



Knowledge Management: KM Portal

The National Infrastructure Simulation and Analysis Center (NISAC) a program under the Department of Homeland Security's (DHS) Infrastructure Protection/ Risk Management Division (IP/RMD), provides advanced modeling and simulation capabilities for the analysis of critical infrastructures, their interdependencies, vulnerabilities, and complexities. These capabilities help improve the robustness of our nation's critical infrastructures by aiding decision makers in the areas of policy analysis, investment and mitigation planning, education and training, and near real-time assistance to crisis response organizations.

NISAC is a partnership between Sandia National Laboratories (SNL) and Los Alamos National Laboratory (LANL), integrating the two laboratories' expertise in infrastructure disruption/vulnerability modeling and simulation..

Knowledge Management

NISAC analysts and modelers require vast amounts of data and information for their critical infrastructure interdependency work. Knowledge management provides an access-controlled, organized, and searchable view on the data for rapid retrieval and update through a suite of web-based tools and programmatic interfaces. The suite of tools currently under development include the KM Portal, the Simulation Library, the Event Library, the Web Search Capture Tool, and the Critical Infrastructure Protection Metadata Database.

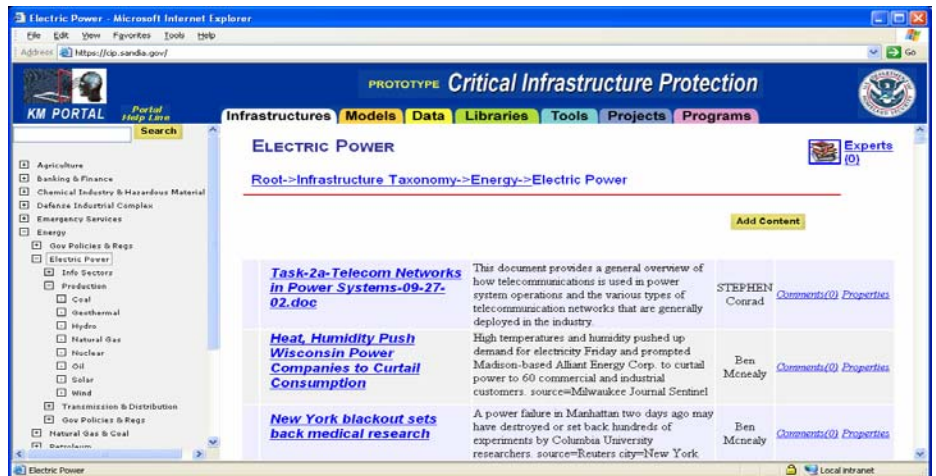
Knowledge Management Portal (KM Portal)

The KM Portal is a one-stop shop where NISAC analysts, modelers, and administrators can contribute and share information. It provides a comprehensive, integrated view of critical infrastructure protection information, including:

- documents & reports
- models, simulations, analyses & data sets
- project and program information
- policies

The KM Portal is a web application with easy access through a web browser, but access is restricted by firewall and access controls. Collaborators and partners can gain access to the KM Portal from their institutions by simply contacting a member of the KM Portal network management team.

Tools accessible through the KM Portal include web interfaces to the various simulation and analytical models, the Critical Infrastructure Protection Metadata Database (CID), the Simulation and Event Libraries (SimLib and EventLib), the Web Search Capture Tool (WeSCaT), the Policy Library, CVS, and Bugzilla.



The KM Portal provides a comprehensive, integrated view of CIP knowledge, including documents, reports, simulations, analytical models, data sets, project and program information, policies, and analyses.



Taxonomies

Knowledge in the KM Portal is organized via a set of taxonomies, each of which provides a different perspective or view on the data. Modelers and analysts can browse knowledge organized by infrastructure decomposition, project organization structure, or by administrative program structure.

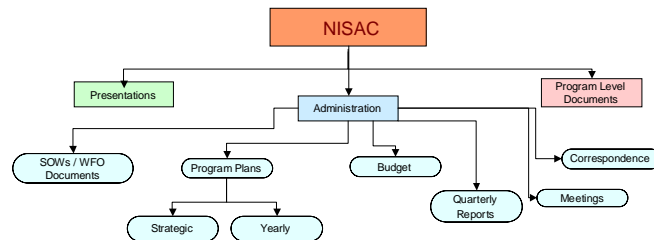
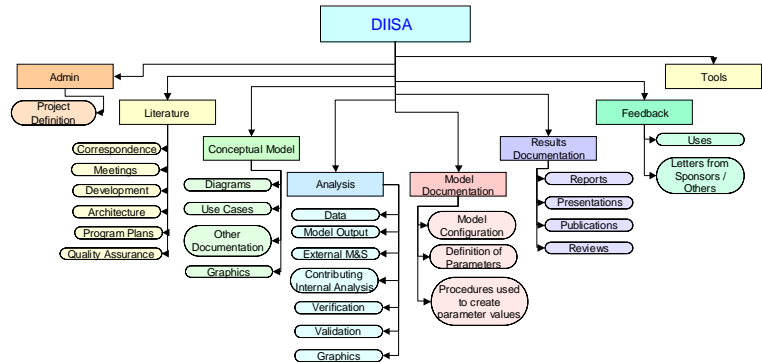
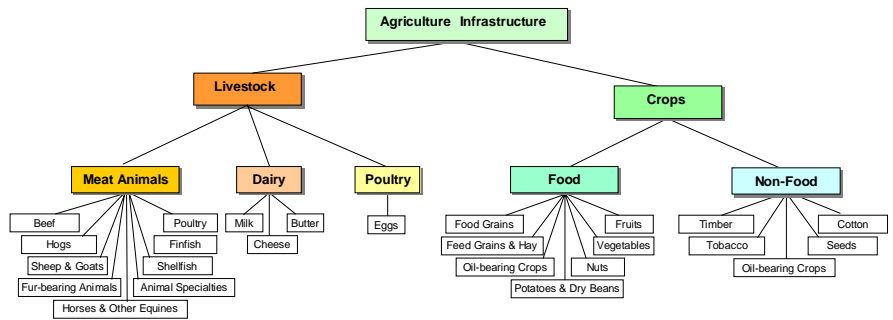
A single document or knowledge element can be associated with multiple nodes within a given taxonomy and/or nodes spanning multiple taxonomies, which exposes it through multiple viewpoints. The taxonomies provide a common vocabulary for describing and organizing critical infrastructure protection knowledge in the KM Portal and across all of the Knowledge Management tools.

Experts

Each node in each taxonomy has a list of experts associated with it. Modelers and analysts requiring access to a list of experts who are knowledgeable in a particular topic can find this list quickly in the KM Portal by selecting the appropriate taxonomy node.

Search

All knowledge in the KM Portal is searchable via metadata, including keywords, title, infrastructure sub-sector, region, description, etc.. Documents in common formats (Word, PowerPoint, PDF, etc.) in the KM Portal can also be searched via their text content.



Knowledge in the KM Portal is organized via a set of taxonomies, each of which provides a different perspective or view on the data.

Access Controls

Access to knowledge in the KM Portal is controlled at the document or knowledge element level using a group-based need-to-know authorization mechanism. Only users who are members of one of the specified groups associated with a document can have access to that document.



Contacts:

Jon MacLaren
DHS-IP
(202) 282-8719; e-mail:
jon.m.maclaren@dhs.gov

Theresa Brown
Sandia National Laboratories,
(505) 844-5247; email:
tjbrown@sandia.gov