

Nevada's Approach to Critical Infrastructure Protection



Presented by: Ernest Chambers Jr.

"All Eyes for All Hazards"

Protected Critical Infrastructure Information (PCII)
LAW ENFORCEMENT SENSITIVE

Infrastructure Protection Relies Heavily upon ESRI/GIS related Technologies & Capabilities

SILVER SHIELD

PERSPECTIVE

“See It, Seize It!”

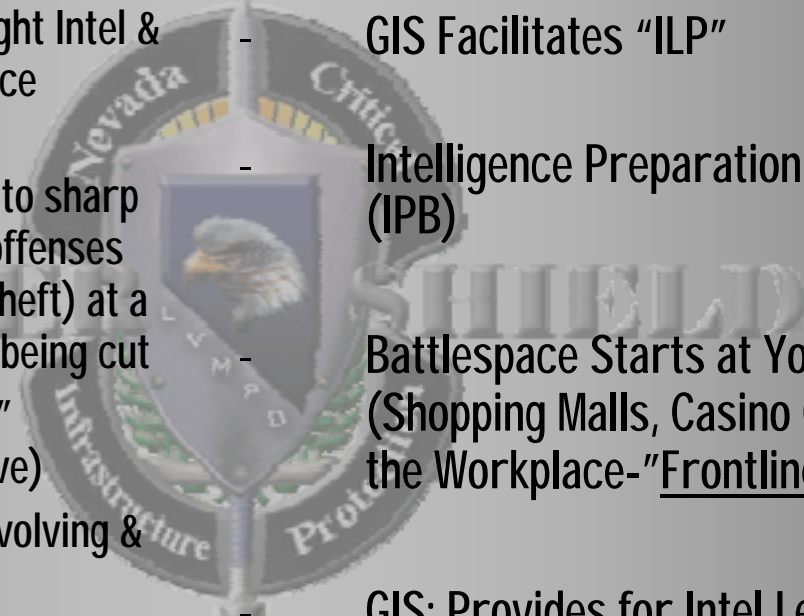
(Opportunity/Position of Advantage/Early Warning)

Pre-Emptive Action

Overview

- Intelligence Led Perspective
- Critical Infrastructure Protection Program “Silver Shield”
- Protecting Critical Infrastructure Information (PCII Program)
- Fusion Center Integration
- Demo of Capabilities & GIS Integration

Intelligence Led Perspective

- Originating in the UK, ILP (Brought Intel & Analysis to the forefront of Police Operations)
 - Kent Constabulary-in response to sharp increases in property-related offenses (e.g., burglary and automobile theft) at a time when police budgets were being cut
 - Focus is on "Leading Indicators" (Proactive) Vs. Trailing (Reactive)
 - Blended Threat Environment "Evolving & Mutating"
 - Al Qaeda ideologues Abu Mus'ab al Suri advocate for "individual jihad" (1604-page book Da'wat al-Moqawma)
 - Active Shooter (New York NY Hotel)
 - Barricaded Suspected/Hostage Takers
 - Suicide Bomber
- 
- GIS Facilitates "ILP"
 - Intelligence Preparation of the Battlespace (IPB)
 - Battlespace Starts at Your Door-Step (Shopping Malls, Casino Gaming, Schools & the Workplace-"Frontline" Soft Targets)
 - GIS: Provides for Intel Led Solutions that assist Public/Private Sector organizations to achieve Strategic, Tactical & Operational Advantage
 - Picture/1000 Words!

Silver Shield's Mission

"Identify, catalogue, prioritize and coordinate for the protection of critical infrastructure / key resources (CI/KR) to support Federal, State, Local & Tribal readiness, prevention, mitigation & response efforts."

Silver Shield's 5 Program Objectives

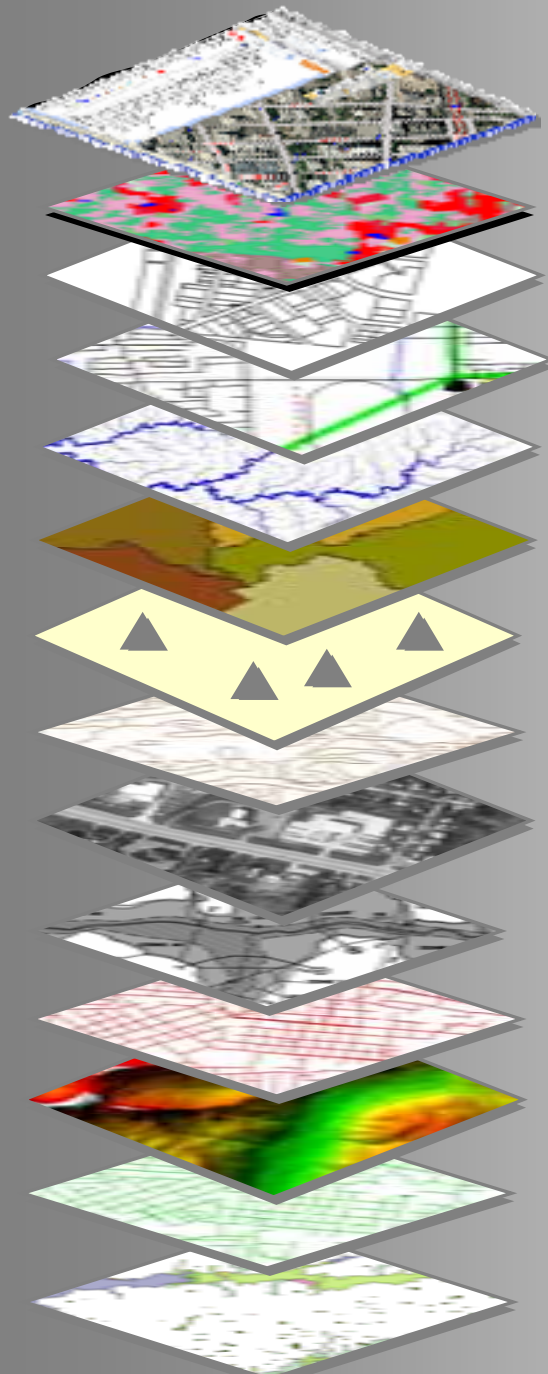
- Identify & Catalogue CI/KR
- Deploy Tactical Emergency Response Planning (TERP) Tool IAW NRS 463.790
- Provide "Incident/On-Scene" Commanders Online Access TERP
- Implement an Infrastructure Liaison Officer (ILO) program
- Deploy an Outreach Program-"Fear Reduction & Enhance Preparedness"

"ALL EYES FOR ALL HAZARDS & CRIMES"

Defining Critical Infrastructure - Critical Infrastructure/Key Resources & LOIs

- Public or private sector assets that by virtue of their function, design and/or interdependencies, if destroyed or rendered inoperable would cause the entire or significant collapse of one or several facets of the Local, State, Regional or National economy; cause mass casualties or damage the public morale/confidence to such a degree as to adversely impact the security, public health, well being & safety of the citizenry.
- Tier I/II criteria established by DHS

17 Critical Infrastructure Sectors Identified by DHS



Government

Agriculture

Transportation

Banking and Finance

Water

Defense Industry

Chemical Industry

Services

Energy

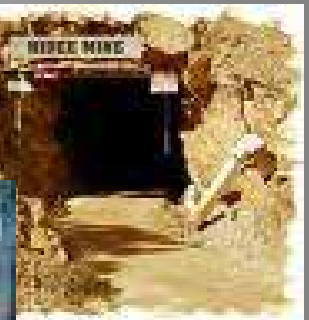
Public Health

Information and Telco

Food

Postal and Shipping

Emergency Services



Silver Shield "Buckets"



**Site Specific Data
Tier I/II
PCII
NADB**

**General Information
LOIs
Executive Order
NRS 463.790-TERP**

"Incident/On-Scene Responders"

Protected Critical Infrastructure Information (PCII)
LAW ENFORCEMENT SENSITIVE

Protected Critical Infrastructure Information (PCII) - Definition

In accordance with the provisions of 6 C.F.R. Part 29, PCII information is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release results in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq., the implementing Regulation at 6 C.F.R. Part 29 and PCII Program requirements.

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION Requirements for Use	
Nondisclosure This document contains PCII. In accordance with the provisions of 6 C.F.R. Part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq., the implementing Regulation at 6 C.F.R. Part 29 and PCII Program requirements. By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII. If you have not completed PCII user training, you are required to read a request to gpi.dhs.gov/pcii.asp within 10 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.	
Access	Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements: <ul style="list-style-type: none">Assigned to homeland security duties related to this critical infrastructure andDemonstrate a valid need-to-know. The recipient must comply with the requirements stated in the Critical Infrastructure Information Act of 2002 found at 6 U.S.C. § 131 et seq., and the implementing Regulation at 6 C.F.R. Part 29.
Handling	Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. Do not leave this document unattended. Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII. Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit. Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. Do not send PCII to personal, non-employment related email accounts. Whenever the recipient forwards or disseminates PCII via email, placeholder information is an attachment. Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no markings on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have our cover markings that indicate the contents are PCII and must bear the following below the return address: "POSTMASTER: DO NOT FORWARD. RETURN TO SENDER." Adhere to the aforementioned requirements for return office mail. Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end. Telephone: You are encouraged to use a Secure Telephone Unit Equipment. Use cellular phones only in secure environments. Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all pages are scanned for PCII. Destroy all unusable pages immediately. Disposition: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete files and empty recycle bin.
Derived Products	You may use PCII to create a work product. The product must not reveal any information that: <ul style="list-style-type: none">Is proprietary, business sensitive, or trade secret;Reveals specifically, or identifies the submitting person or entity (explicitly or implicitly); andIs otherwise not appropriately in the public domain.
Derivative Products	Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "PCII" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Tracking Number(s) of the source document(s) must be included in the derivative created document in the form of an addendum. For more information about derivative products, see the PCII Work Product Guide or speak with your PCII Officer.
Tracking Number: _____	
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION	

GIS

“Geographic Approach”

It Layers...

It Links...

It Exploits...

It Fuses...

