

FGDC Homeland Security Working Group

Guidance Subgroup Report

HIFLD, January 29, 2008

Larry Baucom, HIFLD staff

757-893-6061

baucom_larry@bah.com



- **Chartered** in April 2007 as follow-on to the Guidelines Subgroup (2003-2005) to serve as the focal point for the preparation of recommendations concerning guidance, policy, and process required to ensure that geospatial information technologies support the strategic goals of homeland security (HLS) and homeland defense (HLD) as defined in the FGDC HSWG charter.
- **Purpose** is to initiate draft FGDC policy guidance on issues needing attention to effectively institute or enable the National Spatial Data Infrastructure (NSDI) in the HLS/HLD arena.
- **Functions** as a clearinghouse and action team on guidance, policy, and process issues requiring FGDC attention that are raised by HSWG member agencies or by interagency working groups such as the Homeland Infrastructure Foundation Level Working Group (HIFLD).



- **Identifying**, through FGDC member input or recommendations of other agencies or relevant interagency working groups, those **issues** for which resolution would be facilitated by the promulgation of FGDC guidance, policy, or process change.
- **Developing and implementing guidelines** for the identification, dissemination, and security (web-served or other) of geospatial data that are or may be determined to be Homeland Security-sensitive.
- Assisting in the development and publication of process and policy guidelines applicable to homeland security data
- **Recommending** establishment of, additions to, or changes of homeland security-related NSDI data themes and their lead agencies to the FGDC Steering Committee.
- Compiling **process or policy “best practices”** and posting them for promotion on the FGDC HSWG web site.



- Those Federal agencies that, as part of their mission, collect or finance the collection of geospatial data that are applicable to the HLS/HLD missions;
- Those Federal agencies that are legislatively mandated to directly apply these data (e.g. agencies specified in the National Response Plan and relevant Homeland Security Presidential Directives) in support of the HLS/HLD missions;
- Those organizations holding HLS/HLD responsibilities, defined as HLS/HLD stakeholders, affected by HLS/HLD related geospatial information sharing models and processes.
- CURRENTLY
 - Mike Lee (DHS GMO) and Larry Baucom (HIFLD/ DOD) co- chairs
 - Members from DOE, FCC, DOJ, DOT, NSGIC, DHS LLIS, GSA, OSD DISDI, NGB, DOI, USGS, DHS FEMA



- **Develop link analysis to discover candidate issues requiring FGDC guidance. Develop guidance for FGDC approval. Ongoing action.**
 - Standardize “access” and “use” constraint verbiage for HLS metadata in work. Coordinating with ISE initiative.
 - Data Sharing Guidance development. Initial draft due in Feb 08.

- **Recommend NSDI HLS/HLD data themes and corresponding proposed lead agencies to the FGDC Steering Committee.**
 - Issue of missing data theme leads for HSPD-7 sectors and recommendations briefed to FGDC Coordination Group January 15. Action to work with FGDC Data Life Cycle Group to cross walk how data theme and SSA leads relate and coordinate with LOB work plan for change to A-16.



- **Availability of trans border data (Mexico/ Canada) for HLS/ Law Enforcement purposes at Fed, State and local levels.**
 - Developed GOS HLS Community of Interest Pages as a Clearinghouse for Trans Border Data Discovery and Access.
http://gos2.geodata.gov/wps/portal/gos/kcxml/04_Sj9SPykssy0xPL
 - Researching opportunity to include in grant language
 - Monitoring inclusion of trans border data in HSIP Freedom
- **Post initial Effective Practices for HLS Grantees. Solicit, collect, and post HLS Composite Layer Effective Practices and Metadata Guidance.**
 - Teamed with DHS LLIS project and developed GIS Effective Practices Field Collection Initiative to solicit effective practices from field agencies. Awaiting release.
- **Ascertain effectiveness of, and lessons learned from, “Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns”**
 - Revision due Jun 2010





