia R. Rietz
State's Attorney

Matthew P. Banach
Chief of the Civil Division
email: mbanach@co.champaign.il.us

Courthouse
101 East Main Street
P. O. Box 785
Urbana, Illinois 61801
Phone (217) 384-3733
Fax (217) 384-3816

Office of
State's Attorney
Champaign County, Illinois

October 18th, 2022

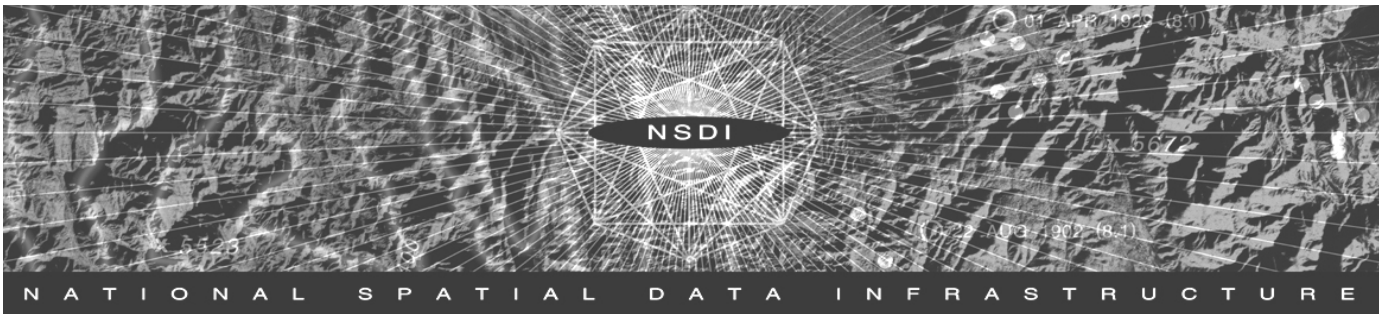
I have been requested to provide a legal opinion as to whether any GIS data or related products based on GIS data are subject to disclosure pursuant to the Freedom of Information Act (FOIA), 5 ILCS 140/1 *et seq*.

Section 7(1)(i) of FOIA provides in relevant part that the following shall be exempt from inspection and copying: *"(i) Valuable formulae, computer geographic systems, designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss. The exemption for "computer geographic systems" provided in this paragraph (i) does not extend to requests made by news media as defined in Section 2 of this Act [5 ILCS 140/2] when the requested information is not otherwise exempt and the only purpose of the request is to access and disseminate information regarding the health, safety, welfare, or legal rights of the general public."* See 5 ILCS 140/7(1)(i).

CCGISC, just like any other public body subject to FOIA, should review the specifics of each FOIA request to ensure that any exemption(s) claimed are appropriate to the relevant facts and specifics of each request. That said, it is my legal opinion that it is very likely that the exemption available pursuant to Section 7(1)(i) of FOIA will be routinely applicable to requests for GIS data and related information, presuming that it remains factually accurate in each instance that disclosure of such data could be reasonably expected to produce private gain or public loss. Such factual considerations may include, but need not necessarily be limited to, instances where the data requested is normally subject to a digital data license agreement or similar arrangement where the agreement includes important precautionary restrictions, as disclosure via FOIA would produce both private gain and public loss by evading a proper license and its protections.

Separately, recall that a public body is not required to copy public records available online. See 5 ILCS 140/8.5. To the extent, if any, CCGISC may deem it feasible and choose to provide online access to additional data beyond what is already currently available, this provision could also alleviate some FOIA disclosure burdens.

Sincerely,
Matthew P. Banach
Chief of the Civil Division
Champaign County SAO



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:

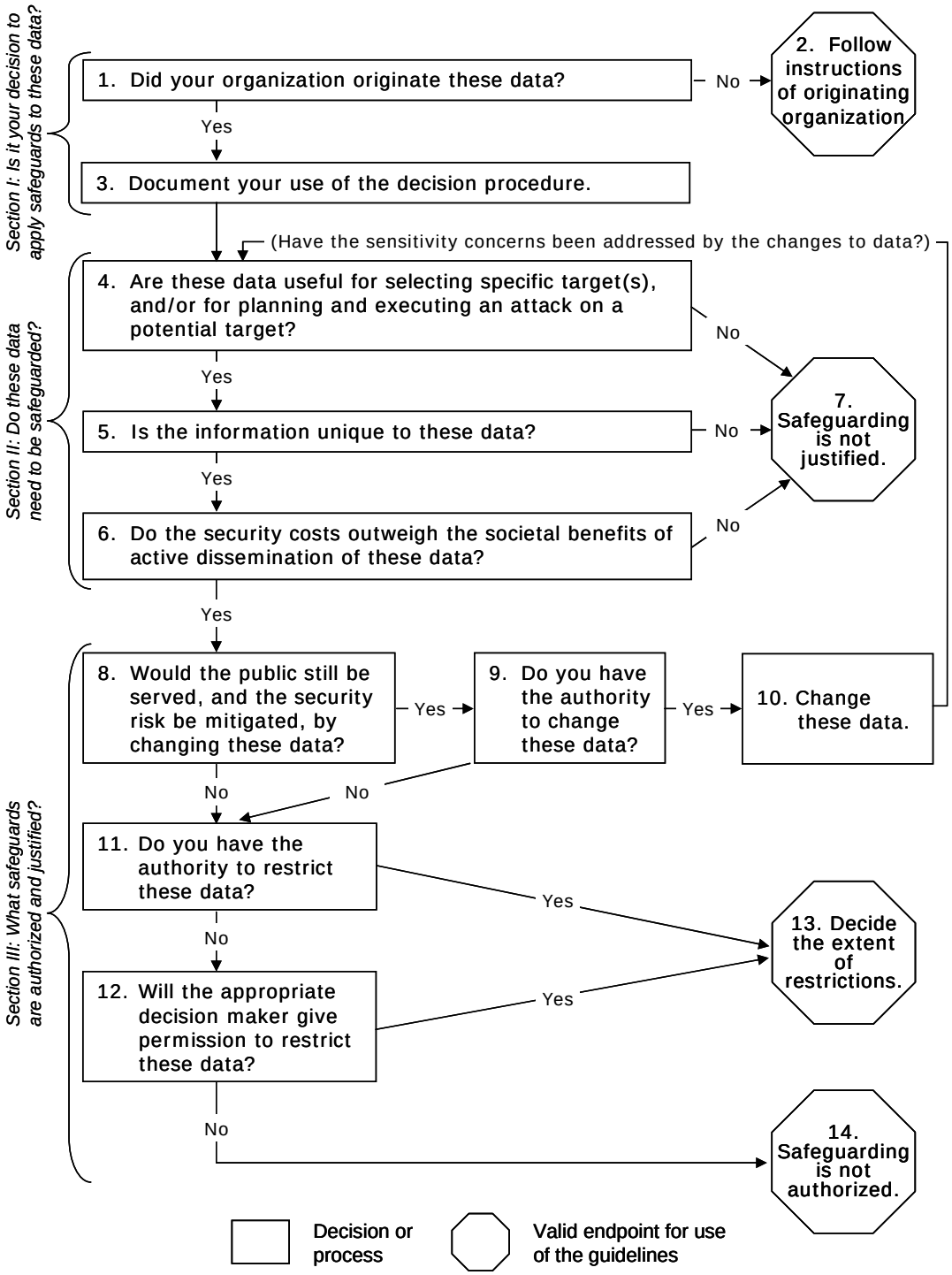
- Change the data: Change the data to remove or modify the sensitive information and then make the changed data available without further safeguards. Organizations are advised to review the changed data to ensure that the change(s) dealt effectively with the security concern.

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.

