CISA GATEWAY HURRICANE SUPPORT

OVERVIEW

Our Nation's critical infrastructure is essential to sustaining our security, the economy, and the American way of life. The Cybersecurity and Infrastructure Security Agency (CISA) leads the coordinated national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

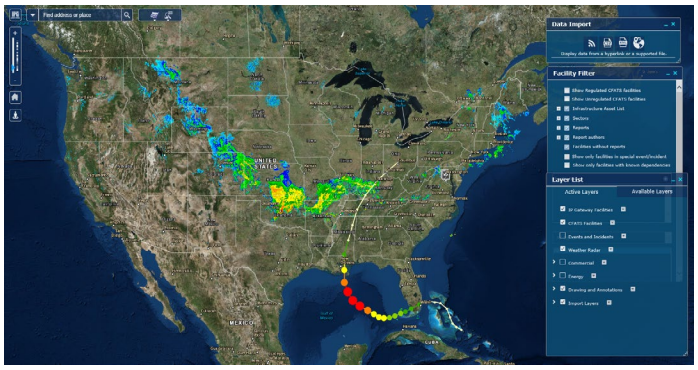
The CISA Gateway is a single interface through which CISA mission partners can access a large range of integrated critical infrastructure data, information, and tools.

- Enables users to collect, manage, protect, and share infrastructure data through a single platform, resulting in more effective data analysis.
- Maximizes the availability of data for cross-government sharing.
- Offers advanced data analysis and planning capabilities in support of day-to-day operations, special events and exercises planning and incident response.

There are multiple ways that the CISA Gateway and the tools and data housed within it can be leveraged in support of domestic special event and incident (e.g., hurricanes) preparation and response actions. Two primary tools to assist with this are the MapView and Special Events and Domestic Incident Tracker (SEDIT) tools.

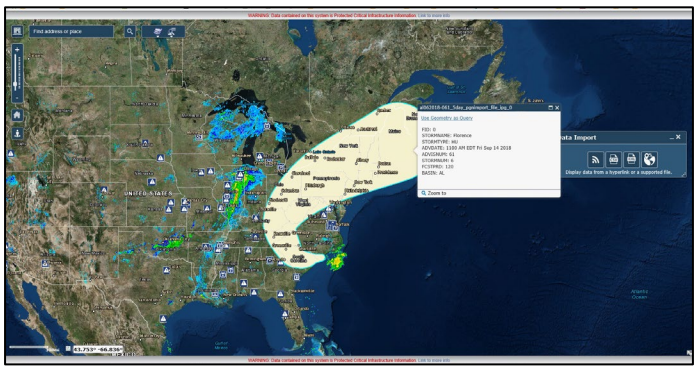
MAPVIEW

MapView is an interactive and robust geospatial data viewer that provides visualization of critical infrastructure resources in a geospatial context, allowing access to numerous data layers for specific States, counties, or cities and offers a wide range of geospatial mapping capabilities. MapView displays critical infrastructure facilities visited by Federal, State, Local, Tribal, & Territorial (FSLTT) homeland security professionals and allows users to interact with facility dependencies and cascading impacts analysis capability. MapView provides a layered geospatial view of critical infrastructure, including:

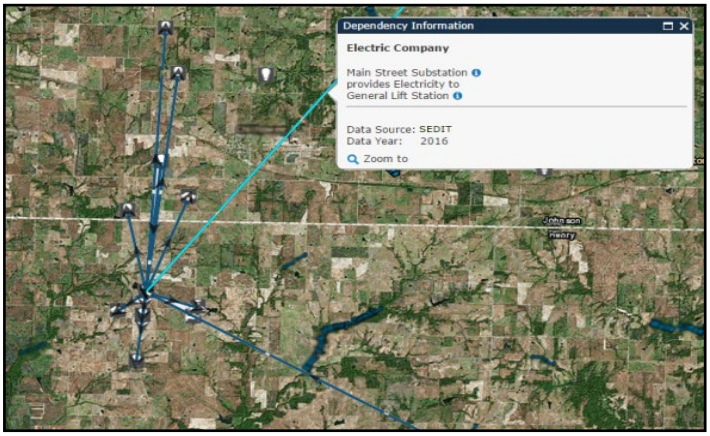


- Static layers, such as facilities-by-sector, daytime/nighttime population, or street-view pictures.
- Dynamic layers, such as current wildfire or weather elements.