Homeland
Security


Guidelines for Data Access in Response to Security Concerns

Mike Lee - FGDC Homeland Security Working Group

HIFLD - January 29, 2008



- **Look Familiar?**



**Guidelines for Data Access in
Response to
Security Concerns**

Michael Domaratz, Co-chair
Homeland Security Working Group

HIFLD – Feb 2005



- **Refresher - Problem and Objective**

- **Concerns**

- *Public access to geospatial data might increase vulnerability to attack*
- *After September 11, Federal agencies and other organizations took different actions (withdrawal, sanitize, no change in access)*
- *What safeguards are sensible and at what cost?*

- **Objective**

- *Provide guidelines for evaluating the need to reduce or eliminate public access to sensitive geospatial data*
- *Need a “community” solution*



- **Refresher - Rand Report**

- *“Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Data”*
- *Framework for making decisions about access*
 - *Usefulness to an adversary*
 - *Uniqueness of the information*
 - *Balance security costs with societal benefits*
- *Available through <http://www.rand.org/publications/MG/MG142/>*



■ *Refresher - How Guidelines were Developed*

○ *The FGDC Homeland Security Working Group:*

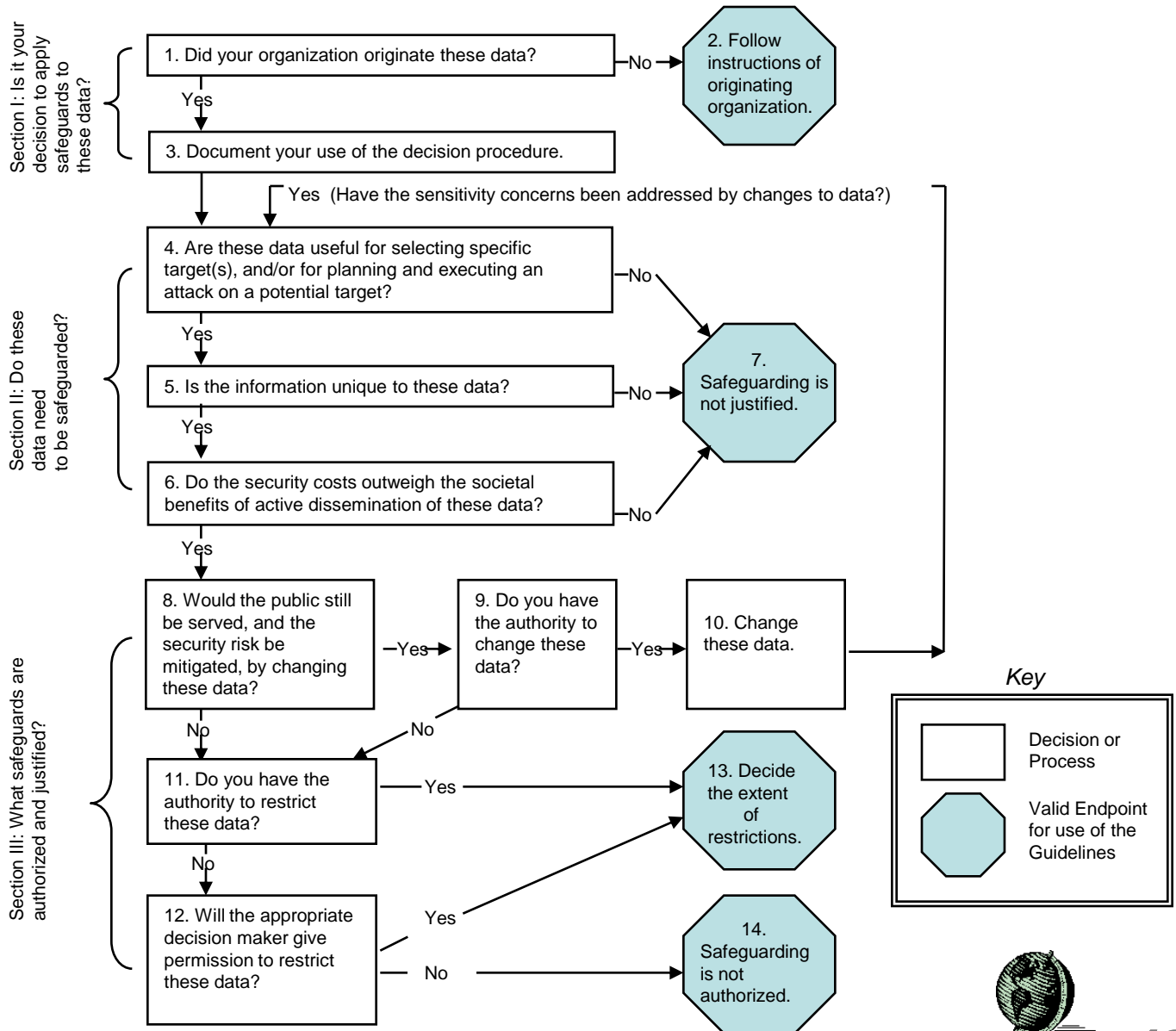
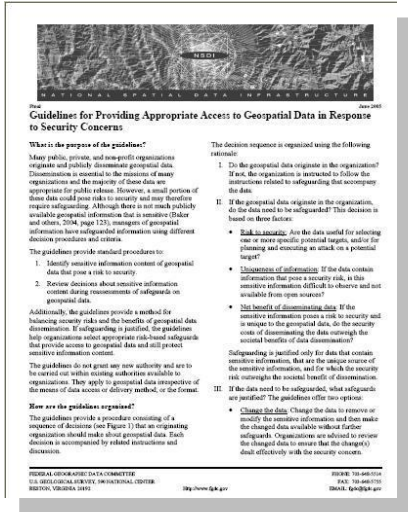
- *Reviewed laws, executive orders, circulars, and other documents to discern principles and broad policies*
- *Analyzed organizations' guidelines to understand how the concern has been addressed*
- *Interacted with RAND study personnel*
- *Took advantage of NSGIC guidelines*
- *Used members' knowledge and contacts*

