Category: Risk Management Initiatives
Project: Critical Infrastructure-Suspicious Activity Reporting (CI-SAR)
State Agency: New York State Homeland Security, State Police, Cyber Security

Protecting New York Through Data Solutions

Prepared by CIO/OFT on Behalf of New York State Homeland Security, State Police, Cyber Security
B. Executive Summary

The New York State Office of Homeland Security, Division of State Police, and the Office of Cyber Security and Critical Infrastructure Coordination collaborated to create a powerful criminal investigation and analysis tool. This tool, *The Critical Infrastructure – Suspicious Activity Reporting (CI-SAR)*, was created using multiple data and infrastructure domains from each participating agency.

New York, like many states around the nation, has been faced with deep budget cuts and has undergone a number of adjustments in its human resources pool through hiring freezes and retirement. To continue critical missions and devise strategies for savings and consolidation, a team from Homeland Security, State Police and Cyber Security convened and analyzed similar functions where resources could be combined to eliminate redundant and duplicative tasks. The area of Suspicious Activity Reporting (SAR) presented a common theme. Thus, the CI-SAR tool was created and has proven to be a valuable tool for intelligence analysts to evaluate threats, risks and suspicious activities.

The CI-SAR tool *uses existing criminal justice, critical infrastructure, and GIS data as an innovative business analytic* to find hidden relationships; perform trend analysis; identify changes in situation awareness; data mine combined dataset; perform threat analysis and assess the overall effectiveness of protective safety/security measures and programs. The implementation of quality control procedures and geo-coding efforts contributed higher data confidence levels to the intelligence data collected.

There are many benefits being realized as a result of this project. One *benefit of this multi-agency collaboration was obtaining higher data confidence levels*, through the quality control procedures and geo-coding efforts that were implemented. Intelligence analysts and interns worked to *extract over 3,000 suspicious activity reports* from the Intelligence Data System (IDS).

The most significant benefit is the ability for *authorized users from multiple agencies to share and access information in a centralized system*. Successful security initiatives require vigilance and cross-agency collaboration. New York State cannot fully detect threats and protect its citizens and visitors without greater information sharing and collaboration. CI-SAR goes a long way to helping NY achieve that goal.

The CI-SAR is directly aligned with New York State strategic priorities to make information available, visible, accessible and understandable; and increase cost-efficient shared services.

This application addresses NASCIO’s State CIO Top Priorities for Budget and Cost Control; Consolidation of Resources; Security Enhancement Tools; and Business Analytics.
C. Description

The New York State Deputy Secretary to the Governor for Public Safety envisioned being able to view the state’s suspicious activity reports and critical infrastructure assets on one interactive map. The task was presented to the agency with a very short, 6-month time frame for development.

Since the information necessary to achieve this was under the control of several different agencies, a team including members from New York State’s Office of Homeland Security (OHS), Division of State Police (NYSP), and Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) was formed.

Problem

Information sharing and data fusion among three agencies—OHS, NYSP, and CSCIC—was extremely difficult because of organizational ‘stove-piping” and data was stored within multiple systems across the agencies. Each agency had specific missions and data domains creating an overlap in function and redundancy for the information gathered about Suspicious Activity Reporting (SAR).

Analytical methods were immature for identifying threats to infrastructure and analysts needed to perform multiple steps to put together a view of suspicious activity and critical infrastructure. Expertise in each agency’s domain was isolated and separate.

Solution

Through inter-agency collaboration the team from Homeland Security, State Police and Cyber Security pooled expertise and open data domains to pull suspicious reporting activities into one system, the CI-SAR (Critical Infrastructure-Suspicious Activity Reporting). Three agencies now share the same unified information and can identify intelligence gaps through improved analysis. The result is improved interagency collaboration, data sharing, reduction of isolation and improved data quality and access.

The initial deployment of the Critical Infrastructure – Suspicious Activity Reporting (CI-SAR) system occurred in March 2008. CI-SAR uses intelligence information along with critical infrastructure data to perform a series of statistical and geographic analyses to uncover hidden or obscure relationships.

Access to the application is through a user’s local browser, which relies on MS Office Web components, to connect to the server. Once connected, the user can query and browse data, download information to their local machine, and manipulate data into a desirable ‘view’ format. When the user is finished, the application saves the ‘view’ onto the server. See Networking Overview in Figure 1.
GIS queries are also accessed through the local browser but use Simple Object Access Protocol (SOAP) web service with MS Office Web components. Users can load data directly into CI-SAR for analysis using ActiveX tools in the desktop browser. See Figure 2.

Figure 2
CI-SAR displays the results in powerful visual and easy to understand statistical and map formats.
The CI-SAR system is a potent tool for intelligence analysts to evaluate threats, risks and suspicious activities. The analysts have the ability to perform trend analysis, identify changes in the situational awareness, data mine combined datasets and to perform threat analysis. Additionally, the CI-SAR system provides analysts with data to assess the overall effectiveness of protective measures and programs. With CI-SAR detailed information about critical information and key resources (CI/KR) including high resolution aerial imagery and specific essential data about other facilities nearby can be easily retrieved and queried in either a map or tabular format to provide a more complete and context-based view of threat data.

Figure 3 is an example view of activity by looking individually at tips or infrastructure or a spatial overall of both. Let’s say, an analyst performs a search on TIPS using the phrase ‘3 males.’ The results show a raise in activity in Erie and Westchester County.

![Figure 3](image-url)

Then by selecting Erie and the surrounding counties, the Figure 4 shows two obvious increases, in 2007 and 2008.
Next, the analyst can get a quick view of the tips on a map. Here the ‘3 males’ tips in Erie and surrounding counties, the data can be mapped in Google Maps or in the state’s Critical Infrastructure GIS application (CIRIS). Tip narratives are also available in the map view in Figure 5.

**Figure 5**

*Erie & Westchester Peaks; Erie and Surrounding Counties*
D. Significance

The most significant achievement was the collaboration between the agencies involved. Information under the “command and control” of an agency was now being shared with other stakeholders for a greater good and accomplishment of the mission. There is no other system in New York State, available to state-level analysts, that helps address the potential nexus of threat and vulnerability at critical infrastructure facilities. As such, this tool will augment existing methods of analyzing suspicious activity reporting, and will assist intelligence analysts in providing useful and timely intelligence, both tactical and strategic, to agency executives, law enforcement and private sector partners, as appropriate.

The CI-SAR is directly aligned with New York State strategic priorities to make information available, visible, accessible and understandable; and increase cost-efficient shared services.

E. Benefits of the Project

There are many benefits being realized as a result of this project. One benefit of this multi-agency collaboration was obtaining higher data confidence levels, through the quality control procedures and geo-coding efforts that were implemented. Intelligence analysts and interns worked to extract over 3,000 suspicious activity reports from the Intelligence Data System (IDS). These reports were received by NYSIC-CTC from New York State and local law enforcement and the public. Tips were then reviewed and quality control performed, to ensure all information necessary for geo-coding (i.e. address) was available. The tips were also coded to account for credibility of the source and validity of the information provided. All final quality control is done inside the “quality control tool”, a database designed by OHS Intelligence Division to help analysts and interns track progress and note gaps in important information. Once tips quality control is completed, the data is imported into CI-SAR. This is a dynamic and ongoing process.

Another benefit was the development of a reusable Application Programming Interface (API) to the New York State Critical Infrastructure Response Information System (CIRIS) mapping application.

The most significant benefit was the ability for authorized users from multiple agencies to share and access information in a centralized system.