

Cugir : Security Assessment Procedure

This page last changed on Aug 31, 2005 by [gss1](#).

The material and methodology in this document was drawn primarily from the Rand Corporation's report, [Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information](#). The complete report is available online: <http://www.rand.org/publications/MG/MG142/>.

Security criteria

The two primary criteria for evaluating the risk posed by a dataset are its usefulness to would-be attackers, and its availability from other sources.

Usefulness:

Is the information useful for target selection or location purposes?

- Does the information provide details that are not common knowledge, which identify particular critical sites?
- Does the information provide specific and accurate geolocation 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 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)?

Ranking

Assign a score of 1 to 5, based on the following criteria:

- 5, high: information is critical (an attack would not be possible without it)
- 4, medium: information potentially useful, but not required
- 3, low: information probably not likely to be useful, but might be "nice to have"
- 2, very low: information not likely to be useful
- 1, none: information not at all relevant

Uniqueness / availability of alternatives:

Is the information readily available from other geospatial and non-geospatial information sources?

- Web sites, including archived internet sites?
- Hard-copy maps?
- Textual documents?
- GIS databases?

Is direct access or direct observation by potential attackers feasible?

Can attackers' information needs be met using general engineering and technical expertise?

Methods for assessing uniqueness / availability of information:

- key word search on the internet
- directed search of key geospatial clearinghouses
- consultation with knowledgeable individuals
- search for alternate (non-GIS) sources of information

Ranking

Assign a score of 1 to 4, based on the following criteria:

- 4, high: an equivalent amount of information is available from many sources, it is easy to recreate the information, and the information can be easily acquired by direct observation (for example, information is available in road maps, phonebooks, and on multiple web sites)
- 3, medium: some alternative sources are available, it takes a higher level of analysis to derive or access the information, and direct observation is not easy, even though public access is not completely restricted
- 2, low: only a few alternative sources exist, the information is not readily accessible by direct observation, and it is not easy to re-create the information
- 1, none: no alternative sources exist