

Part B

WORKING GROUP REPORTS – Homeland Security (USGS/NIMA)

1. Program/Activity Name: **Homeland Security Working Group**
2. What are the specific federal programs this data supports? **The working group ensures that the National Spatial Data Infrastructure (NSDI) supports all elements of homeland security, including the preparation for, prevention of, protection against, response to, and recovery from threats to the nation's population centers and critical infrastructures. Member agencies' programs employ and provide geospatial data that enable readiness for, response to, and recovery from events.**
3. Uses of Data: How does your data benefit customers and support agency missions? **Timely, accurate information easily accessed and capable of being shared across federal, state, and local political jurisdictions is fundamental to the decision-making capability of those responsible for homeland security. Absent the real-time ability to visualize activity patterns quickly, map locations, and understand the multi-layered geospatial context of emergency situations, homeland security will not be achieved.**
4. Charter/Plan: Do you have a current charter or plan for collection? If so - please describe (include how recently the charter/plan was implemented and whether it is in need of update). **Charter approved May 2002.**
5. Metadata Status: Is metadata discoverable and served through the NSDI Clearinghouse? What percentage of this theme's data has metadata and is in a Clearinghouse node? **Not applicable.**
6. Standards: What is the status of this theme's data, process, transfer, and classification standards? **Map symbology: Use of different map symbols for the same information slows and degrades communication, especially when many organizations need to work together. A standard would establish a common set of symbols for features that are commonly portrayed for homeland security applications. The working group identified symbols needed to support emergency response as the highest priority, and organized a subgroup to examine relevant work by member agencies, to identify issues to be resolved in developing a standard, to develop a plan, and to begin work on a standard.**

Information content: Early identification of "common" minimum information content that supports homeland security activities, especially that for critical infrastructure, will encourage convergence and enable sharing among those charged with developing data. To begin work on this item, the working group is reviewing a set of "minimum essential data" compiled by two member agencies.

The working group has identified the need for work on extensions to metadata standards that might be needed to support homeland security (such as special data handling instructions and data sharing restrictions), and on interface specifications for systems that support homeland security applications.

7. Progress: List FY 2001/2002 activities/progress to date (quantify where possible).
Policy concerns:
 - **Developed a position paper titled "Homeland Security and Geographic Information Systems" that identified factors preventing effective use of data, including:**
 - **Lack of standards, data frameworks, and E-911 support.**
 - **Need to promote and provide resources for collaborative relationships.**
 - **Lack of uniform approaches to homeland security that rely on standardized data and systems.**

- Need for mobile GIS resources that can be available within 12 hours of an event.
- Tracking changes in public access to Federal geospatial data caused by Federal agencies' security concerns. The working group is following the progress of a RAND Corporation study, sponsored by two member agencies, that is evaluating the relationship between publicly available geospatial data and vulnerabilities of critical infrastructure and other potential targets.

Standards: See item 6.

Outreach and education:

- Members provided briefings on the importance of geospatial data to homeland security efforts at the fall 2002 meetings of the National States Geographic Information Council and the Federal Geographic Data Committee, and at a September 2002 "Homeland Security Infrastructure Program (HSIP) Leaders' Summit".

8. Policy: Do you have a formal agency policy in place for full and open access or data sharing? Are you able to fulfill this policy and provide public access with your current agency financial resources as allocated or are you in pursuit of collaborative federal partnerships to support data access? **Not applicable. See item 7 on working group activities related to changing Federal agencies' approaches to public access to data caused by homeland security concerns.**

9. Are there areas or issues regarding lead responsibilities for spatial data themes that require attention, or lessons-learned that you would like to share with others? Please describe.

The working group has identified the following important issues:

- **Process for "fast and broad" consensus** – Homeland security activities include a large number of public, private, and non-profit organizations whose responsibilities range from local to international in geographic scope, and whose potential roles and contributions vary significantly in type and size. Achieving consensus among these different parties is a challenging task. This challenge is compounded by the urgency of the activity, which requires fast action to stay ahead of this quickly developing field.
- **Need for continual resources for standards** – As a consequence of the factors described above, standards that support homeland security applications are likely to require continual support for development and implementation. In part this is a consequence of the need for "fast and broad" consensus. This approach likely will result in a triage of action, in which standards will be first sought and achieved for those items on which consensus can be reached quickly. Meanwhile, more contentious issues will require additional attention. For items for which no single solution can be found, it will be helpful to support the community through registries of solutions. In addition to support for this baseline of standards, resources will be needed for outreach, training, and implementation of standards, as well as to ensure that the standards are kept current with new and maturing applications.
- **Security concerns** – A unique factor added by homeland security applications is the need for confidentiality for some information and processes. Challenges in this area include markedly different views regarding what is sensitive and the authorities for protecting information, and the contradictions between the need to restrict access to information and to provide for broad participation in data development, data sharing, and other needed collaboration.