Spatial Analysis

Modeling

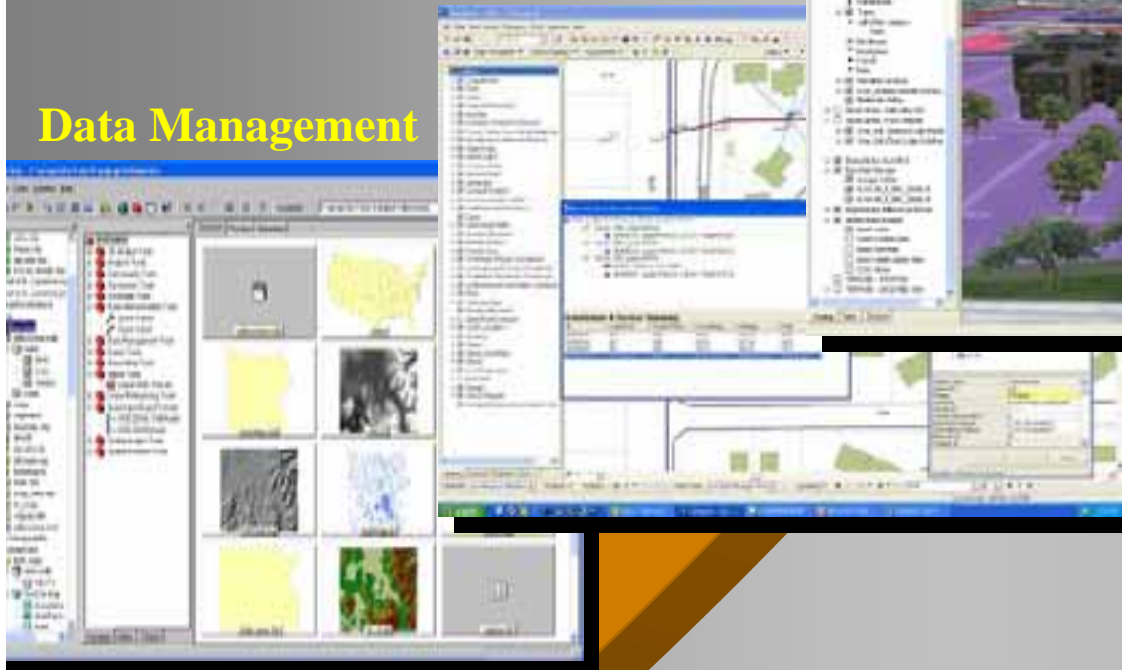
Visualization

Mapping

Imagery

Data Management

Information

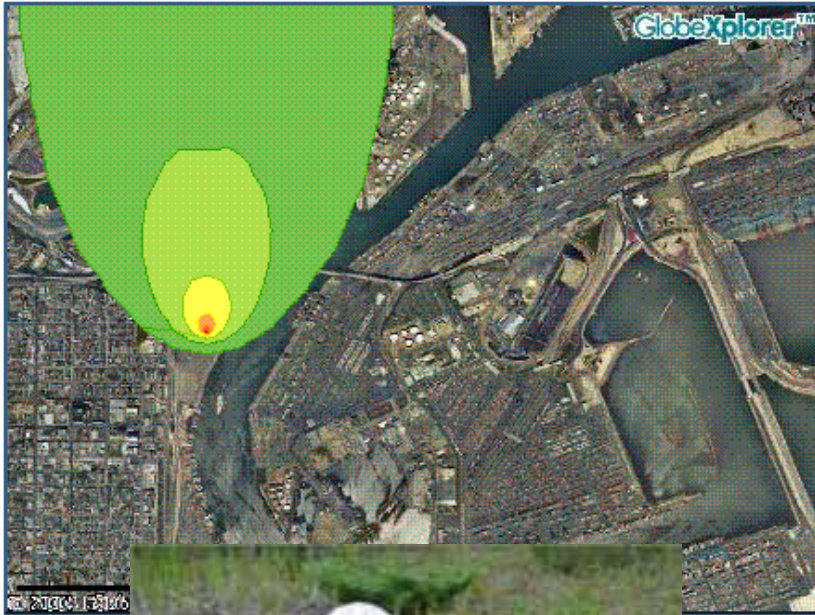


Response

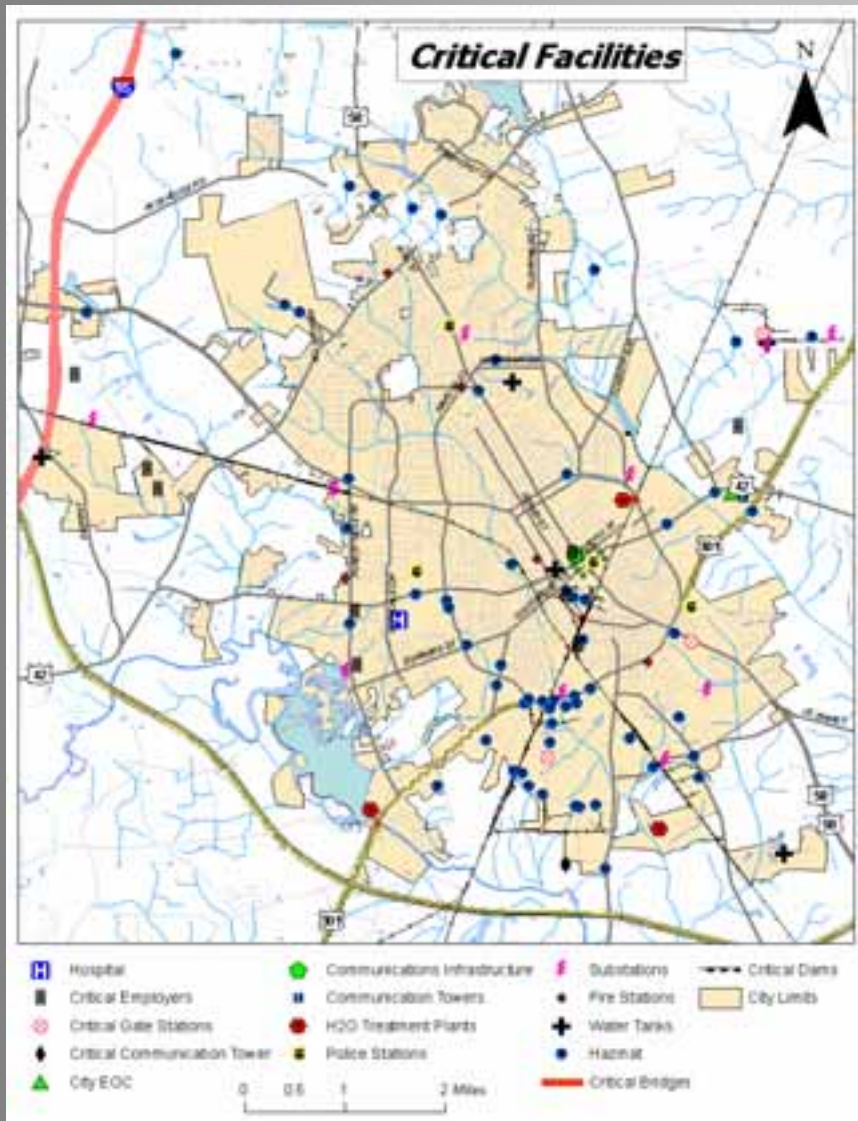
- Emergency Response



Complex Incident Management

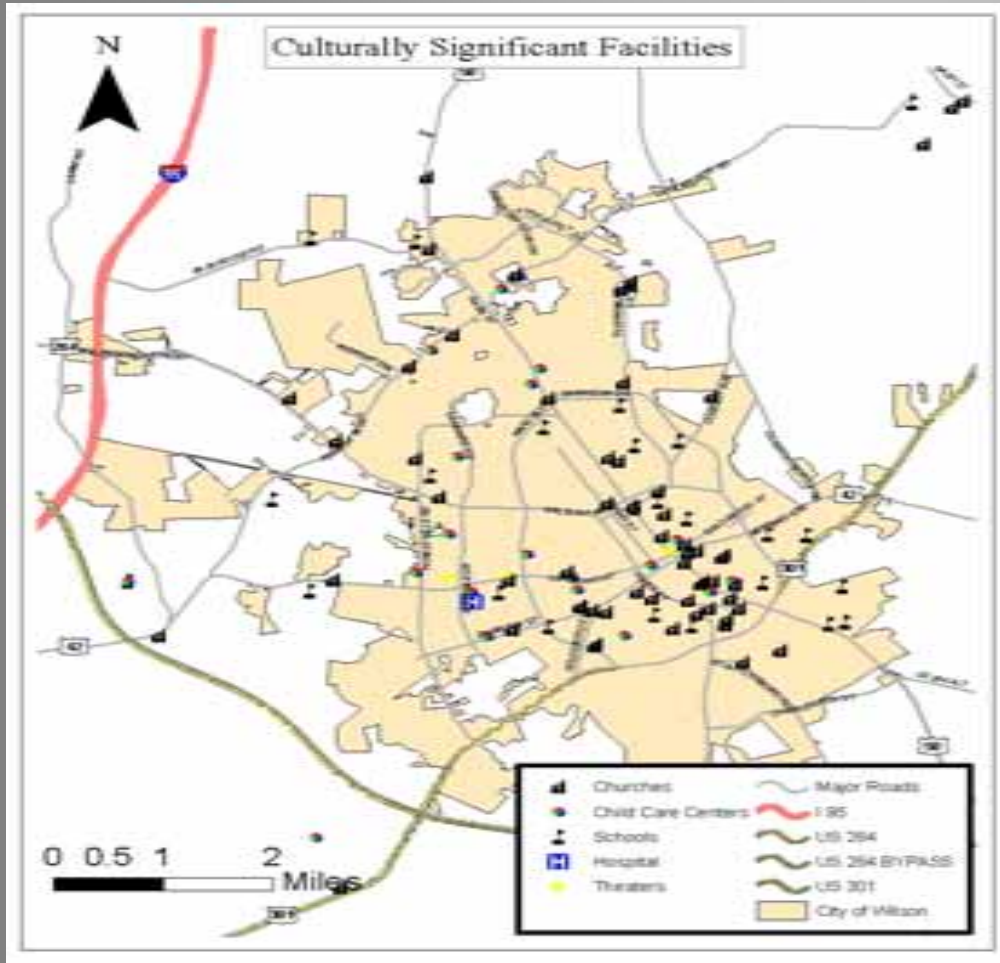


Critical Facility Identification



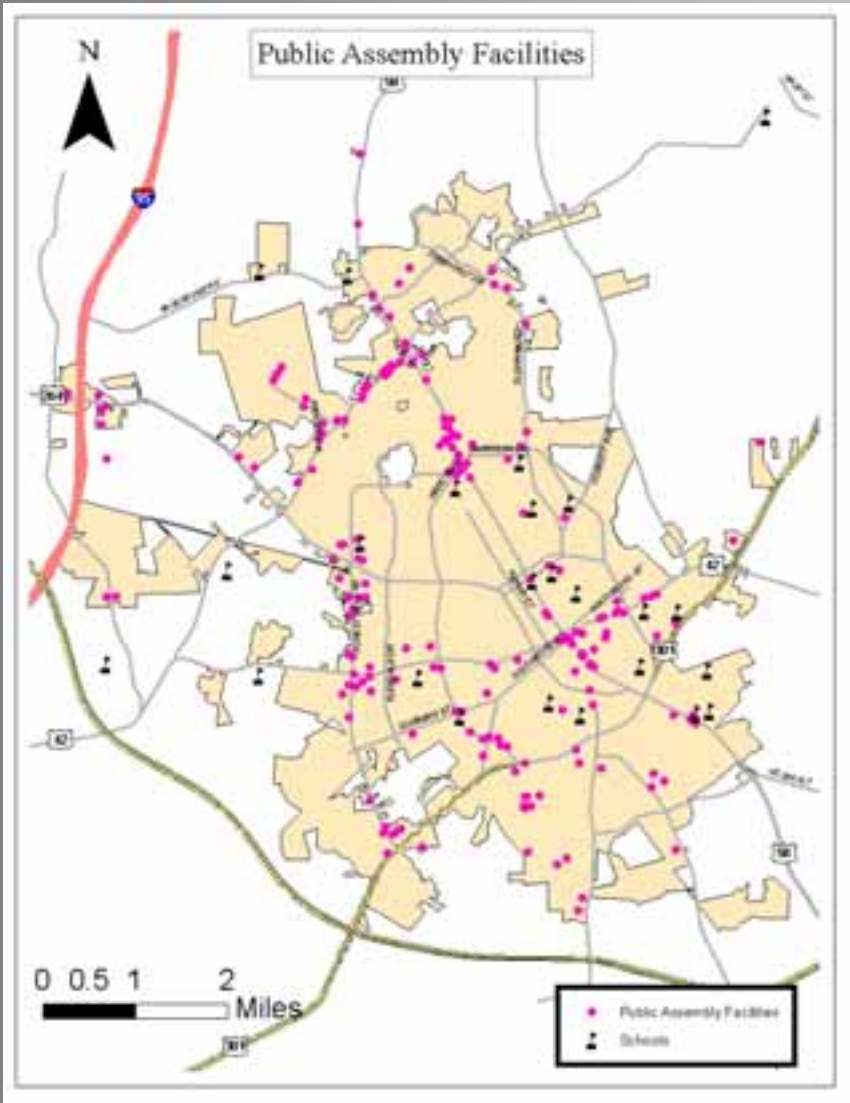
- Cultural Significance
- Public Assembly
- Criticality to City Operations
- Economic Significance
- Technological Hazards

Culturally Significant Facilities



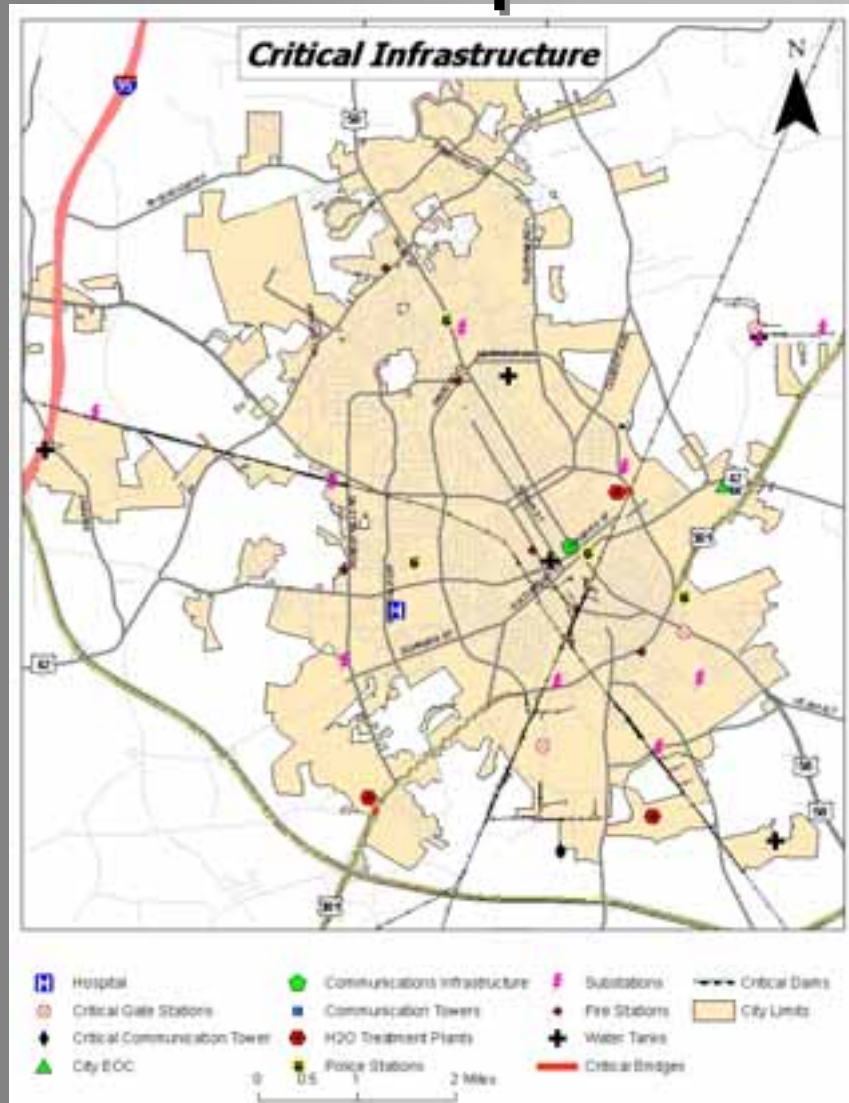
- Churches
- Child Care Centers
- Schools
- Hospitals
- Theaters

