

# New York State's Critical Infrastructure Suspicious Activity Reporting



Linking Threat, Consequence and  
Vulnerability to Counter-terrorism  
Planning

# Vision

The United States will forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructure and key assets from terrorist attack.

The National Strategy for Homeland Security

July 2002

# Threat Spectrum Germane to NYS

- **Groups**
- **Environmental**
- **Health**
- **Man-Made**

# Critical Infrastructure Intel Integration

- **Issue:**
  - Improving the way the Intelligence Community coordinates with Critical Infrastructure Stakeholders
- **Discussion:**
  - How can the IC help CI?
  - How can CI help IC?

# CI Intel Integration

## Intel:

- Awareness of Terrorist Groups
- Capability
- History
- Intention
- Targeting of CI

## Critical Infrastructure:

- Identifying Critical Infrastructure
- Defining dependence /interdependence
- Understanding integrated networks
- Mission Assurance
- SME

# CI Intel Integration

- **Chemical Project – Advisories & CSXT NOW Pilot**
- **State Threat Papers**
- **NYS Partnership w/ DHS HITRAC**
- **CI Threat Unit**
- **New York State capabilities**
  - ✓ Intelligence analysis, information sharing, threat assessments
  - ✓ Site security and vulnerability assessments
  - ✓ “Target hardening”
  - ✓ Grants to localities for equipment, training, communication

# CI-SAR Project

- Critical Infrastructure- Suspicious Activity Reporting (CISAR)
- New tool for intelligence analysts that combines suspicious activity reporting, infrastructure data and statewide datasets in one system for geospatial analysis
  - Threat/Vulnerability Overlays
  - Allows for the identification and analysis of patterns of suspicious behavior
  - Data analysis
  - Visualization/Mapping
- Built in statistical analysis capability

# Project Overview

- Assist state in supporting full range of intelligence cycle activities



# Demonstration of Analytical Capabilities for Incident & Critical Infrastructure

CI → Tip

Tip → CI

# Example: Search for Tips Around Critical Infrastructure of Interest



Search **Map** Browse Events CIRIS News Links Admin Utilities

Home | Help | Logout

Current Zoom Area



Zoom

Miles Across Map

1.59

Geographic Coordinates

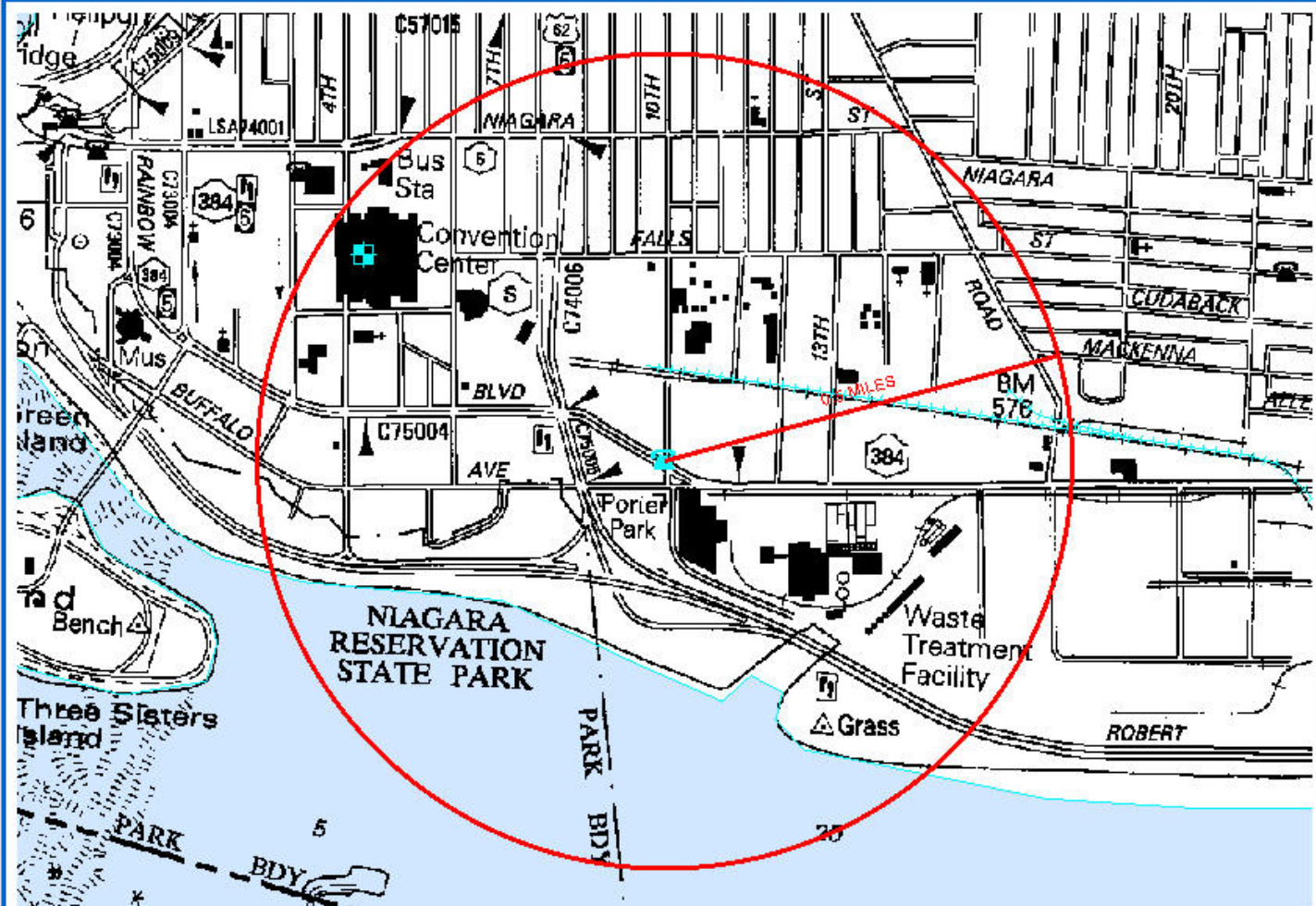
Latitude: 43.0901N  
Longitude: 79.0602W