○ <http://www.fgdc.gov/policyandplanning/Access%20Guidelines.pdf>

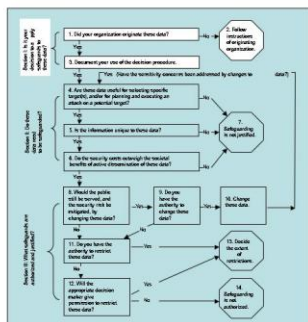
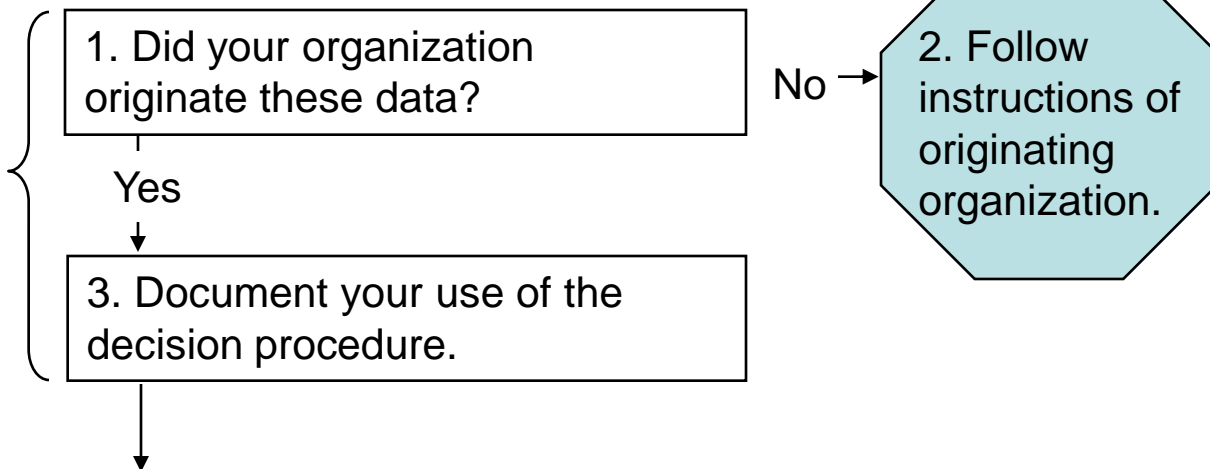


- **Refresher - Guidelines Overview**
 - *Section I: Is it your decision to apply safeguards to these data?*
 - *Section II: Do these data need to be safeguarded?*
 - *Usefulness*
 - *Uniqueness*
 - *Security cost and societal benefit*
 - *Section III: If so, what safeguards are authorized and justified?*
 - *Change data (have authority?)*
 - *Restrict access (have authority?)*





Section I:
Is it your decision to apply safeguards to these data?