Public Assembly Facilities



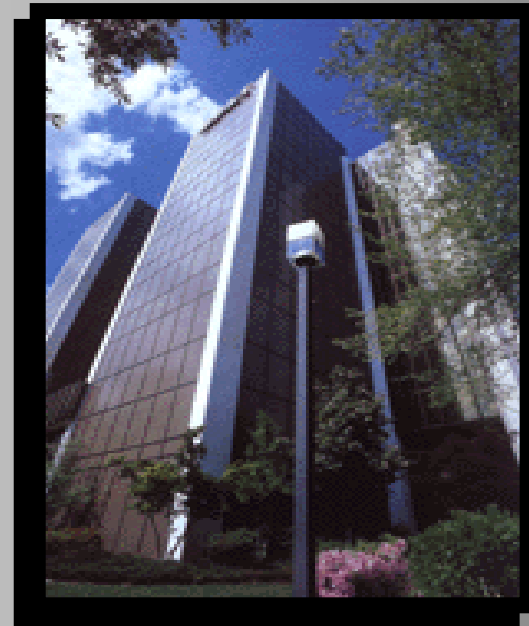
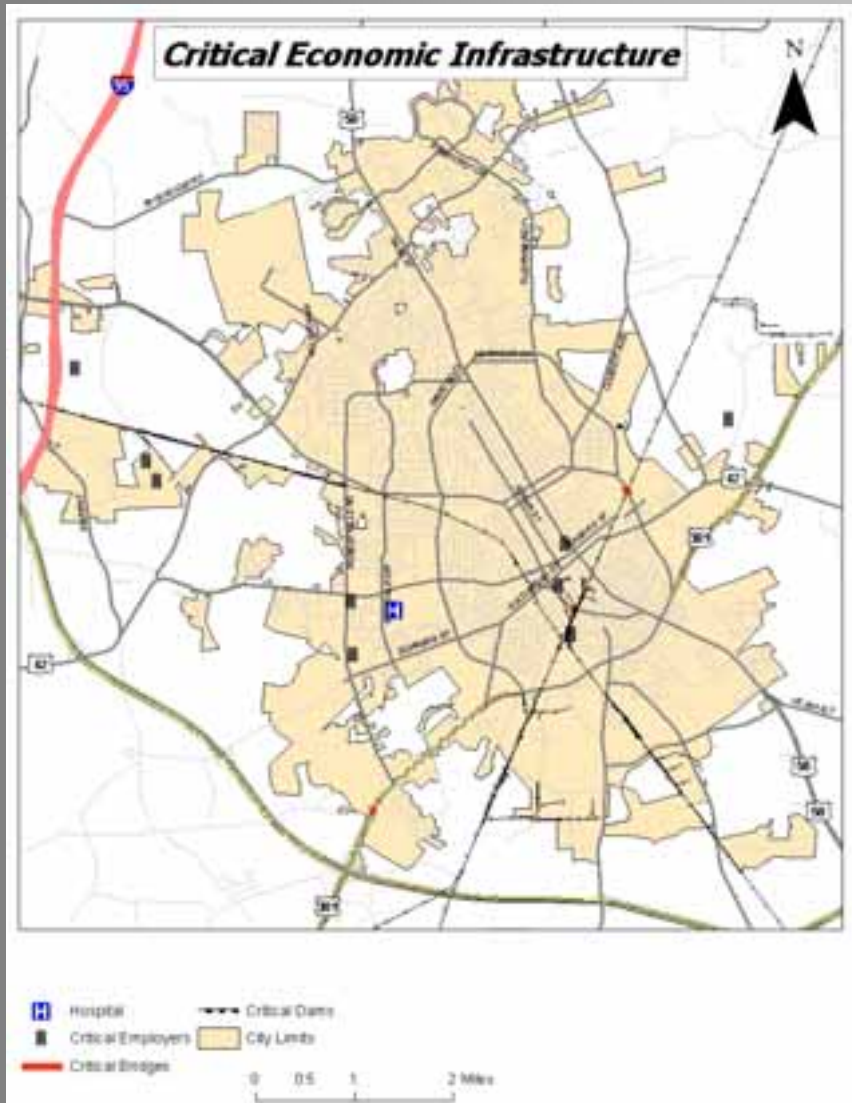
- Churches
- Child Care Centers
- Schools
- Hospitals
- Theaters
- Major Employers
- Recreation Facilities

Infrastructure Interdependencies/Essentials



- Power
- Telecommunications
- Water / Sewer Treatment Facilities
- Hospitals

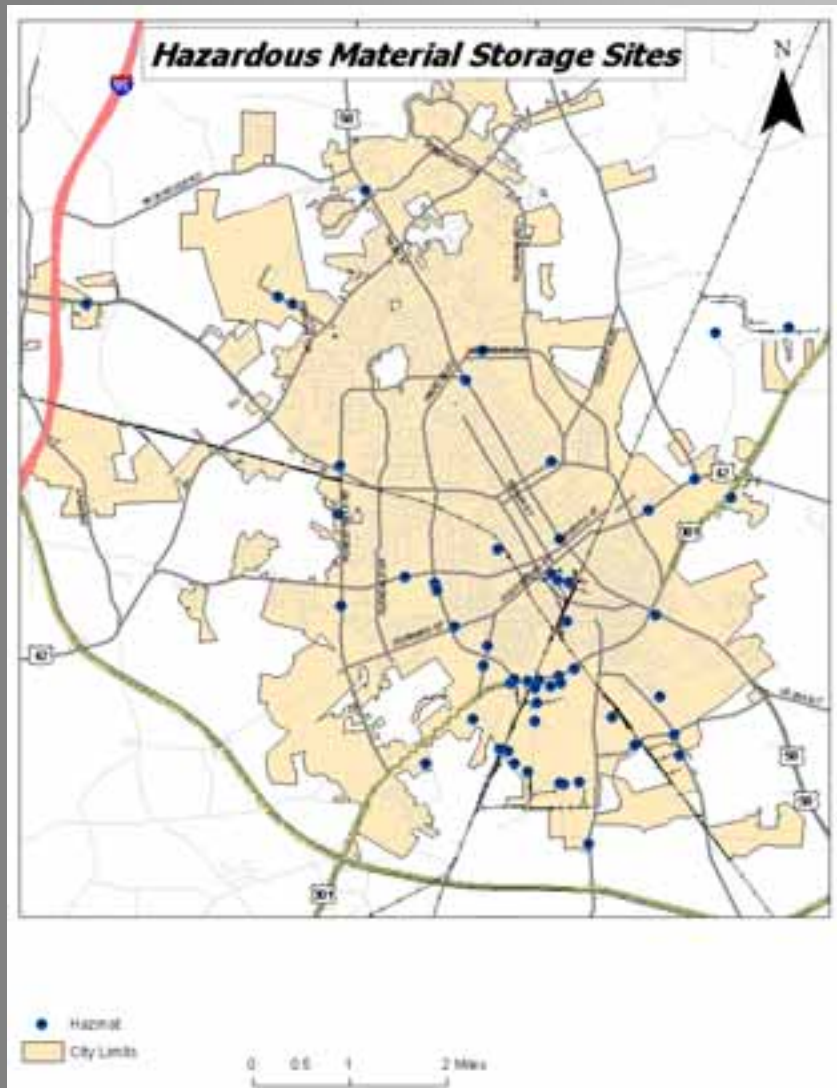
Economically Significant Facilities



Major Employers

- *Financial Centers*
- *Pharmaceutical Facilities*

Technological & Hazardous Facilities



- Pharmaceutical Plants
- Agricultural Chemical Storage Sites
- Pest Control Sites
- Large Box Stores, *etc...*

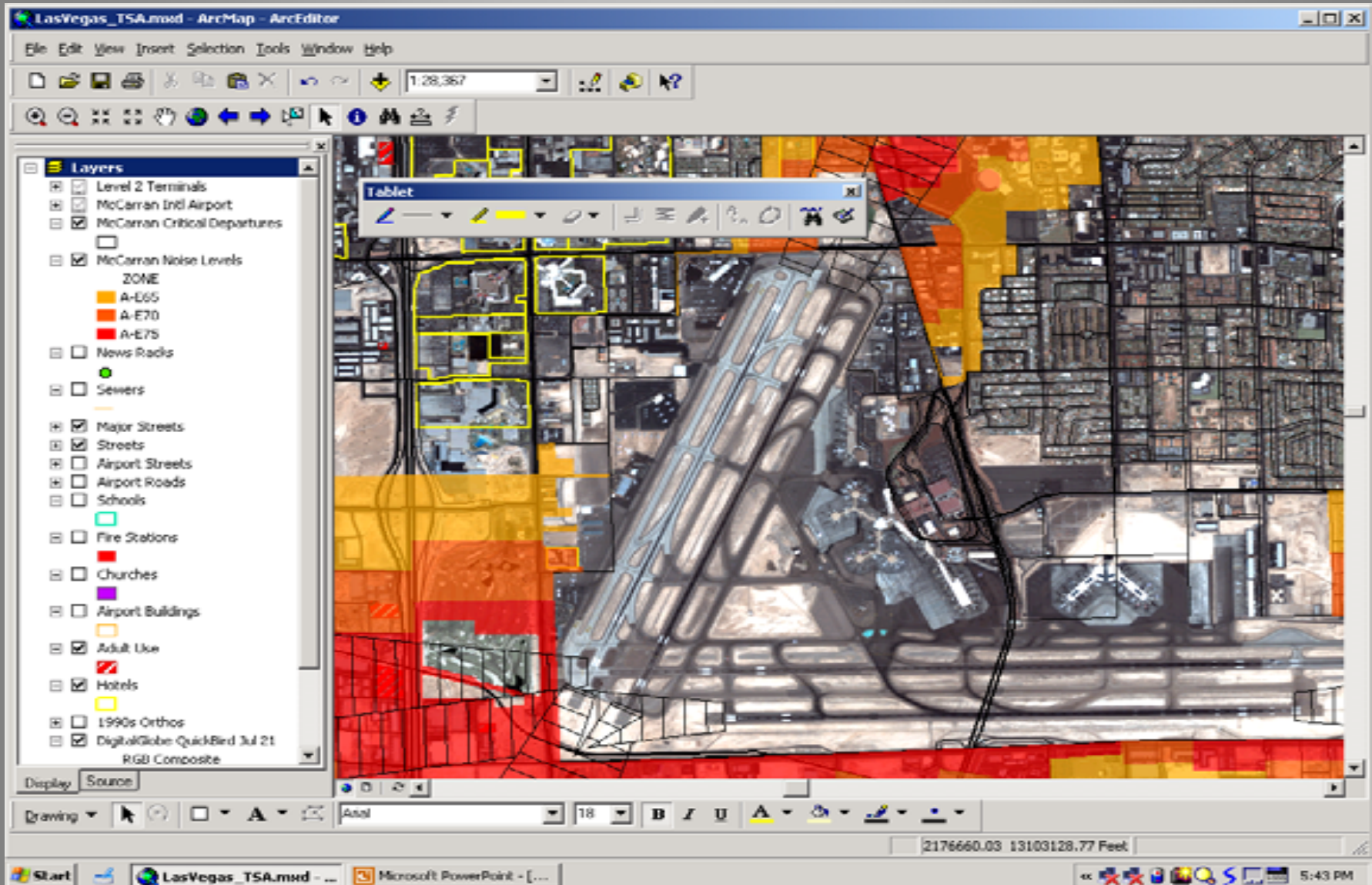


Pandemic Response

Patient, transport
analysis



McCarran IAP



Silver Shield'