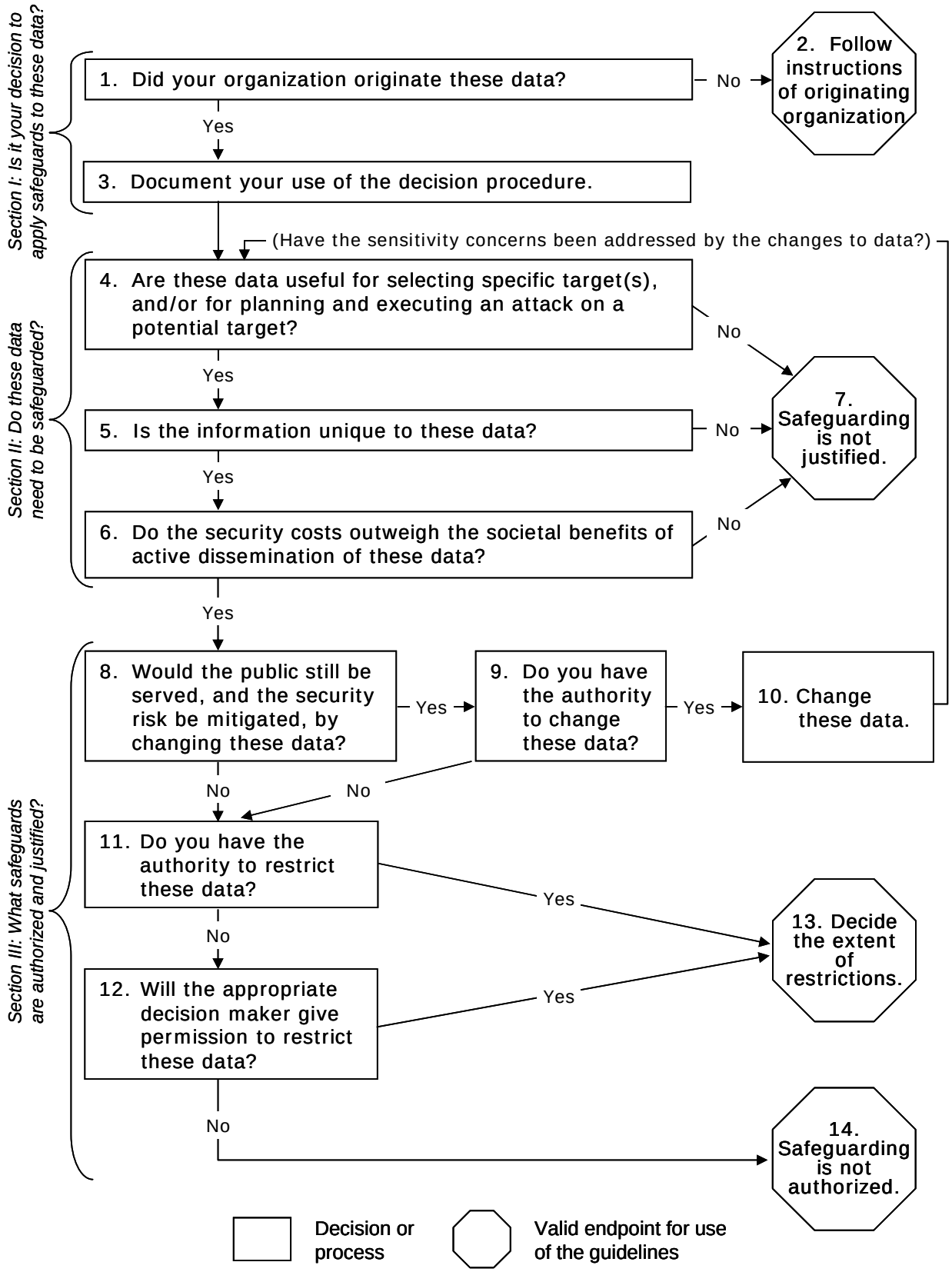
National States Geographic Information Council, 2002, Data access decision tree: National States Geographic Information Council web site at http://www.nsgic.org/hot_topics/security/080702_HS_Decision_Tree_CI_Data _Version7.ppt (Accessed August 12, 2004)

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.)



University of Illinois Student, Faculty or Staff Data Requests

Any CCGISC custodial data classified as a security risk by the University of Illinois in accordance with Section 11a of the CCGISC Data Policy document are governed by the University of Illinois "Campus Administrative Manual" policy on "Distribution of Building Plan Documents and Architectural Drawings" (FO-28). Their approval process begins with the Facilities Data Security On-line Form: https://police.illinois.edu/em/facilities-data-security/. For questions regarding the form or its review please refer to the "Campus Administrative Manual" to obtain the appropriate contact person at the University of Illinois Division of Public Safety.

CCGISC Data Disclaimer

Map Application Disclaimer

“This map application was prepared with geographic information system (GIS) data created by one or more entities including the ***insert Member Agency name here,*** the Champaign County GIS Consortium (CCGISC), or other CCGISC member agency, these entities do not warrant or guarantee the accuracy or suitability of GIS data for any purpose. The GIS data within this application is intended to be used as a general index to spatial information and not intended for detailed, site-specific analysis or resolution of legal matters.”