Section II:
Do these data need to be safeguarded?

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

Yes

5. Is the information unique to these data?

Yes

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

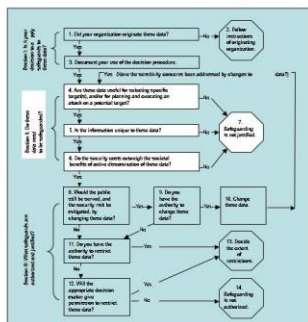
Yes

No

No

No

7.
Safeguarding is not justified.



Section II: Do these data need to be safeguarded?

Usefulness:

• *Is the publicly accessible geospatial information useful for target selection purposes?*

—Does the information provide details that are not common knowledge, which identify particular critical sites?

—Does the information provide specific and accurate geo-location coordinates?

—Does the information provide insights on choke points within a critical infrastructure sector?

—Is the information relatively current, or is it dated (and does that matter)?

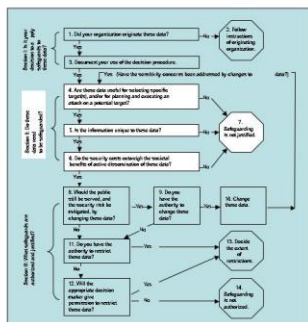
• *Is the geospatial information useful for attack planning purposes?*

—Does the information identify key internal features?

—Does the information provide details on facility layout and vulnerabilities?

—Does the information provide insights into operational practices at critical sites?

—Is the information relatively current, or is it dated (and does that matter)?



Section II:
Do these data need to be safeguarded?

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

Yes

5. Is the information **unique** to these data?

Yes

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

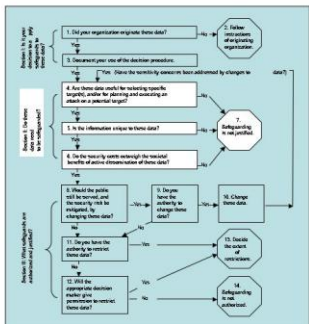
Yes

No

No

No

7.
Safeguarding is not justified.



Section II:
Do these data need to be safeguarded?

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

Yes

5. Is the information unique to these data?

Yes

6. Do the security **costs** outweigh the societal **benefits** of active dissemination of these data?

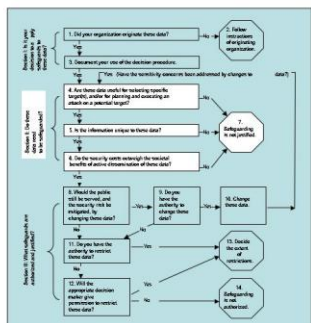
Yes

No

No

No

7.
Safeguarding is not justified.



Section II: Do these data need to be safeguarded?

Security and Societal Benefits and Costs:

- *What are the expected security benefits of restricting public access?*

—*Increase the difficulty of potential attackers to undertake effective attacks against U.S. critical sites?*

—*Damage costs avoided or minimized if public access to certain geospatial information is restricted?*

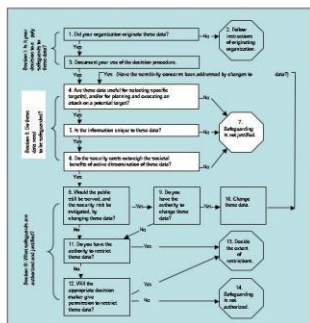
- *What are the expected societal costs of restricting public access to this geospatial information?*

—*Do people need this information for physically accessing (or avoiding) particular locations?*

—*Public safety purposes (e.g., pipeline locations, hazardous chemical facilities)?*

—*Is the information publicly available for legal reasons (e.g., community right-to-know laws)?*

(Cont...)



Section II:
Do these data need to be safeguarded?