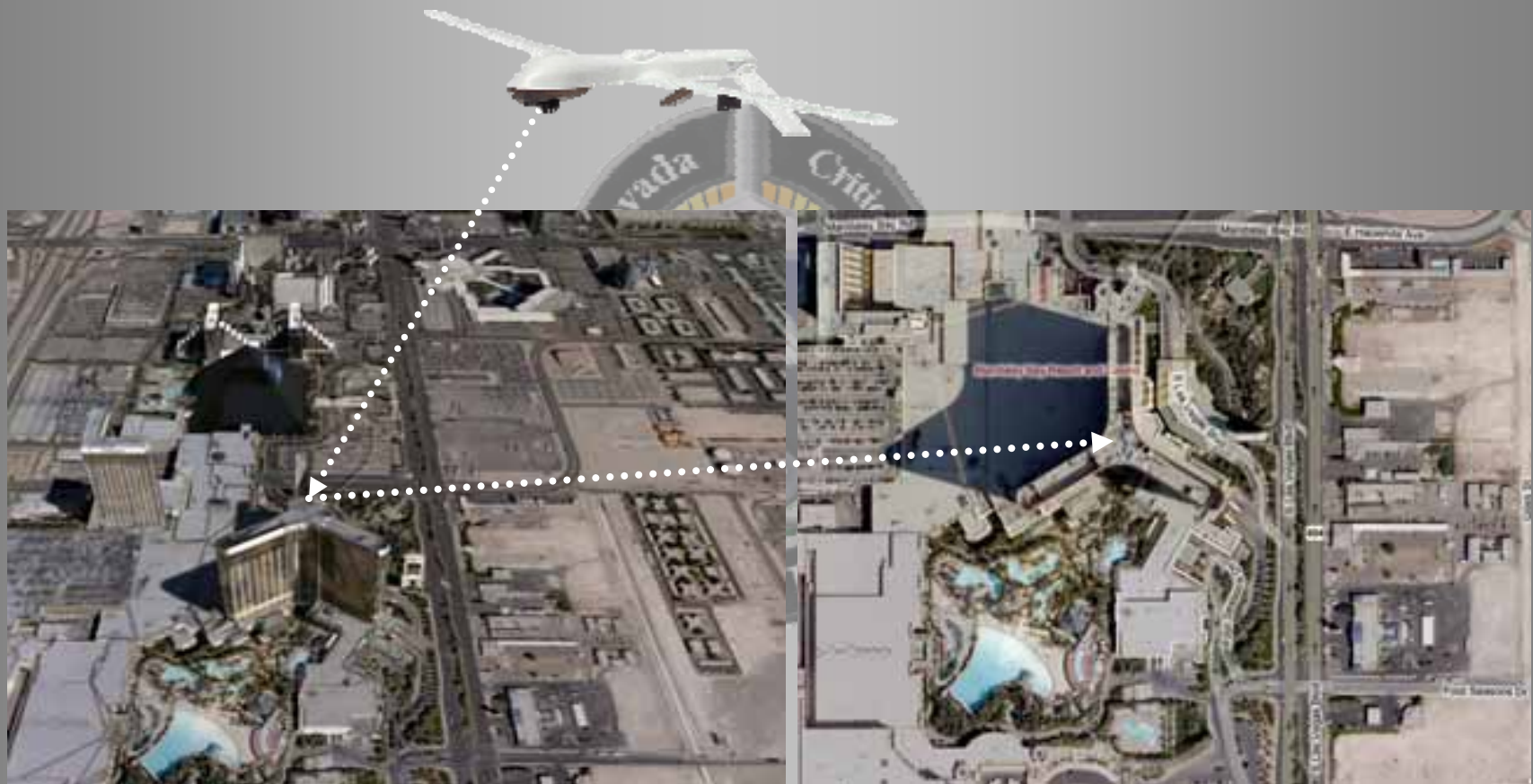
The logo is a circular emblem. The top arc contains the word "Nevada" on the left and "Critical" on the right. The bottom arc contains "Infrastructure" on the left and "Protection" on the right. In the center is a shield with a blue field and a green field, separated by a vertical line. A sword is positioned vertically behind the shield, with its hilt at the bottom and its tip at the top.

HIGH-TECH PLATFORM INTERCONNECTIONS

Protected Critical Infrastructure Information (PCII)
LAW ENFORCEMENT SENSITIVE

UAV/UAS

Unmanned Aerial Vehicle/Systems:



Special Event (New Year's Eve Sites)

Aerial Picture – Used for buffer zone & emergency planning

Resource Management Database



Catalogues the location, condition, owner & availability of critical recovery resources to include operators and other subject matter experts (SMEs)

Protected Critical Infrastructure Information (PCII)
LAW ENFORCEMENT SENSITIVE

Tactical Emergency Response Plans (TERPs)

Includes:

- General Site Characteristics (Periods of Ops)
- Impact Estimates (Plume Modeling, Economic, Psychological, Mass Casualty)
- Threat Definition (DBTs-Int/Ext, CBRNE, etc.)
- Key Staff Contacts (24/7 Contacts)
- Site Population Statistics
- HAZMAT Diary (MSDS, Contamination Est.)
- Site Security Characterization (PPS, Access Control, Lighting, Surveillance, Route Analysis, Vulnerabilities)
- Quick Reaction/Response Checklists
- Surrounding Infrastructure/Attachments



Suspicious Activity Reporting-SARS:

The logo is a circular emblem. The top arc contains the word "Nevada" on the left and "Critical" on the right. The bottom arc contains "Infrastructure" on the left and "Protection" on the right. In the center is a shield with a blue field containing a white star and a green field containing a white mountain range. A sword is positioned vertically behind the shield.

PRIVATE SECTOR PARTICIPATION
"ALL EYES FOR ALL HAZARDS & CRIMES"

Suspicious Activity Reporting System (SARS)

Encrypted online system for reporting suspicious activity/behavior:

- 128 bit encryption
- Submissions sent directly to assigned analyst
- Geared toward terrorist type activities
- Multiple subject, vehicle, & activity entries supported.
- Support images & documentation upload

Overview	✓
Location	✓
Activities	✓ 3
Subjects	✓ 2
Vehicles	✓ 2
Support Files	✓ 3
Actions Taken	✓

NEW SUSPICIOUS ACTIVITY REPORTING ENTRY
Please enter a short descriptive title for this Suspicious Activity Report and click the "Submit New" button to begin.

Descriptive Subject

Suspicious Activity Reports for Bank of America Building
Listed below are the Suspicious Activity Reports entered by your organization. You may view any of the reports listed. You may also edit any report that has not been closed out.

Entered	Title	SAR Date	SAR Time		
8/21/2007	Unauthorized entry attempt	8/21/2007 12:00:00 AM	06:00 hrs		
8/21/2007	Something happened		: hrs		
8/20/2007	Suspicious Person taking Video at Passenger Entry	8/20/2007 12:00:00 AM	14:20 hrs		
11/20/2007	Suspicious Person with Video Camera	7/20/2007 12:00:00 AM	14:00 hrs		
7/20/2007	Suspicious Person in Bank	7/12/2007 12:00:00 AM	10:10 hrs		

Subject(s) Involved in Suspicious Activity

First Name <input type="text" value="Jane"/>	Last Name <input type="text" value="Smith"/>	Middle Name <input type="text" value="Sally"/>
Alias <input type="text" value="na"/>	DOB <input type="text" value="01/22/1992"/>	Marital Status <input type="text" value="Unknown"/>
Age <input type="text" value="17"/>	Race <input type="text" value=""/>	Gender <input type="text" value=""/>
Height <input type="text" value="5"/> Ft.	Weight <input type="text" value="120"/> Lbs.	Build <input type="text" value="Slim/Slender"/>
Hair Color <input type="text" value="Brown"/>	Hair Length <input type="text" value=""/>	Eyes Color <input type="text" value=""/>
SSN <input type="text" value=""/>		
Additional <input type="text" value="This is property and then"/>		
<input type="button" value="Clear Form"/>		
Added Subject <input type="text" value="Jane Smith"/>	Vehicle <input type="text" value=""/>	Vehicle Color <input type="text" value=""/>

Suspicious Activities of the Incident

Activity Type

Suspicious Activity Reporting System (SARS)

Suspicious Activity Reports created in a standardized format to facilitate analysis!

OVERVIEW						
DATE 7/30/2007 13:00	TIME 13:07 hrs					
INCIDENT CATEGORY A person was seen taking video of our facility. The subject was seen video taping the layout of the lobby and surrounding area of our primary banking facility.						
LOCATION						
ADDRESS 113 Whisman Office Las Vegas, NV 89101						
ADDITIONAL LOCATION INFORMATION The Main Bank of America building for Las Vegas and Western United States region.						
INCIDENT ACTIVITIES						
Suspicious Person(s) This person was seen with a video camera.						
Unusual Items Left Behind When the person left, an unidentified package was left behind.						
Surveillance (Pedestrian Vehicle) Individual was video taping the building and surrounding area.						
SUBJECTS						
FIRST Unknown	LAST Unknown	MIDDLE SM	ALIAS SM	DOB 01/01/1960	AGE	RACE White/Caucasian
GENDER Male	HEIGHT 6'00ft: 2.00m	WEIGHT 200.00 lbs	BUILD Average	HAIR CLR Blonde	HAIR LENGTH Long	EYE COLOR Blue
SSN Unknown	MARITAL STATUS Unknown	FBI NUMBER				
ADDITIONAL INFORMATION This subject was seen in a white minivan communicating to a third person via cell phone. When security approached the vehicle, the subject fled the scene.						
FIRST Jana	LAST Smith	MIDDLE SM	ALIAS SM	DOB 01/10/1960	AGE	RACE Black/African descent
GENDER Female	HEIGHT 5'00ft:	WEIGHT 132.00 lbs	BUILD Slender	HAIR CLR Brown	HAIR LENGTH Long	EYE COLOR Brown
SSN Missing	MARITAL STATUS Missing	FBI NUMBER				
ADDITIONAL INFORMATION This is the subject who was video taping the property. Security detained her for questioning and then released her.						
VEHICLES						
TYPE Sport	MAKE Ford	MODEL Mustang	YEAR 2000	COLOR Silver	LIC PLATE N13-397	STATE NV
Subject was seen leaving the area in this vehicle. Left fender was damaged and dented.						
TYPE Van	MAKE Ford	MODEL Aerostar	YEAR 2000	COLOR White	LIC PLATE 485-2GJ	STATE NV
This van was seen parked on the northwest corner of the property. A second subject was seen inside the van talking on a cell phone and apparently giving descriptions to the other party.						
ACTION TAKEN						
A Female subject was detained shortly for questioning.						
Report Created: 7/30/2007 13:08:00AM						
Page 1 of 1						

Protected Critical Infrastructure Information (PCI)

LAW ENFORCEMENT SENSITIVE

Suspicious Activity Reporting System (SARS)

- Fully Searchable Database
- Scalable to authorized personnel (Fusion Center-Crime, CT, etc.)
- Facilitates speedy identification of patterns and trends, across disciplines



The screenshot displays the 'Suspicious Activity Report Search' interface. It features a search form with various filters including date range, activity type, subject demographics, and vehicle information. Below the form, a 'Search Results' table is shown with columns for 'Enterer', 'Entered', 'Title', 'SAR Date', 'SAR Time', and 'du'.