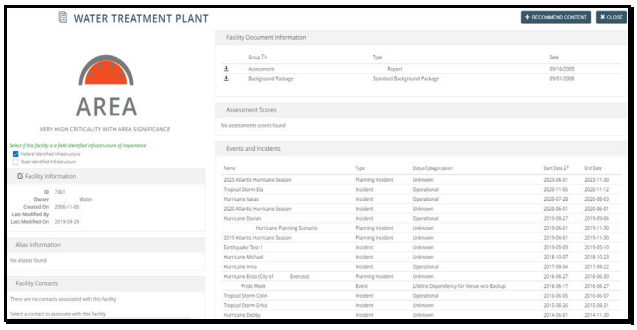
Within MapView, you can utilize polygons to create a query area, or you can overlay an "GeoRSS," "CSV," "KML/KMZ," or "Shapefile", e.g., hurricane cone of uncertainty, to query an area to identify critical infrastructure facilities that are within the query zone.

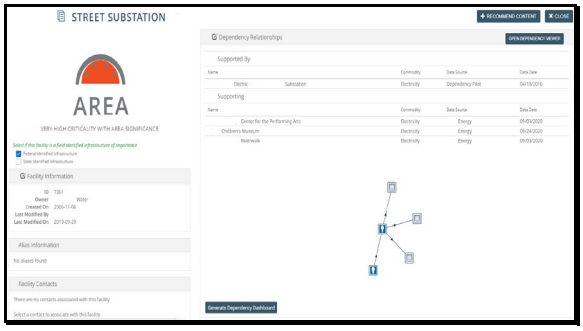


DEPENDENCIES & CASCADING IMPACTS



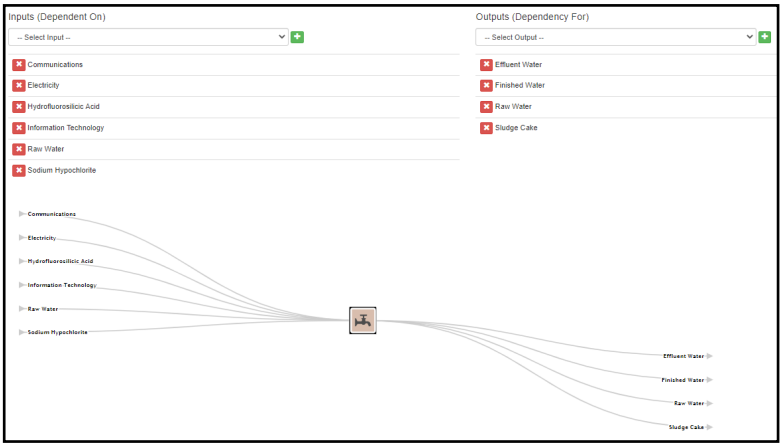
The Dependency Tool provides a rapid visual representation of the relationships and dependencies between critical infrastructure. These capabilities provide increased knowledge about critical infrastructure dependencies and enable improved stakeholder support for special events & incidents planning and decision-making processes. The Dependency Tool integrates several CISA Gateway applications. The methodologies produce a more streamlined interface for approved users to capture, enter, analyze, visualize, and manipulate dependency information. One or more facilities can have their upstream and downstream dependencies displayed along with simulating a compromise of a facility and viewing the cascading impacts over time for those facilities along with their upstream and downstream dependencies.





Using the Infrastructure Data Taxonomy (IDT) as a framework, the Dependency Profile Editor stores the master general definitions about the inputs and outputs of a critical infrastructure facility, system, or area. The general profiles include established characteristics of critical infrastructure (e.g., inputs and outputs). This capability is also integrated into the dependency surveys found in the Surveys & Assessments area, automatically populating a base layer of data if no information currently exists for a specific facility. If an assessed facility has multiple taxonomy assignments, all general inputs and outputs will be prepopulated into the survey. The Dependency Profiles feed the dependency capability that is integrated into the facility dependencies.