Security and Societal Benefits and Costs:

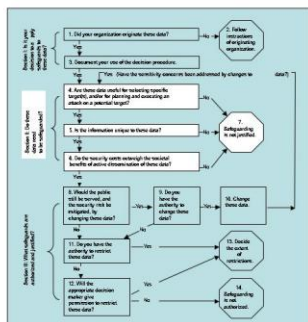
- *What are the expected societal costs of restricting public access to this geospatial information? (Cont...)*

—Who are the main users of the information (e.g., businesses, state or local governments, universities, NGOs, the general public)? How much do they depend on publicly accessible information?

—Do domestic users have alternative sources of comparable information at similar costs?

—What are the estimated costs to primary users if public access to this information is restricted?

- *What are the expected costs to the information supplier for imposing restrictive measures on information access?*



Section II:
Do these data need to be safeguarded?

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

Yes

5. Is the information unique to these data?

Yes

6. Do the security costs **outweigh** the societal benefits of active dissemination of these data?

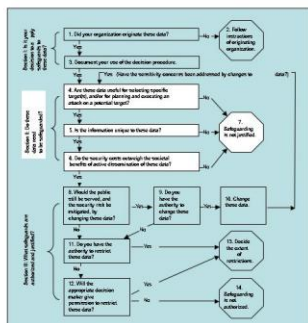
Yes

No

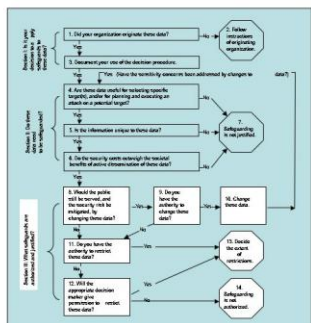
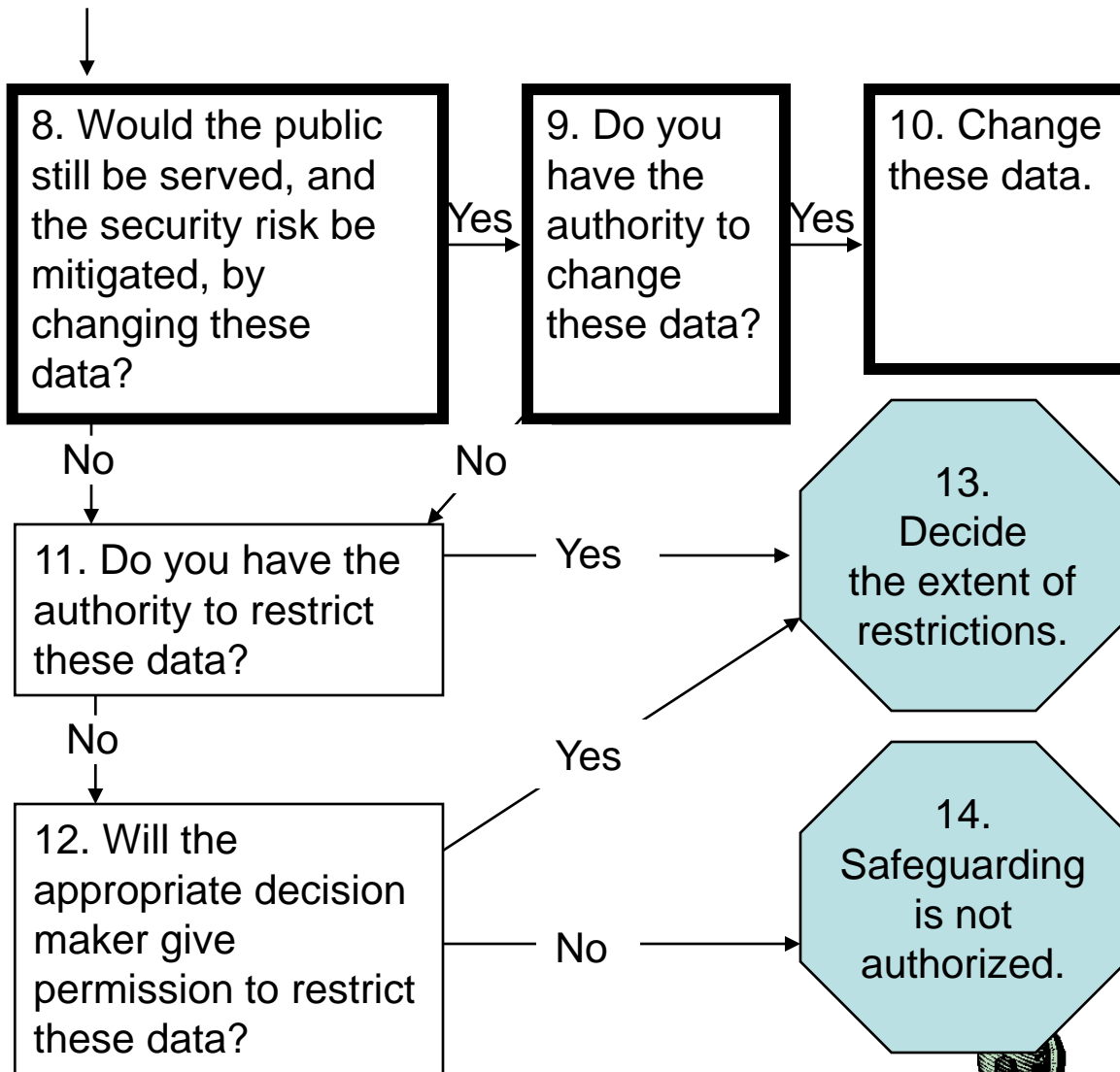
No