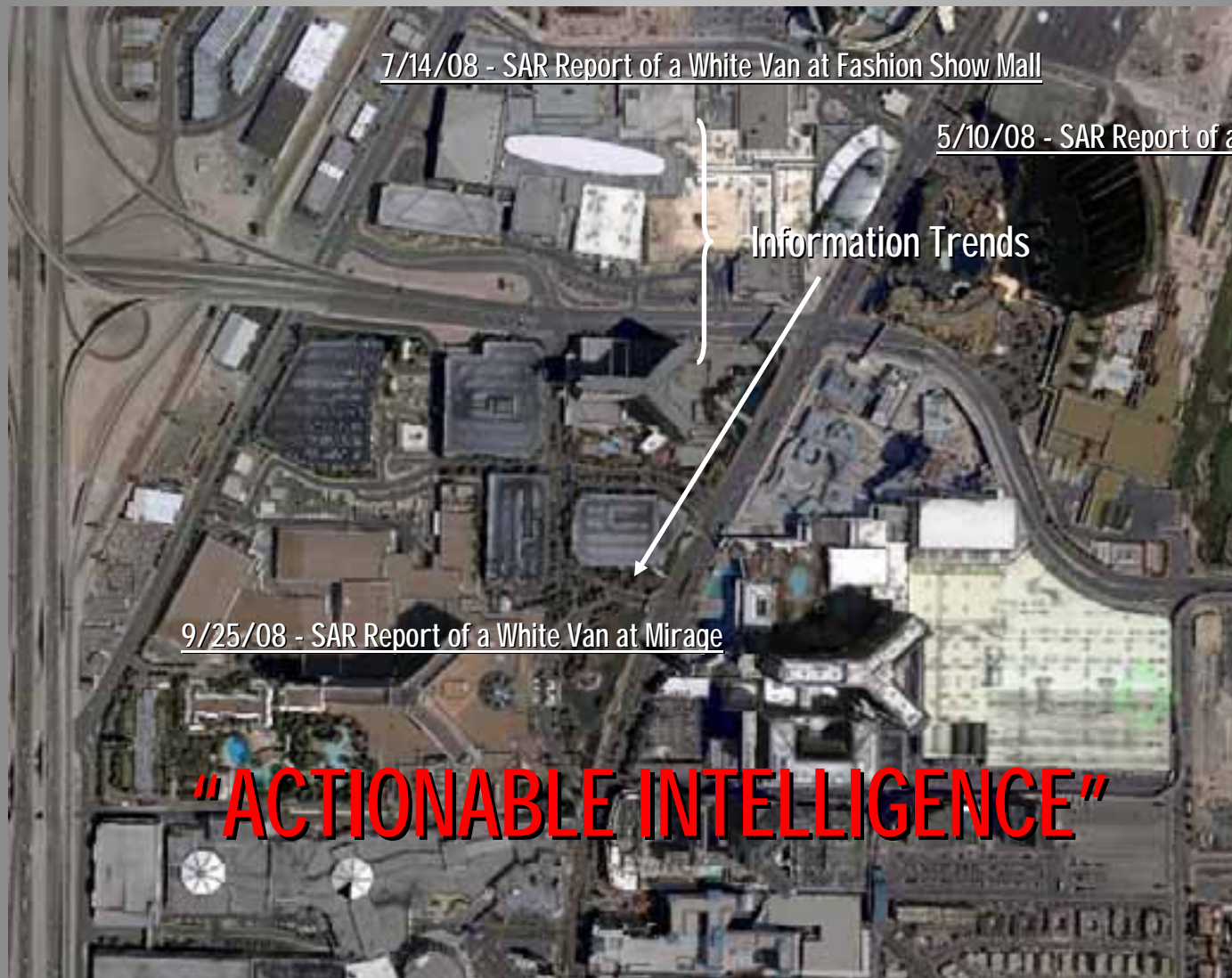
Enterer	Entered	Title	SAR Date	SAR Time	du
Nevada Power	7/17/2007	Subject goes here	7/17/2007 12:00:00 AM	11:26 hrs	du
Bank of America Building	7/20/2007	Suspicious Person in Bank	7/20/2007 12:00:00 AM	10:13 hrs	du
Bank of America Building	7/20/2007	Suspicious Persons with Video Camera	7/20/2007 12:00:00 AM	12:07 hrs	du

Protected Critical Infrastructure Information (PCII)

LAW ENFORCEMENT SENSITIVE

SARS

Actionable Intelligence



Protected Critical Infrastructure Information (PCII)
LAW ENFORCEMENT SENSITIVE

FUSION CENTER INTEGRATION



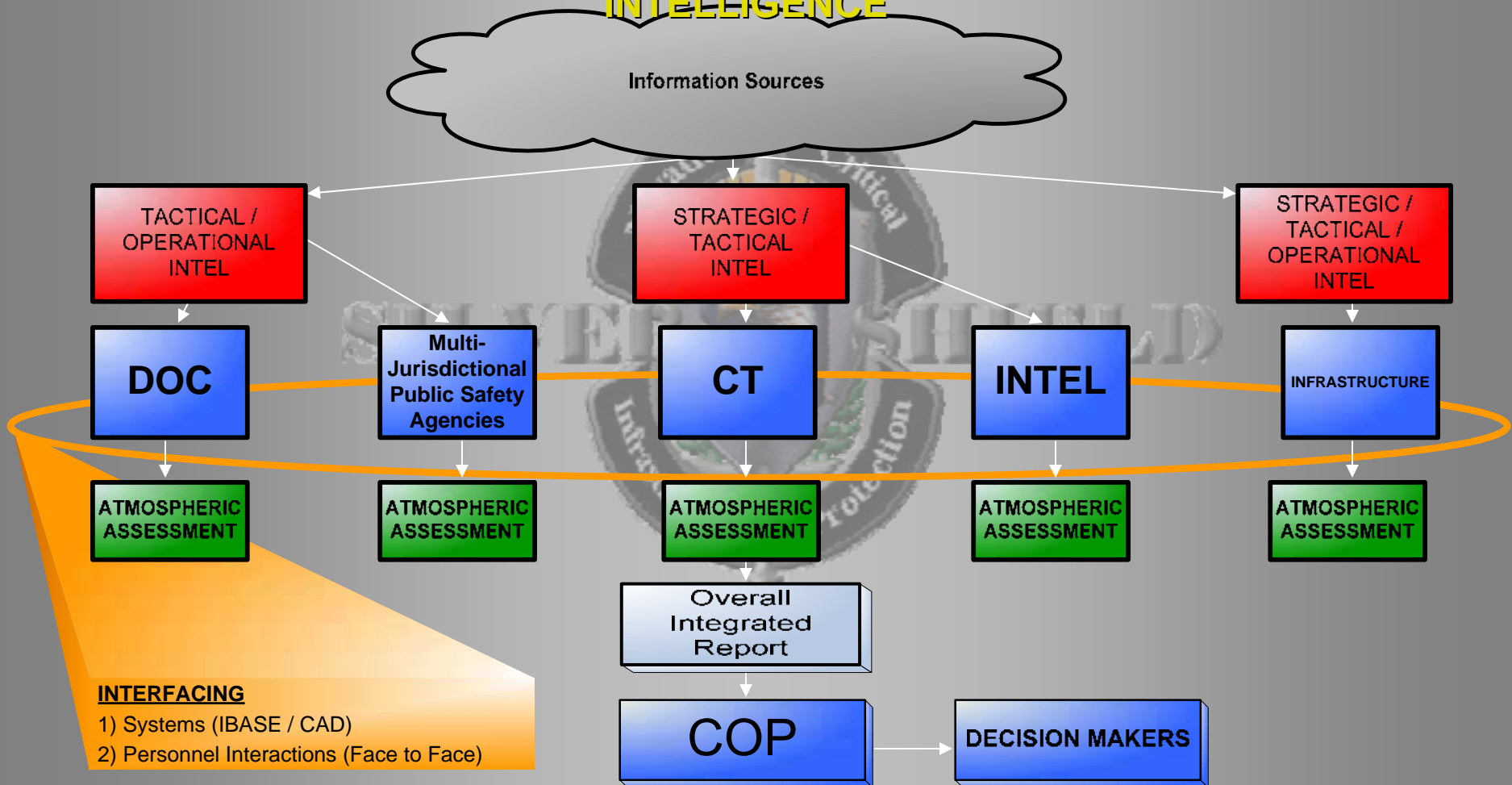
Protected Critical Infrastructure Information (PCII)
LAW ENFORCEMENT SENSITIVE

The Fusion Center - Definition and Operation of Fusion

- Unclassified Integrated multi-agency (FSLT) operation that facilitates the rapid exchange and analysis of cross-jurisdictional information stores
- Timely and Consistently between public safety and private sector entities to provide early warning of emerging threats (Terrorist/Pandemic or Natural Hazard).
- PREVENTION is paramount. If we are RESPONDING, we've failed!
- Fusion is about "SITUATIONAL AWARENESS" at such a level that preemptive action can be taken to thwart or mitigate an attack or all hazard event.
- Fusion creates the "COP-Common Operational Picture"

The Fusion Center -

ALL SOURCE INTELLIGENCE



The Fusion Center - How Fusion Works

Step 1: Multi-Agency Integration & Interoperability:

"All Eyes for All Hazards/Crimes"

- Public Safety: Police, Fire, Emergency Medical, Public Health
 - LVMPD/Henderson PD/NLV PD
 - County/City FD
 - ARMOR Group (Hazmat Response)
- Federal Partners: FBI, FAA, DHS-NOC, FEMA, etc.
- Emergency Management: State DEM/County EM
- Critical Infrastructure Protection "Silver Shield" Program-Private Sector Partners (ILOs)
- Intelligence (Crime/Counter-Terror Analysis)

"CO-LOCATED INTO A "ONE-STOP SHOP"

The Fusion Center - How Fusion Works

Step 2: Collection, Assessment & Analysis of Information:

"Common Operating Picture-COP through Info-Sharing"

- Independent Analysis which results in an "Atmospheric Assessment" in each functional area derived from:

-OSINT Analysis

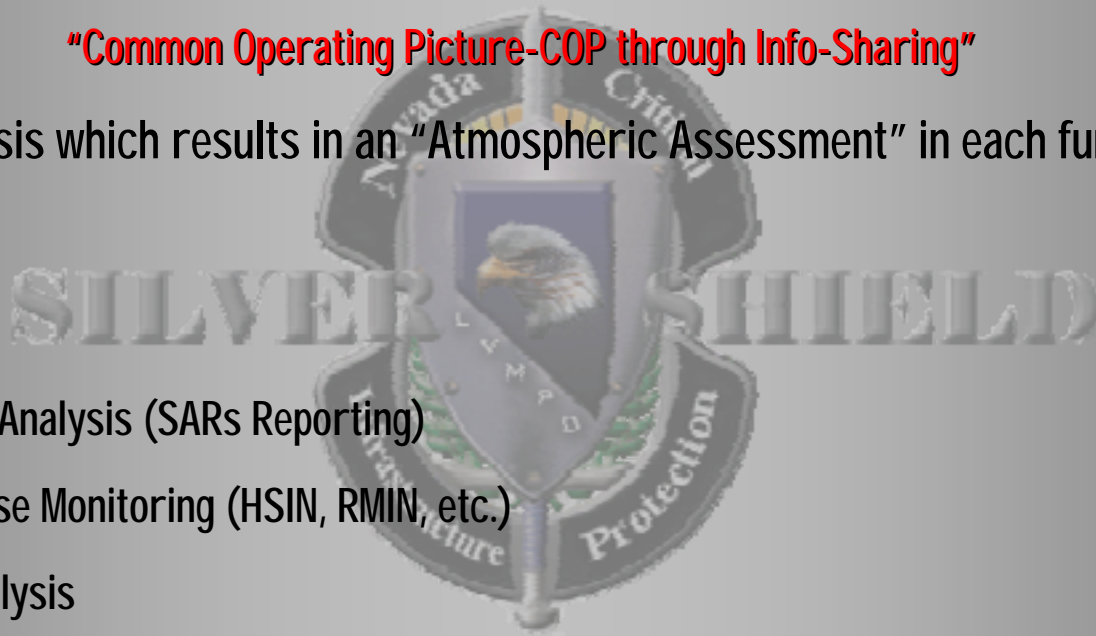
-Private Sector Analysis (SARs Reporting)

-Federal Database Monitoring (HSIN, RMIN, etc.)

-Crime Data Analysis

-Citizen Reporting Analysis (Hotline, 911/411, etc.)

- Provides "Context" for determining/understanding if there exists a terrorist "Nexus" (Link to National COP) or any pre-operational indicators of terrorism



The Fusion Center - How Fusion Works

Step 3: Production & Timely Dissemination of Products:

"Actionable Intelligence"

Information derived from multiple sources/entities that provides agencies (public/private sector) with a clear and accurate "operational picture" and hence, the ability to act preemptively/preventatively to thwart, mitigate and/or otherwise neutralize an impending threat

- Intelligence Bulletins & Advisories (SBU/LES/CUI/PCII)
- Intelligence Briefings
- Threat Assessments
- Red Teaming Exercises & Operational Efficiency Analysis (OEAs)

The Fusion Center - The Process

"Actionable Intelligence"

Information derived from multiple sources that provides public/private sector entities with a clear and accurate "operational picture" and hence, the ability to act preventatively!

"The Right Information into the Hands of the Right People & Organizations at the Right Time"

"The Right People"

- Private Industry (Commercial Business/17 Sectors & LOIs)
- Private Citizens

Tactical Emergency Response Plan - Demonstration

[Tactical Emergency Response Plan](#)

[Special Events Markup Maps](#)

[Special Events Markup Previous Year](#)

AS SOON AS POSSIBLE

Suspicious Activity Reporting Hotline:

(702) 828-8386 or 911

or at

WWW.SILVERSHIELDNEVADA.ORG

- Suspicious Activity Reporting Link



Ernest Chambers Jr.

Program Manager/Technical Lead

Cell: (702) 439-8955

Office: (702) 828-2223

Email: echambers@lvmpd.com

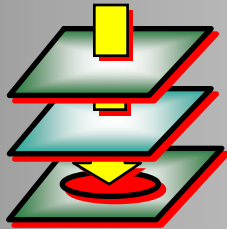
SUSPICIOUS ACTIVITY REPORTING HOTLINE: (702) 828-8386



Why is GIS Important to Law Enforcement, Security Professionals, and the Private Sector?

