CISA GATEWAY FEATURES

OVERVIEW

The CISA Gateway is an information system that provides a single interface through which DHS mission partners can access a range of integrated critical infrastructure information, tools, and features that facilitate the collection, analysis, and dissemination of critical infrastructure data.

SURVEYS AND ASSESSMENTS

Surveys and Assessments provides access to non-regulatory surveys and assessments utilized by Cybersecurity and Infrastructure Security Agency (CISA) Protective Security Advisors (PSAs) and their State, Local, Tribal, and Territorial (SLTT) counterparts during visits to critical infrastructure facilities. Surveys and Assessments is designed to gather critical infrastructure data, including security, vulnerability, threat, and consequence information by providing templates that range from high-level surveys to comprehensive in-depth assessments so PSAs and SLTT mission partners may conduct various visits and assessments (e.g., Security at First Entry (SaFE), Infrastructure Survey Tool (IST), and Dependency Survey Tool (DST)) and in addition to storage and protection of the data while associating it with Critical Infrastructure Facilities within the CISA Gateway. Additionally, Surveys and Assessments provides the user with the ability to:

- Schedule a site visit
- Add assets/facilities to the system
- Access online & offline assessment templates
- Create & edit assessments
- Search assessments
- Access assessment metrics

SPECIAL EVENTS AND DOMESTIC INCIDENTS TRACKER (SEDIT)

SEDIT is a planning capability that integrates security and resilience data from facilities' surveys and assessments. Special event and incident scenarios are created to make decisions regarding the impact, protection, mitigation, response, and recovery efforts. 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. SEDIT is a powerful web-based tool and web-based infrastructure analysis application used by homeland security professionals at all government levels to optimize steady state, special event, and domestic incident support capabilities. SEDIT 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.

MAPVIEW

MapView is an interactive and robust geospatial data viewer that allows for the visualization of critical infrastructure resources in a geospatial context. Through MapView, users can access to numerous data layers for specific states, counties, or cities and offers a wide range of geospatial mapping capabilities (querying, drawing, and charting). MapView provides:

- The ability to geospatially display of critical infrastructure facilities.
- The ability to import and overlay external data sources (KML/KMZ/Shape files/HTML links).
- The ability to draw & annotate maps for planning purposes.

- The ability to create new events & domestic incidents.
- The ability to view critical infrastructure facility resource dependencies.
- The ability to simulate cascading impact scenarios to view upstream/downstream impacts to infrastructure caused by an incident (e.g., hurricanes, terrorist attack, etc.).

STAKEHOLDERS RISK ASSESSMENT MITIGATION (SRAM)

SRAM provides templates for various visits and assessments conducted by CISA Cybersecurity Advisors (CSAs) and provides the storage and protection of the data while associating it with critical infrastructure facilities within the CISA Gateway. SRAM provides the ability to schedule, conduct, and finalize cyber-focused assessments including the:

- Cyber Resiliency Review (CRR)
- Cyber Infrastructure Survey Tool (C-IST)
- External Dependency Management (EDM)

DIGITAL LIBRARY

The Digital Library is a search tool that provides the ability for a user to access thousands of documents related to critical infrastructure ranging from facility assessments to sector specific standards. Providing data management capabilities and presents information in a textual and geospatial format using a search engine. This information helps users enhance critical infrastructure protection programs prepare for and respond to incidents and events, facilitating the ability to research and analyze infrastructure security and resilience data specific to their mission needs. Digital Library provides:

- The ability to conduct searches with keyword and guided search modes.
- The ability to access records about critical infrastructure facilities and assets.
- The ability to access analytic products or guidance on assessing infrastructure.
- The ability to collaborate and share information (larger files) using “My File Shares”.

FACILITY DASHBOARDS

The dashboards provide owners and operators with snapshots of their facility’s security and resilience posture and compare those results with those of similar facilities across the Nation. The information in the dashboards, derived from completed ISTs and C-ISTs, allows owners and operators to view and modify assessment data, and develop planning scenarios. This allows them to explore potential future capital improvement options and view the impacts of the scenario-based changes to see immediate impacts on a facilities security and resilience indexes.

EXECUTIVE ORDER (EO) 13650 PORTAL

The EO 13650 portal is a geospatial mapping tool that provides federal agencies, SLTT officials, and first responders access to non-Chemical-terrorism Vulnerability Information (CVI) Chemical Facility Anti-Terrorism Standards (CFATS) data. The EO13650 portal provides:

- The ability to geospatially display and view chemical facilities.
- The ability to import and overlay external data sources (KML/KMZ/Shape files/HTML links).
- The ability to draw & annotate maps for planning purposes.

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.