No

7.
Safeguarding is not justified.



Section III:
What safeguards are authorized and justified?



Section III:
What safeguards are authorized and justified?

4. Data useful, unique, ...

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

9. Do you have the authority to change these data?

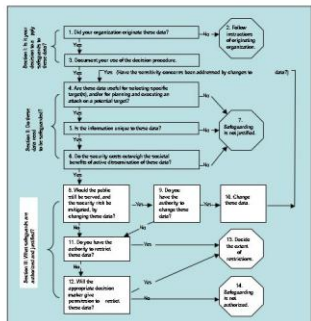
10. Change these data.

11. Do you have the authority to restrict these data?

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

13. Decide the extent of restrictions.

14. Safeguarding is not authorized.



Section II:
Do these data need to be safeguarded?

Changed Data

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

Yes

5. Is the information unique to these data?

Yes

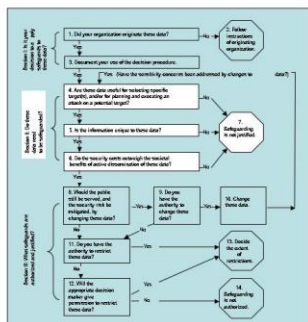
6. Do the security costs outweigh the societal benefits of active dissemination of these data?

No

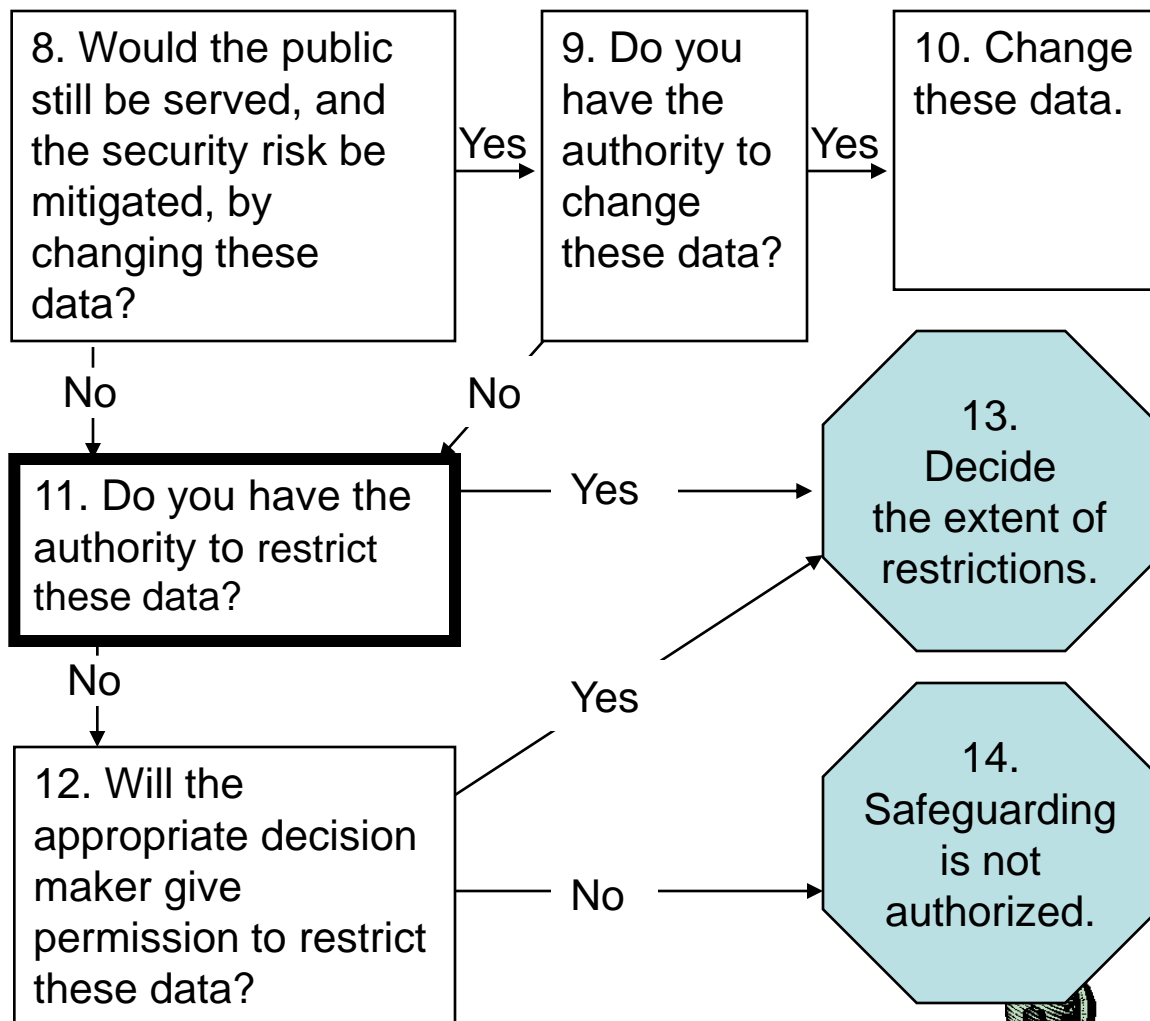
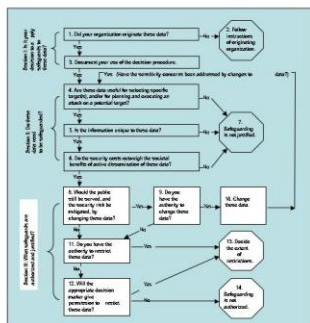
No