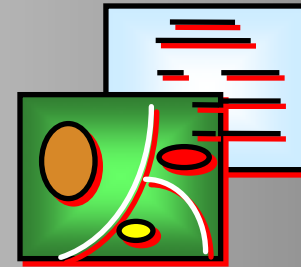
GIS enables the National Security Strategy

Tactical
and
Strategic
Planning

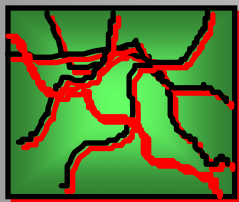


*Improved
Preparedness
And
Response*

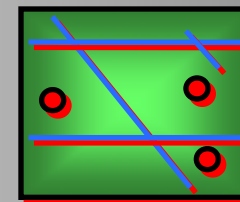
Policies
And
Procedures



Event
Modeling, Training
And Forecasting



Incident
Analysis



Better Situational Awareness
Faster response and higher immediate utility
Enabling Information Sharing

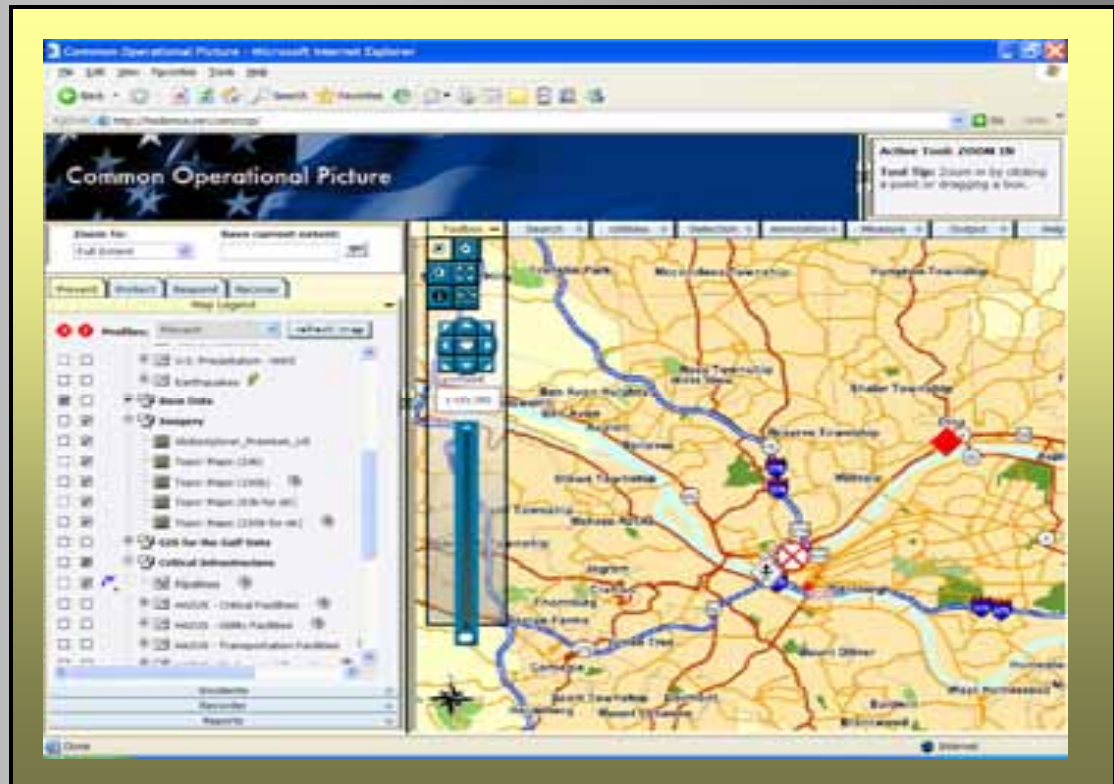
Common Operating Picture (COP)

A COP Involves....

- Integrating spatially enabled dynamic data with static spatial data relevant to a specific mission.
 - Dynamic data - Weather, Tracking, Video, Sensors, Field Observations
 - Static Data - Critical Infrastructure, Elevations, Imagery, etc.

A COP Provides....

- Situational Awareness
- Data Fusion
- Command and Control
- Incident Management



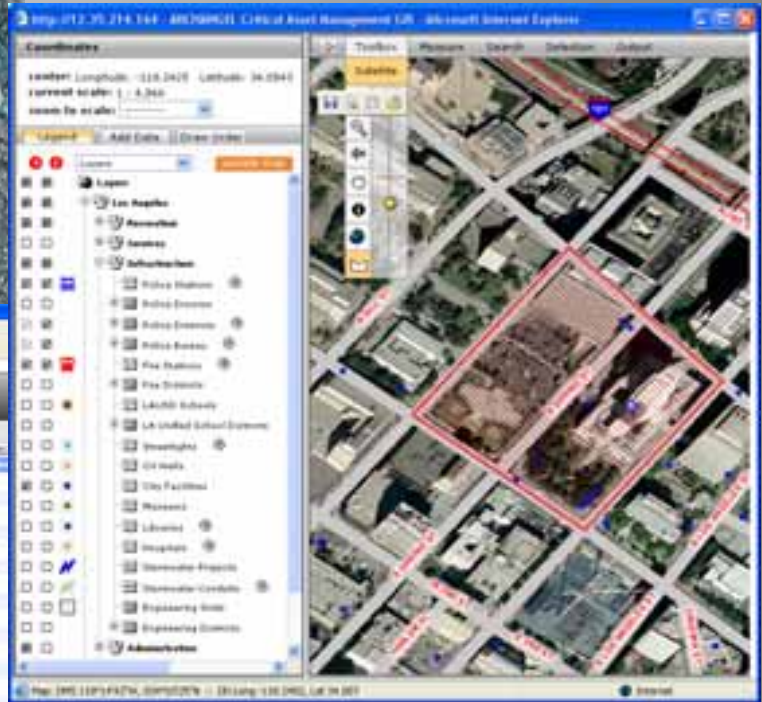
Critical Infrastructure Sectors

Agriculture
Banking and Finance
Chemical Industry
Defense Industrial Base
Emergency Services
Energy
Food
Finance
Government
Telecommunications
Postal Operations
Public Health
Transportation
Water



A satellite map of a city, likely New York City, showing a dense urban area. A red polygon is drawn on the map, enclosing a specific region. Within this red polygon, a yellow circle highlights a particular building or structure. The text "Around Critical and Infrastructure" is overlaid on the map in a large, black, serif font. The bottom of the image shows a portion of a computer screen with a blue taskbar and various application icons.

The screenshot shows the UCSD Engineering Systems website. The main content area lists several courses, including ENR 100 and ENR 101. The page is titled 'Engineering Systems' and includes a navigation bar with links like 'Home', 'About', 'Contact', 'FAQ', 'Links', and 'Search'. The course list is organized into columns: Course Number, Course Title, Course Description, Credits, and Prerequisites. The page also features a sidebar with links to various resources like 'Policies', 'Academic Resources', and 'Engineering Systems'.



Author Knowledge, Information, and Data

GIS Servers Makes It available As a *Service*

Leveraging Knowledge and Tradecraft...*(Recipes)*



- *Data*
- *Information*
- *Maps*
- *Models*
- *Visualizations*
- *Metadata*
- *Workflows*
- *Analysis*
- *Intelligence*

... From Desktop to Enterprise Services

NCIPP PROGRAM



MISSION: Identify, catalogue, prioritize and implement protective strategies/counter-measures to protect critical infrastructure and key resources in support of Federal, State, Local & Tribal readiness, prevention, mitigation and response efforts

PROGRAM OBJECTIVES:

1. Identify CI/KR Statewide
2. Deploy Emergency Response Planning Tool for Responders
3. Implement an Infrastructure Liaison (Intelligence) Program
4. Deploy a Community Education & Awareness Program
5. Assessment (TVS-Threat/Vulnerability/Security) Program

"ALL EYES FOR ALL HAZARDS & CRIMES"

ASSESSMENT METHOD



NCIPPs Assessment Method is Risk Based and Checklist "Best Practices" informed: (Sensitivity to Time & other exigencies-Volume)

Assessment Model: (Critical Components)

1. Facility Characterization "Peeling the Onion" Approach
2. Threat Analysis "Targeting" or DBT (Designed Based Threat)
3. Policy & Process Analysis "Enterprise Approach/Systems"
4. CPTED (Crime Prevention Through Environmental Design)
5. System Effectiveness (Physical Protection Systems-PPS)

"ALL EYES FOR ALL HAZARDS & CRIMES"

SPECIFIC CONSIDERATIONS



SPECIFIC ASSESSMENT CONSIDERATIONS:

- PERIMETER/BOUNDARY CONCERNS
- NEIGHBORING ASSETS & INTERDEPENDENCIES
- BUILDING/FACILITY DESCRIPTION
- DESIGN BASED THREAT & CRITICAL NODES
- CPTED CONCERNS
- PARKING
- ACCESS CONTROL
- OPERATIONAL POLICY & PROCEDURES (SECURITY)
- SURVEILLANCE & CCTV
- HAZMAT

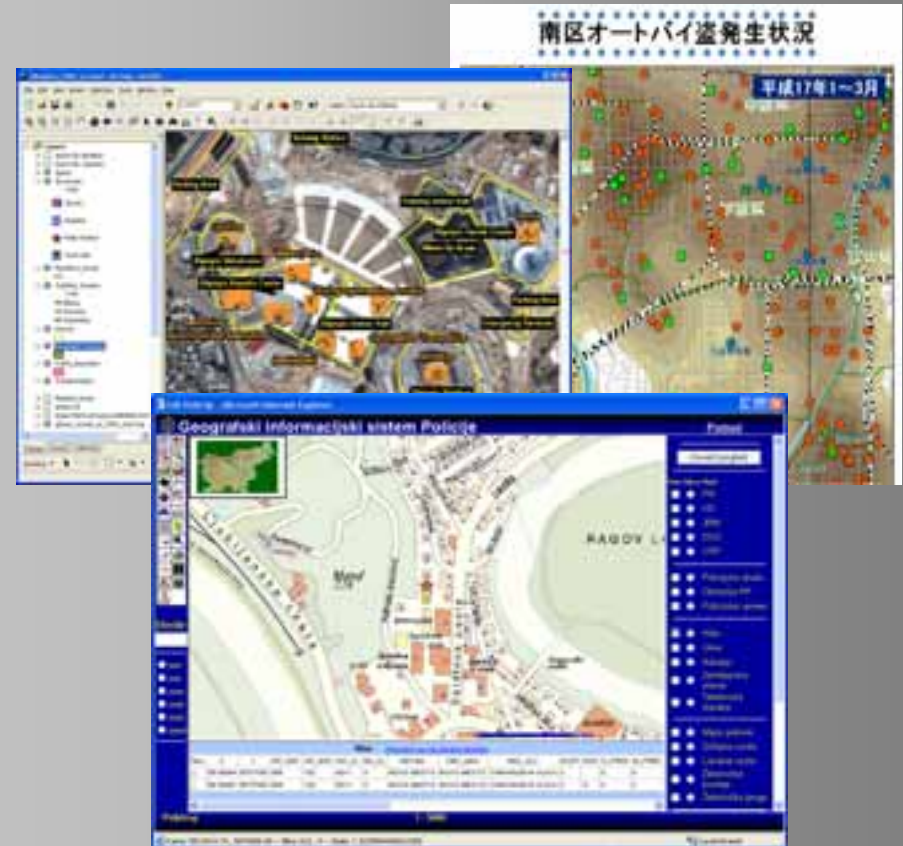
GIS: An Integrated Technology

GIS is a cross-departmental integrating technology used in all Critical Infrastructure Sectors to solve daily operational challenges.



