

CRITICAL INFRASTRUCTURE PROTECTION



Critical Infrastructure and Key Resources (CIKR) are a component of the risk equation that traditionally has not been within the realm of the Fusion Center's core mission. That is changing as Fusion Centers begin to recognize how tightly integrated the understanding of a jurisdiction's CIKR is for deterring, disrupting, and/or mitigating threats.

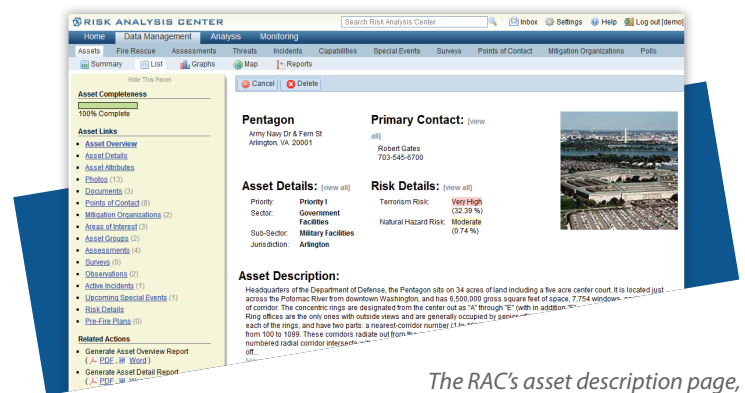
Digital Sandbox's Risk Analysis Center (RAC) provides users the ability to gather CIKR information in a single location, establish asset priority, and systematically assess asset vulnerability to and consequences of a jurisdiction's threats and hazards. This foundational database of CIKR information can be viewed geospatially, linked to external systems, and integrated with the RAC's target capabilities assessments.

RAC Fusion Integrates CIKR and Threats

Digital Sandbox's RAC incorporates CIKR vulnerability and consequence-related information into the fusion process. Built-in intelligent data collection and risk analytics enable analysts to assess asset vulnerability to locally-relevant threats and hazards, providing a regional risk picture based on current, local likelihood data.

As a secure, cloud-based application, the RAC allows users to easily and quickly update their CIKR data when faced with new vulnerability and threat information, at any location, via workstation or mobile access.

Multi-level security and role-based access features enable 100% data control, while allowing the ability to share data with private and public organizations at will, through secure channels.

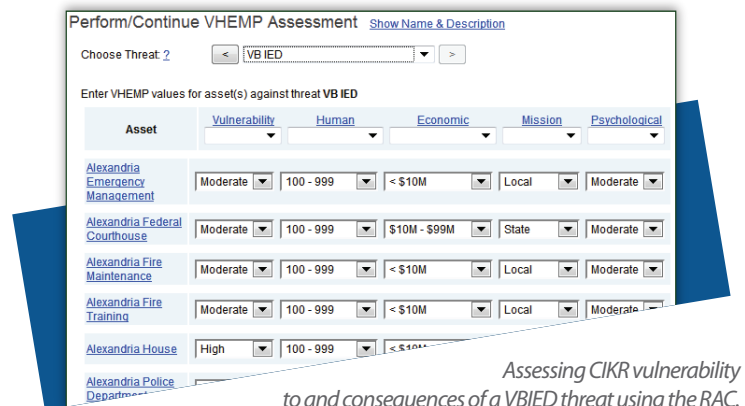


The RAC's asset description page, presenting key asset details and currently associated risk, based on threat, vulnerability, and consequence data within the system.

The RAC's CIKR Data Management

Collecting and integrating critical asset data is a core function of the Risk Analysis Center. The relational database inherent in the RAC captures a universe of key asset data that, when used by the internal risk analytics, can inform multiple aspects of risk for a given jurisdiction.

- **PCII and C/ACAMS Integration:** The RAC supports the requirements established for interacting with Protected Critical Infrastructure Information (PCII) data and for transferring asset data into the C/ACAMS system, according to Federal guidelines.
- **Security Features:** The RAC contains multiple types and levels of security. Administrator-configurable permission levels provide pinpoint access to the RAC's CIKR data. Standard reporting functions enable secure transmittal of risk data to private and public partners.



Assessing CIKR vulnerability to and consequences of a VBIED threat using the RAC.

- **Vulnerability and Consequence Assessments:** Users can generate detailed assessments of asset vulnerability and consequence impact using completely customizable assessment metrics, directly through the RAC.

Digital Sandbox's Risk Analysis Center's core critical infrastructure management and protection function is tightly integrated with its risk analytics and can generate real-time risk statistics for jurisdictions, assets, sectors, sub-sectors, and threat likelihoods.