Housed within the Digital Library facility records, the Dependency Capabilities of a critical infrastructure facility can be viewed. The dependency Tools provide a rapid visual representation of the relationships and dependencies between critical infrastructures for both upstream and downstream relationships and the input and output of dependent commodities supporting each of those relationships. This is accessed using the Dependency Viewer.

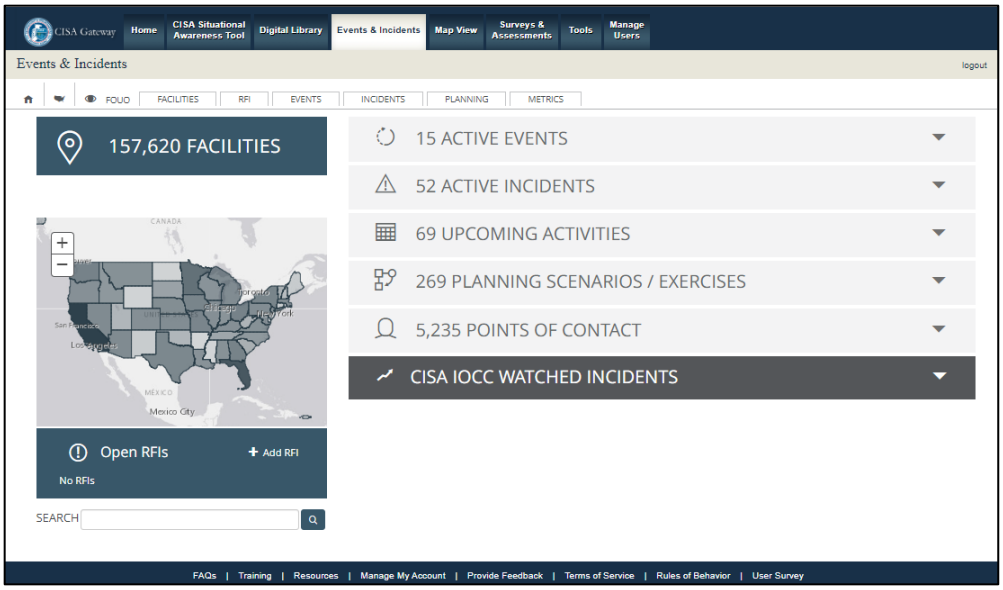


SEDIT

SEDIT is part of CISA Gateway's integrated system of data collection, analysis, and response tools designed to support efforts to strengthen critical infrastructure security and resilience. The tracker is a powerful Web-based infrastructure analysis application used by homeland security professionals at all levels of government to optimize steady state, special event, and domestic incident support capabilities at the national, regional, State, local, tribal, and territorial levels. The tracker's scalable, integrated, and intuitive design enables users to make risk-informed decisions by leveraging infrastructure collection, prioritization, dependency/ interdependency analysis, mapping, and visualization features during planning, protection, response, and recovery.

- Improves information sharing between Federal, State, and local partners, service providers, facility owners/operators.
- Enhances DHS's ability to analyze data and produce improved protection and resilience measures.
- Presents streamlined and user-friendly functionality in support of special events, domestic incidents, planning scenarios, and exercises.
- Increases efficiency in the field by cross-feeding data between steady state (baseline), special events, and domestic incidents.
- Historical information of previous event, incident, and exercise scenarios is available for analysis and utilization with future events, incidents, and exercises.

SEDIT enables the users to bring in multiple facilities and their dependent facilities into a planning scenario to facilitate a scenario-specific facility criticality and significance and prioritize their protection or restoration during an event or incident. SEDIT scenarios can be built to support pre-planning for an event or incident, response and recovery for an event or incident, or in support of a mock event, incident, or exercise.



RESOURCES

If you would like to learn how the CISA Gateway can support your organization's homeland security efforts, to inquire about eligibility for accessing the CISA Gateway, or if you would like to establish access to the system, please contact the CISA Gateway Program Office at CISA-Gateway@mail.cisa.dhs.gov.

To learn more regarding the CISA Gateway, visit cisa.gov/cisa-gateway.