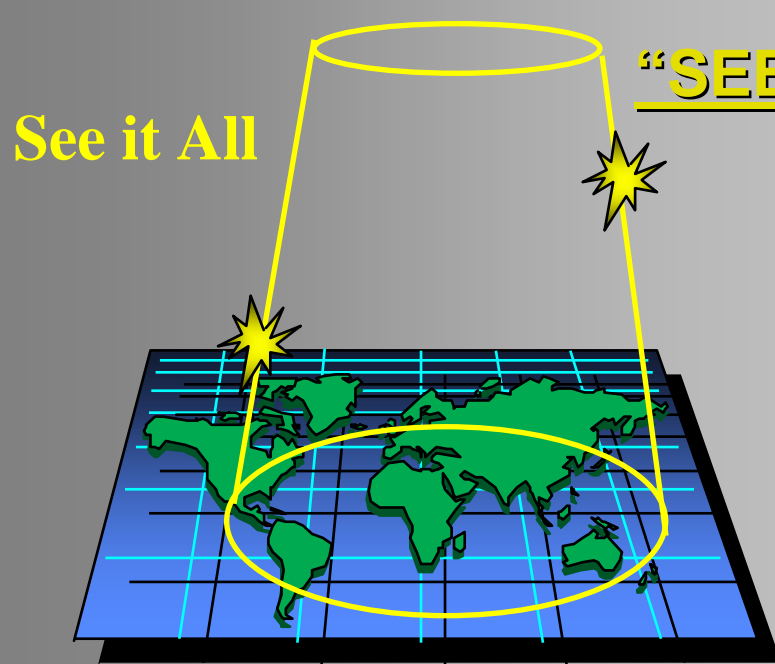
Data Fusion GIS Requirements

- An easy-to-use interface that can be queried, filtered, sorted, organized, etc. in a manner that results in meaningful information for the analysts -
 - Crime Patterns
 - Intelligence
 - Activity Flow
 - Geographic Profiling
 - Geographic Distribution
 - Association / Link Analysis
 - and much more



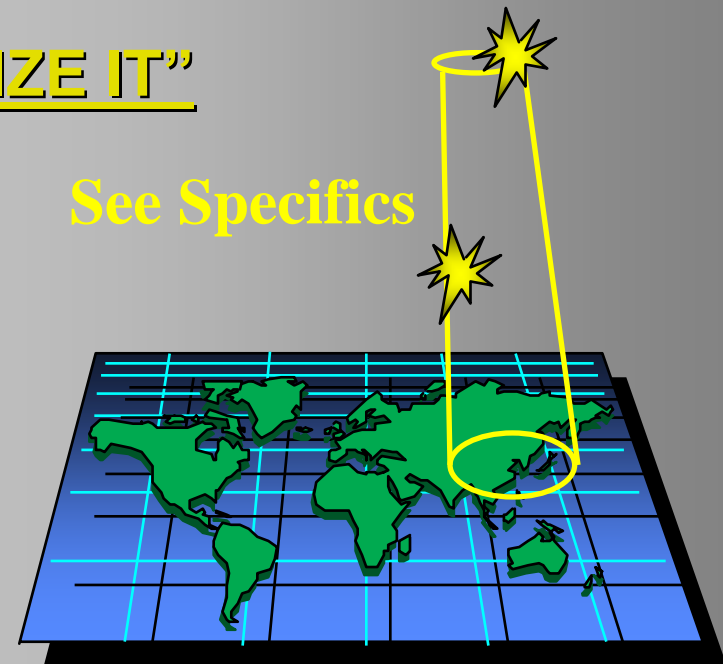
Moving Response & Command/Control Out of the Hypothetical Realm to that of “Real Time”

Exploitation of the Data

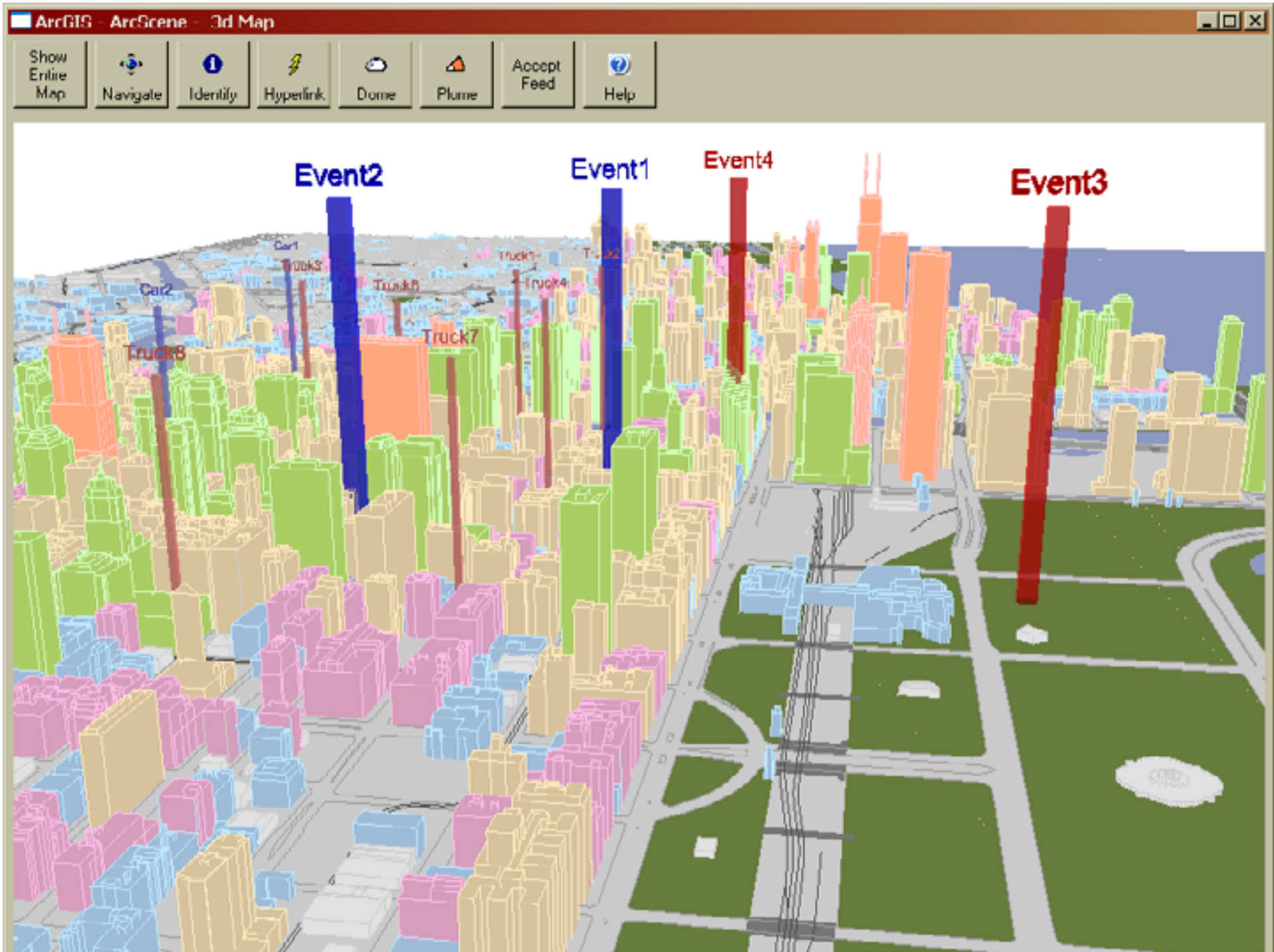


- Processes
- Trends
- Patterns
- Linkages

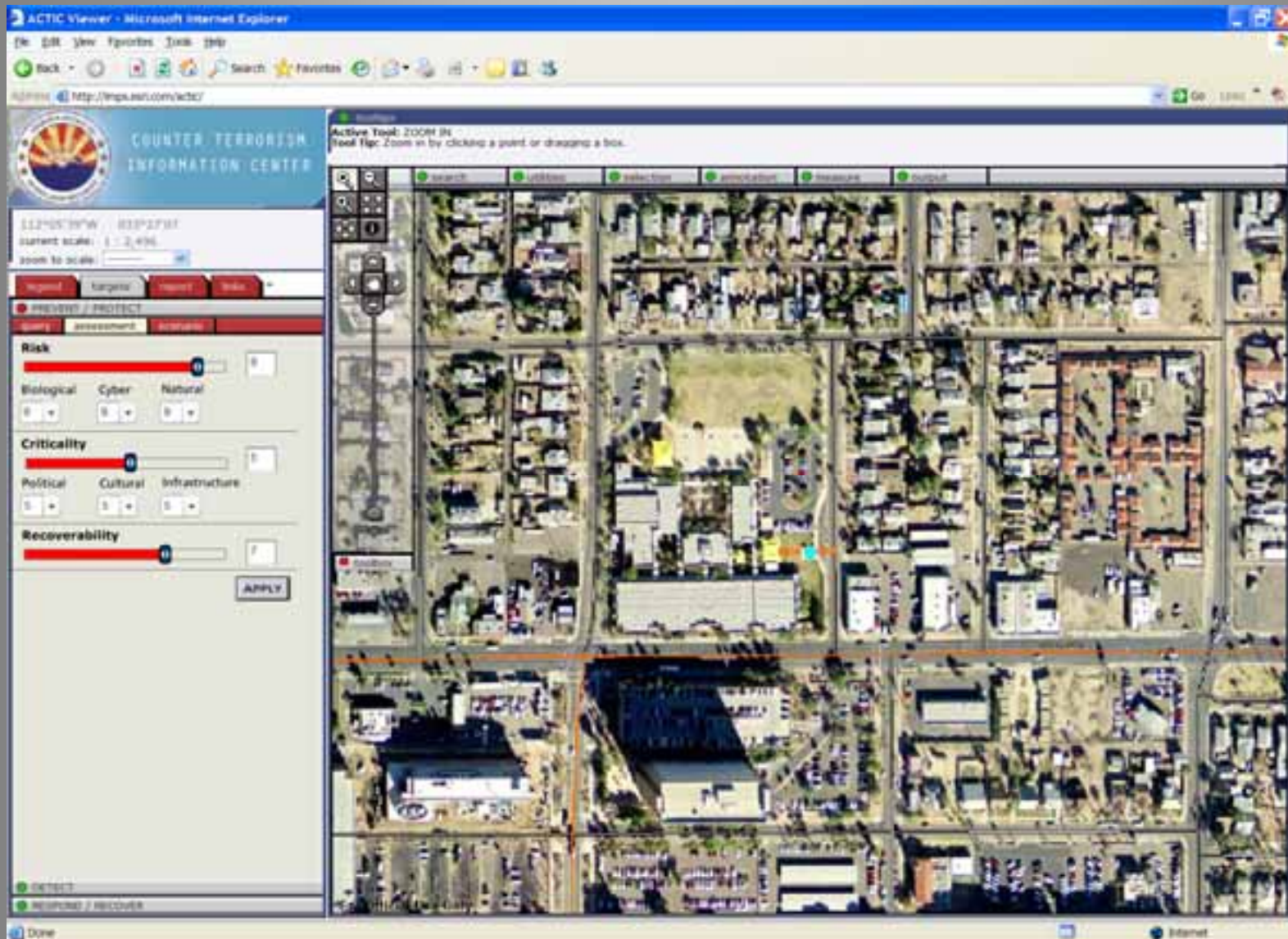
“SEE IT & SEIZE IT”



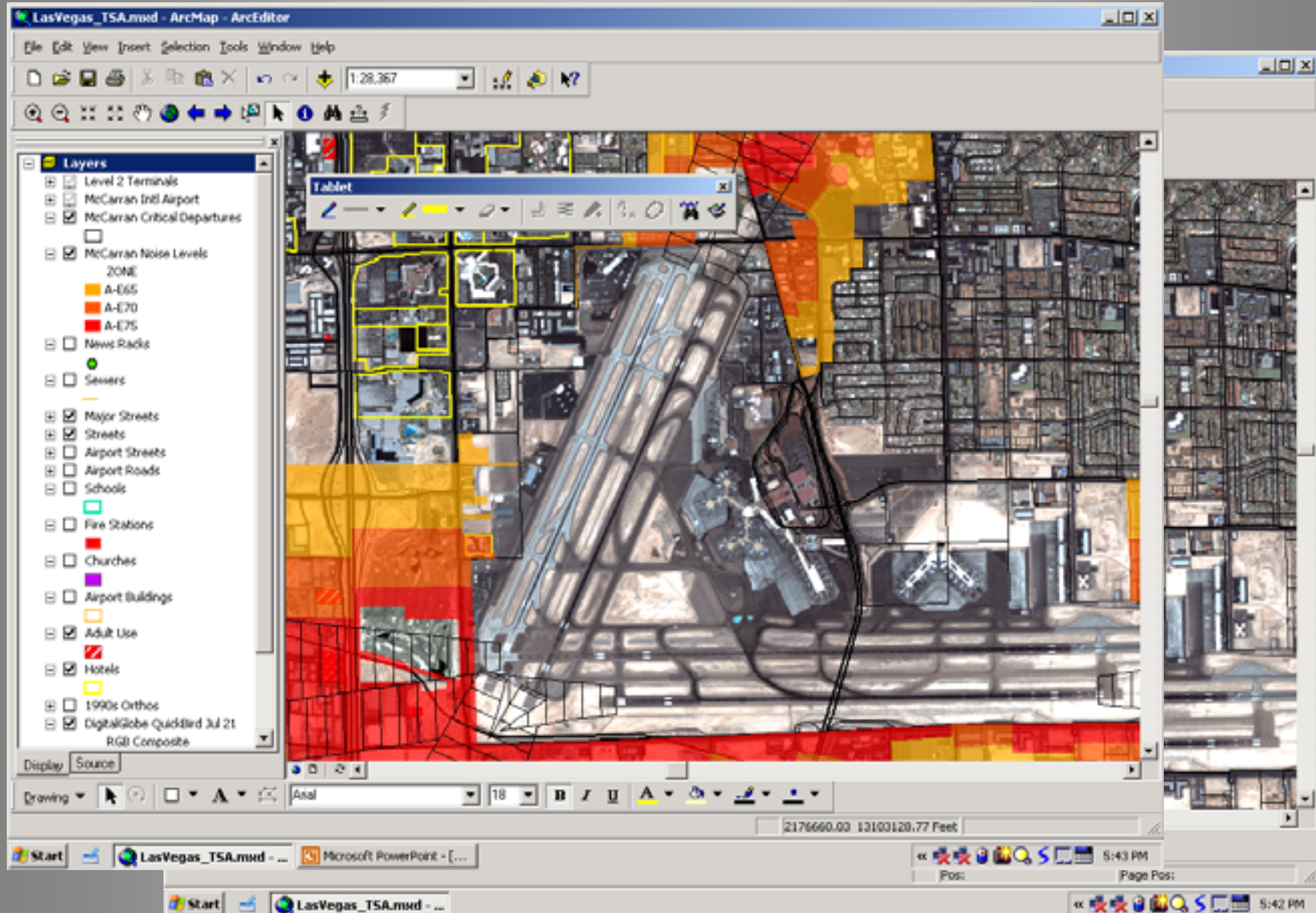
- People
- Threats
- Facilities
- Communities