No

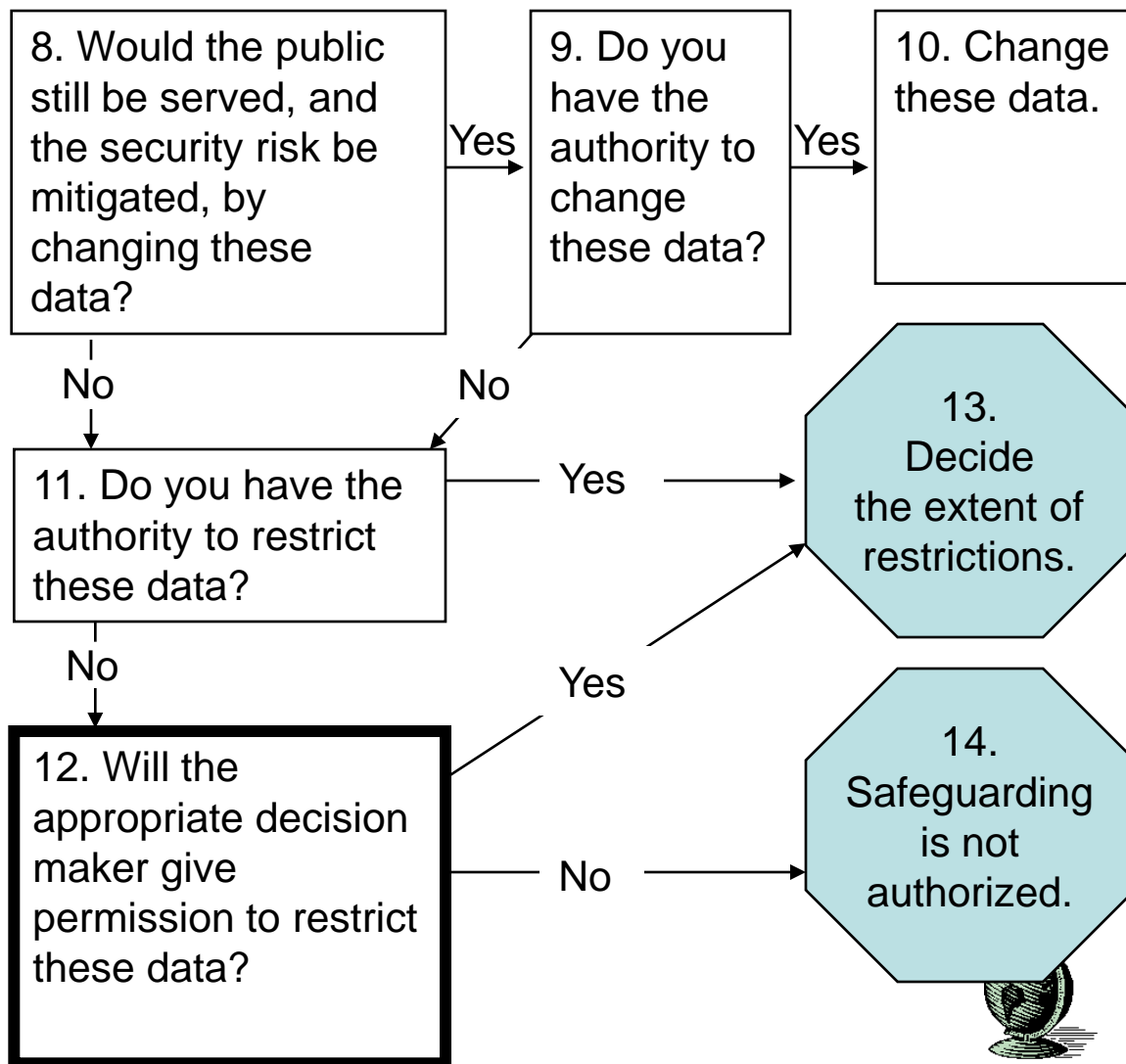
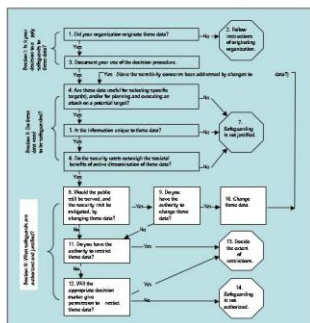
7.
Safeguarding is not justified.



Section III:
What safeguards
are authorized
and justified?



Section III:
What safeguards
are authorized
and justified?



■ *Take Aways*

- *Data Providers/Originating Organizations should consider using these Guidelines*
 - *Contributes to a Community Solution aimed at Coherence and Consistency regarding security assessments of Geospatial Information*
 - *Consider new restrictions*
 - *Modify existing safeguards*
- *Defer to Originating Organizations' decisions on safeguards*
 - *Resist applying safeguards to other organizations' data*



■ Documents

Guidelines for Data Access in Response to Security Concerns

- <http://www.fgdc.gov/policyandplanning/Access%20Guidelines.pdf>

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

- <http://www.rand.org/publications/MG/MG142/>

FGDC Homeland Security Working Group

- http://www.fgdc.gov/participation/working-groups-subcommittees/hswg/index_html

■ Contact Information

Michael P. Lee

Senior Geospatial Liaison

Dept of Homeland Security

Geospatial Management Office

michael.p.lee@dhs.gov

Larry Baucom

OASD-HD

HIFLD WG Staff

baucom_larry@bah.com