Document Disclaimer

"This document was prepared with geographic information system (GIS) data created by one or more entities including the ***insert Member Agency name here,*** the Champaign County GIS Consortium (CCGISC), or other CCGISC member agency, these entities do not warrant or guarantee the accuracy or suitability of GIS data for any purpose. The GIS data within this document is intended to be used as a general index to spatial information and not intended for detailed, site-specific analysis or resolution of legal matters.”

Champaign County
City of Champaign
City of Urbana
University of Illinois
Village of Rantoul
Village of Mahomet
Village of Savoy
Village of St Joseph

CCGISC Digital Data Policy – Rules of Engagement

The CCGISC Digital Data Policy defines and outlines the general terms, conditions, and procedures related to the distribution and use of CCIGSC digital data as approved by the CCGISC Policy Committee. The Rules of Engagement detail the specific requirements related to the access, distribution, and use of CCGISC data and infrastructure. These rules are instituted to provide reasonable access to member agencies and member agents (collectively "users") while offering the necessary security and protection to the Champaign County and CCGISC.

DEFINITIONS

1. **CCGISC Infrastructure:** Includes, but is not limited to, all CCGISC and/or Member Agency computer hardware and software hosted on the Champaign County network.
2. **CCGISC Data:** Custodial, Repository, or Production data as defined in the CCGISC Digital Data Policy.
3. **Member Agent:** A third-party consultant hired by a CCGISC Member Agency that acts on behalf of the Member Agency. See the CCGISC Digital Data Policy for additional details.

RULES OF ENGAGEMENT

The Rules of Engagement apply to all users of CCGISC Data and/or CCGISC Infrastructure *(software, hardware, etc.)*. These rules are subject to change based on technology and security configuration changes.

1. Administrative level access is prohibited.
2. Enterprise Geodatabases hosted on CCGISC Infrastructure are limited to one data owner.
3. A Member Agent may be granted access to Member Agency data hosted on the CCGISC Infrastructure upon request of Member Agency. Access by a Member Agents is only allowed from the internal network of the Member Agency.
4. Member Agent access to Member Agency data hosted on the CCGISC Infrastructure will be supplied with a database connection file - passwords will not be provided.
5. Database connection files to any Enterprise Geodatabase housed on CCGISC Infrastructure shall not be published. This applies, but is not limited to, Portal accounts.
6. Member Agents shall not be provided direct access to CCGISC Data. Appropriate access to CCGISC Custodial data shall be provided to Member Agents. The data will typically be supplied to Member Agents as outlined below:
    - ***MEMBER AGENCIES THAT UTILIZE THE CCGISC INFRASTRUCTURE, SPECIFICALLY ARCGIS PORTAL OR ARCGIS ONLINE:*** CCGISC shall be responsible for publishing CCGISC Custodial Data and shall grant appropriate access to the published services.
    - ***ALL OTHERS***: CCGISC Custodial Data shall be copied to the Member Agency Enterprise Geodatabase and clipped to an area not greater than the ETJ. This may be automated and scheduled. Member Agents may publish the supplied CCGISC Custodial data following the rules contained herein.

7. Users shall not be allowed to collect, store, or process large amounts of data that will strain or overburden the CCGISC Infrastructure. As such, a variety of Enterprise features and functions are expressly prohibited without expressed written permission from the CCGISC Director. These include, but are not limited to, the following:
    - File Attachments
    - Raster Datasets
    - Published Geoprocessing Tools
    - Location Tracking
    - Data Syncing Tasks
8. No published service containing CCGISC Data or data hosted on the CCGISC Infrastructure shall be shared publicly. Views of the services may be shared publicly when URL restrictions are applied. The restrictions must limit the usage of any published data in a manner that prohibits consumption outside of the member organization. Exceptions to this rule may be granted with written permission from the CCGISC Director.
9. CCGISC Data, in any form, may not be downloadable.
10. Users that publish services from CCGISC Infrastructure must provide CCGISC staff access to source maps, data, and connection files used to publish the services. The source maps and connection files must be organized in an agreed upon structure.
11. Users that publish 1) CCGISC Data in any form, 2) data stored on the CCGISC Infrastructure or 3) data to the CCGISC Infrastructure must complete training supplied by CCGISC staff.