Counter Terrorism COP (ACTIC) Data Fusion Center

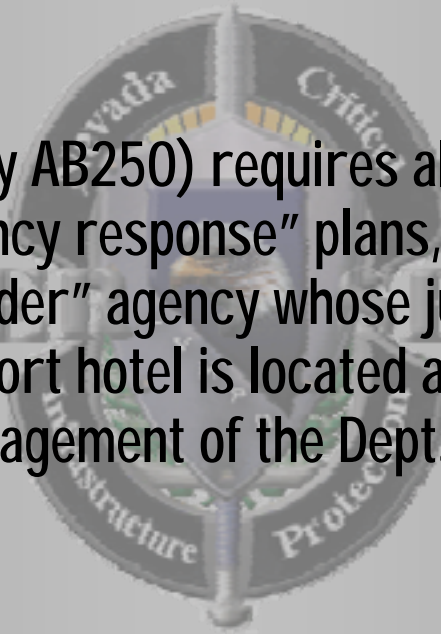


Critical Infrastructure Protection - Airport



Defining Critical Infrastructure - Emergency Response

NRS 463.790 (formerly AB250) requires all resort hotels to adopt and maintain “emergency response” plans, filed within 3 days with the local “first responder” agency whose jurisdiction includes the area in which the resort hotel is located and with the Division of Emergency Management of the Dept. of Public Safety



Epidemiological & Pandemic Alerting - Overview

- Pre-plot of Public Health Network+: Hospital ER Locations/ Community Clinics/ Veterinary Hospitals with ERs/Animal Shelters/ Food & Beverage Manufacturers- Processing Plants (? More ?) **Web-Enabled or Internet Connected!**
- GIS Map Overlays (Locality Specified)
- Deployed EPAS (Epidemiological/Pandemic Alerting System) to Public Health Network
- Analyze incoming EPAS SAR-Reports
 - Update Screening Database Continuously
- Evaluate & Activate Emergency Notification Network for Expert Analysis & Response

Epidemiological & Pandemic Alerting -

- Hospital Emergency Room
- Veterinarian ERs
- Food Processing Plants
- Scanning/Monitoring Emergency Response Channels
- Food Distribution Plants (Schools & Airlines, etc.)

Epidemiological & Pandemic Alerting - Emergency Rooms in Clark County



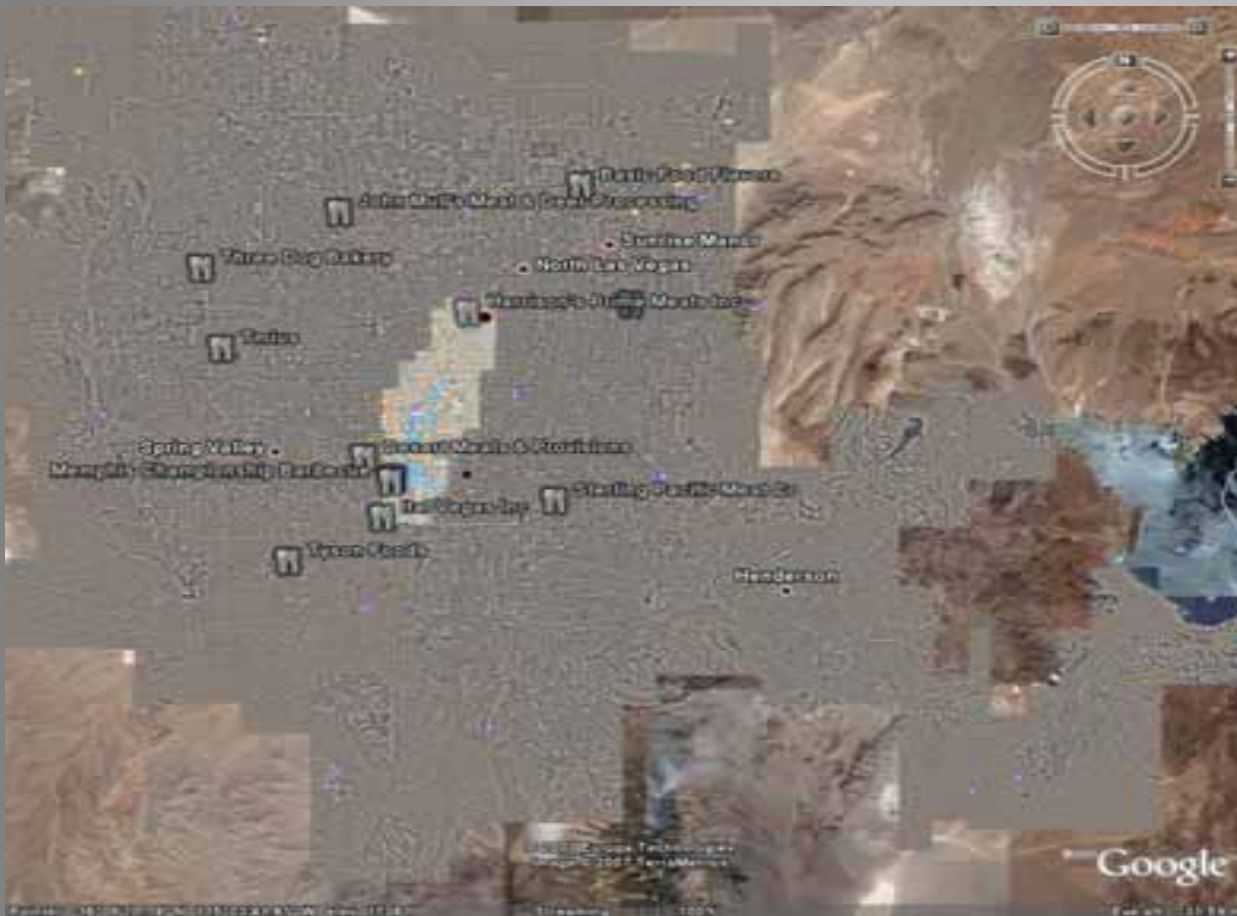
- Mountain View Hospital
- Health South Hospital of Tenaya
- Summerlin Hospital
- Lake Mead Hospital Medical Center
- Health South Rehabilitation Hospital
- Sunrise Hospital & Medical Center
- Sunrise Children's Hospital
- Montevista Hospital
- Desert Springs Hospital
- Spring Valley Hospital
- Saint Rose Dominican Hospital (San Martin Campus)
- Saint Rose Dominican Hospital (Rose de Lima Campus)
- Health South Rehabilitation Hospital
- Boulder City Hospital

Epidemiological & Pandemic Alerting - Animal Hospitals in Clark County



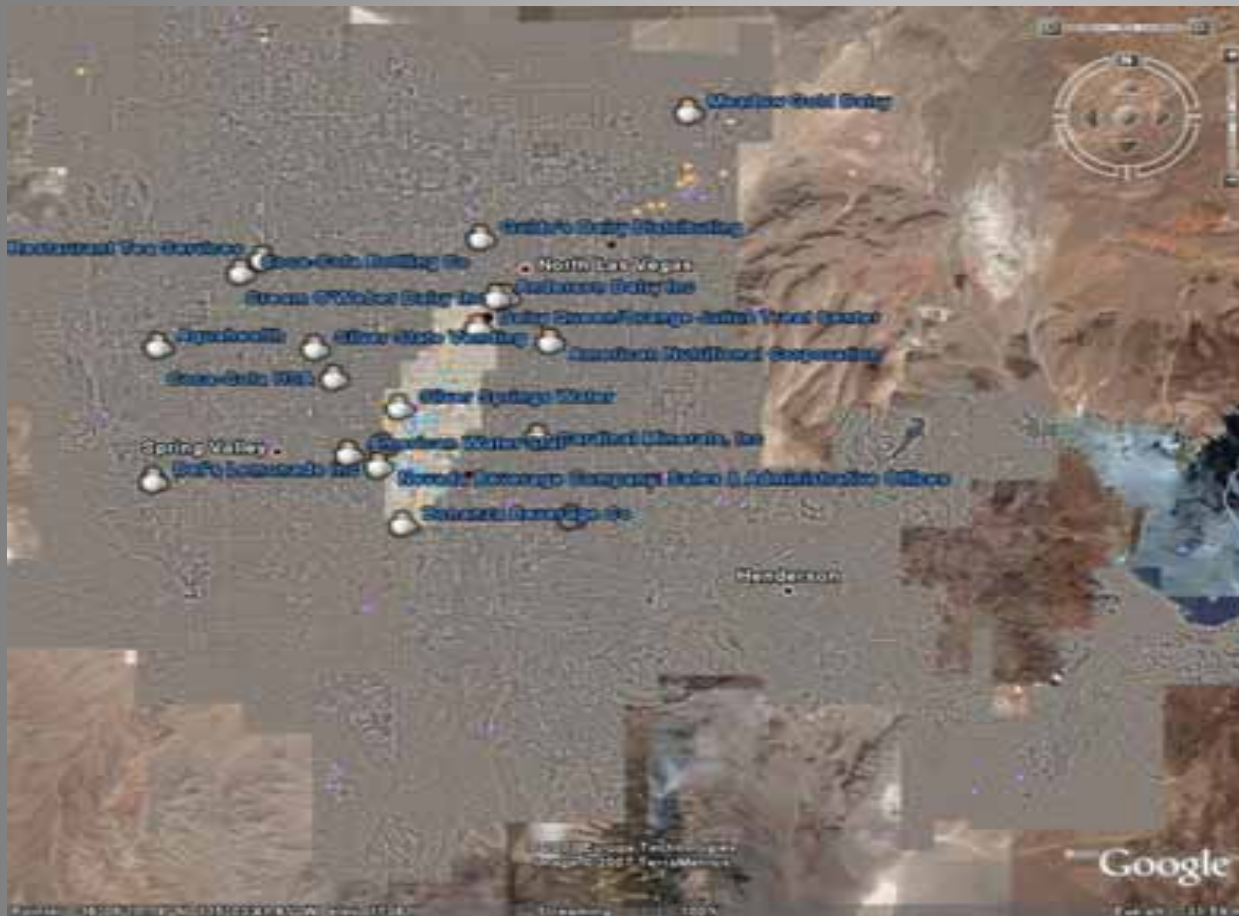
- Island Pet Hospital
- Craig Road Animal Hospital
- Lone Mountain Animal Hospital
- Ark Animal Clinic
- Rainbow Animal Hospital
- Sunrise Veterinary Clinic
- Mauer Animal Clinic
- Banfield the Pet Hospital
- Desert Inn Animal Hospital
- West Flamingo Animal Hospital
- Mountain Vista Animal Hospital
- Tropicana Animal Hospital
- Cat Care Hospital: Goldsboro Heather DVM
- Pebble Road-Maryland Parkway Animal Hospital
- Sunridge Animal Hospital

Epidemiological & Pandemic Alerting - Food Processing Plants in Clark County



- Basic Food Flavors
- John Mull's Meat & Deer Processing
- Three Dog Bakery
- Harrison's Prime Meats Incorporated
- Tmius
- Desert Meats & Provisions
- Memphis Championship Barbecue
- Sterling Pacific Meat Company
- Ital Vegas Incorporated
- Tyson Foods

Epidemiological & Pandemic Alerting - Bottling/Beverage Plants in Clark County



- Meadow Gold Dairy
- Guido's Dairy Distributing
- Restaurant Tea Services
- Coca-Cola Bottling Company
- Cream O'Weber Dairy Incorporated
- Anderson Dairy Incorporated
- Dairy Queen/Orange Julius Treat Center
- Aquahealth
- Silver State Vending
- American Nutritional Corporation
- Coca-Cola USA
- Silver Springs Water
- Cardinal Minerals Incorporated
- American Water Star
- Del's Lemonade
- Nevada Beverage Company
- Bonanza Beverage Company