Latitude/Longitude (DD)

Legend [Manage Layers](#)

- NYS Tier 3 Critical Infrastructure
- Tips 2005 and 2006
- Interstate & Major Highways
- Railroads (Line)
- County Boundaries

Map Layers  Bookmarks  Locate Area  Query  Preferences



- Zoom In
- Zoom Out
- Full View
- Pan
- Previous
- Next
- Get Info
- Annotate
- Measure
- Clear
- Print
- Email

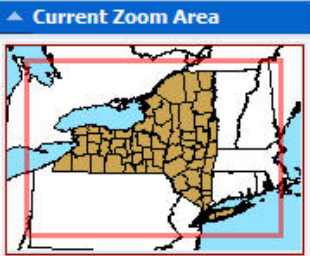
# Example: Clusters of Suspicious Incident(s)



Search **Map** Browse Events CIRIS News Links Admin Utilities

Home Help Logo

Map Layers Bookmarks Locate Area Query Preferences



Zoom

Miles Across Map

512.98

Geographic Coordinates

Latitude: 44.7488N

Longitude: 79.0703W

Latitude/Longitude (DD)

Legend [Manage Layers](#)

- Tips near Nuclear
- Nuclear Power Plants
- Interstate & Major Highways
- County Boundaries



- Zoom In
- Zoom Out
- Full View
- Pan
- Previous
- Next
- Get Info
- Annotate
- Measure
- Clear
- Print
- Email

# Project Participants

- **Office of Homeland Security**
  - **Critical Infrastructure Protection Division**
    - Supports NIPP and other Federal missions
    - Risk assessment & Sector prioritization
    - Site Security & vulnerability assessments of CI/KR
    - Develop NY contributions to NADB
    - Maintains statewide inventory of CI/KR
  - **Intelligence Unit**
    - Strategic intelligence products
    - Provide internal support to OHS units and NYS Executive Chamber
    - Advisories and bulletins to local law enforcement and private sector
    - Member assigned to NYSIC-CTC
    - Information memorandum

# Project Participants

- Office of Cyber Security and Critical Infrastructure Coordination
  - Critical Infrastructure Protection Division
    - Cyber Incident Response Team
    - Deploy/monitor intrusion detection for statewide networks
    - Red team or ethical hacking exercises
    - Statewide coordination of Geographic Information Systems (GIS) for emergency response
    - Multi-State Information Sharing and Analysis Center

# Project Participants

- **New York State Police**
  - **Office of Counter Terrorism**
    - Prevention, Investigation, Response to terrorism
    - Response teams for terrorist events, hazmat, special events
    - Response training unit
    - Executive Director of NYSIC
    - NYSP GIS for investigations, response, planning and research
    - Staffing and oversight of specialized units
      - Counter Terrorism Intelligence Units
      - Border Intelligence Units
      - Special Investigations Unit
      - Joint Terrorism Task Force members
      - Criminal Intelligence Section

# Project Participants

- **New York State Intelligence Center**
  - **Counter Terrorism Center (5 agencies)**
    - Collection, analysis and dissemination of all-source intel
    - Operate the SAFENYS terrorism tips hotline
    - Tactical/Investigative intelligence support
    - Support Federal, state and local information sharing
    - Access Federal Intelligence Community classified intelligence on-site (personnel and systems)
    - Daily Counter Terrorism Report (situational awareness)
    - Situational Reports for emerging incidents
    - Coordination with OHS-Intel on special projects, reports
    - GIS for intelligence analysis and reporting
  - **Other Specialized Units**
    - Border, Criminal, Gangs, Guns, Financial, Narcotics

# Strategic Benefits for CI/Intel Integration

- Potentially identify unseen patterns of suspicious activity, improving the risk management framework
- Improves information sharing practices
- Creates a culture of information sharing
- Reduces barriers to information sharing
- Institutionalizes information sharing

# Tactical Benefits

- Activity trending data analysis visualization
- Supports day to day public-private coordination structures, information sharing networks, and risk management frameworks.
- Directs resource allocation through actionable intelligence.
- Prioritizes CIP activity.
- Influences private sector steady state protection efforts.

# Questions?



**Benedict Conboy**

**New York State Office of Homeland Security**