

**Overview of Threat and Vulnerability  
Assessments of Critical  
Infrastructure**

**Michael Chipley, Ph.D.**



**Building for the Future  
October 22 - 24, 2002  
The Army Navy Country Club  
Arlington, Virginia**

**UTD INCORPORATED  
10242 BATTLEVIEW PARKWAY  
MANASSAS, VIRGINIA 20109  
(703) 393-0800  
FAX (703) 330-1459**

## What is driving the need for a Threat and Vulnerability Assessment and what are the objectives?

- **Legislation/Executive Directives**
- **Insurance Industry**
- **Financial Accountability Standards**
- **Nature of Threats**
- **Threat vs. Vulnerability**
- **Examples of Critical Infrastructure Assessments**
- **Summary**

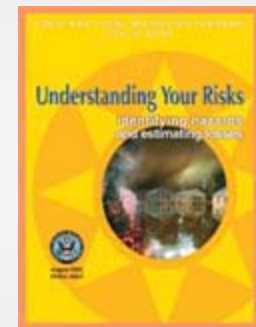
# LEGISLATIVE/EXECUTIVE



- National Security Presidential Directive 1 (G.W. Bush) and Presidential Decision Directive 63 (Clinton) – Federal government to identify and protect infrastructure
- DOD
  - TM 5-853-1/AFMAN 32-1071 Vol 1 Security Engineering
  - DOD CIP Plan
  - Antiterrorism Construction Standards 2002
  - Draft Army COE Protecting Buildings and Their Occupants From Airborne Hazards
- DOC/CIAO
  - Vulnerability Assessment Framework 1.1 Oct 1998



- **FEMA**
  - **DMA 2000**
  - **386-2 Understanding Your Risks**
  - **386-7 Integrating Human-Caused Hazards Into Mitigation Planning**
  - **FPC 66 Test, Training and Exercise Program and COOP**
  - **FPC 67 Acquisition of Alternate Facilities for COOP**
  - **HAZUS**



- **CDC/NIOSH**
  - **Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks**
  - **Draft Filtration & Air-cleaning Systems to Protect Building Environments**
- **Naval Criminal Investigative Service Crisis and Consequence Exercise Handbook**



# LEGISLATIVE/EXECUTIVE



- **The Partnership for Critical Infrastructure (PCIS)**
  - <http://www.pcis.org/>
- **The Infrastructure Security Partnership (TISP)**
  - <http://www.tisp.org/>



# INSURANCE INDUSTRY



- Insurance Industry and Federal Government promulgating definitions and coverage for terrorism insurance
- Define and quantitize risk
  - Risk is higher when located near federal properties, ports, tunnels, bridges, etc
- Liability exposure/responsible party
- Government and private company bond and debt ratings directly affected

**GASB Statement No. 34, *Basic Financial Statements-and Management's Discussion and Analysis-for State and Local Governments* (and related pronouncements), is effective beginning after June 15, 2001.**

**Under the new standard, anyone with an interest in public finance—citizens, the media, bond raters, creditors, legislators, and others—will have more and easier-to-understand information about their governments.**

- **Include for the first time information about the government's public infrastructure assets—such as bridges, roads, and storm sewers**

# NATURE OF THE THREAT



- **Government, business, and the general public have experienced first hand the disruption in mission, service, and business continuity due to large scale events/threats (hurricanes, terrorism, etc.)**
- **A threat can be a natural disaster, act of war, act of terrorism, or accident that impacts mission capability or business continuity**
- **Recovery and reconstitution can be in hazardous conditions for extended periods of time**

# THREAT VS VULNERABILITY



- **A threat assessment is usually conducted by intelligence and law enforcement**
  - **General Threat Scenarios/Spectrum**
  - **Specific Threat**
- **A vulnerability assessment is typically conducted by A&E, Physical Security, specialty expertise firms/agencies (DTRA, Army COE, Sandia, etc.)**
- **Objective is to evaluate systems and interdependencies in some quantifiable form:**
  - **Risk**
  - **Criticality**
  - **Recoverability**

# THREAT EVALUATION



| THREATS | TOOLS | SYSTEM ELEMENTS |
|---------|-------|-----------------|
|---------|-------|-----------------|

Accidents

Criminal Activity

Espionage

Cyber Attack

Terrorism

Civil Unrest

Natural Disaster

Technological Failure

Conventional Warfare

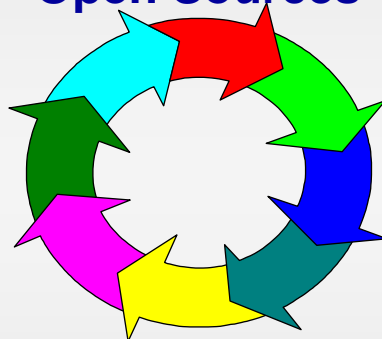
WMD

Models

Observation

Interviews

Open Sources



Population Dynamics

Red Teams

SPV Analysis

Lessons Learned

Structural Protection

Physical Security

Communications

Emergency

Preparedness

Fire Protection

Utilities

Information Assurance

Damage Control/Recovery

Key Positions

EM/Lightning Protection

## ASSET VULNERABILITIES

# INFRASTRUCTURE ASSESSMENT



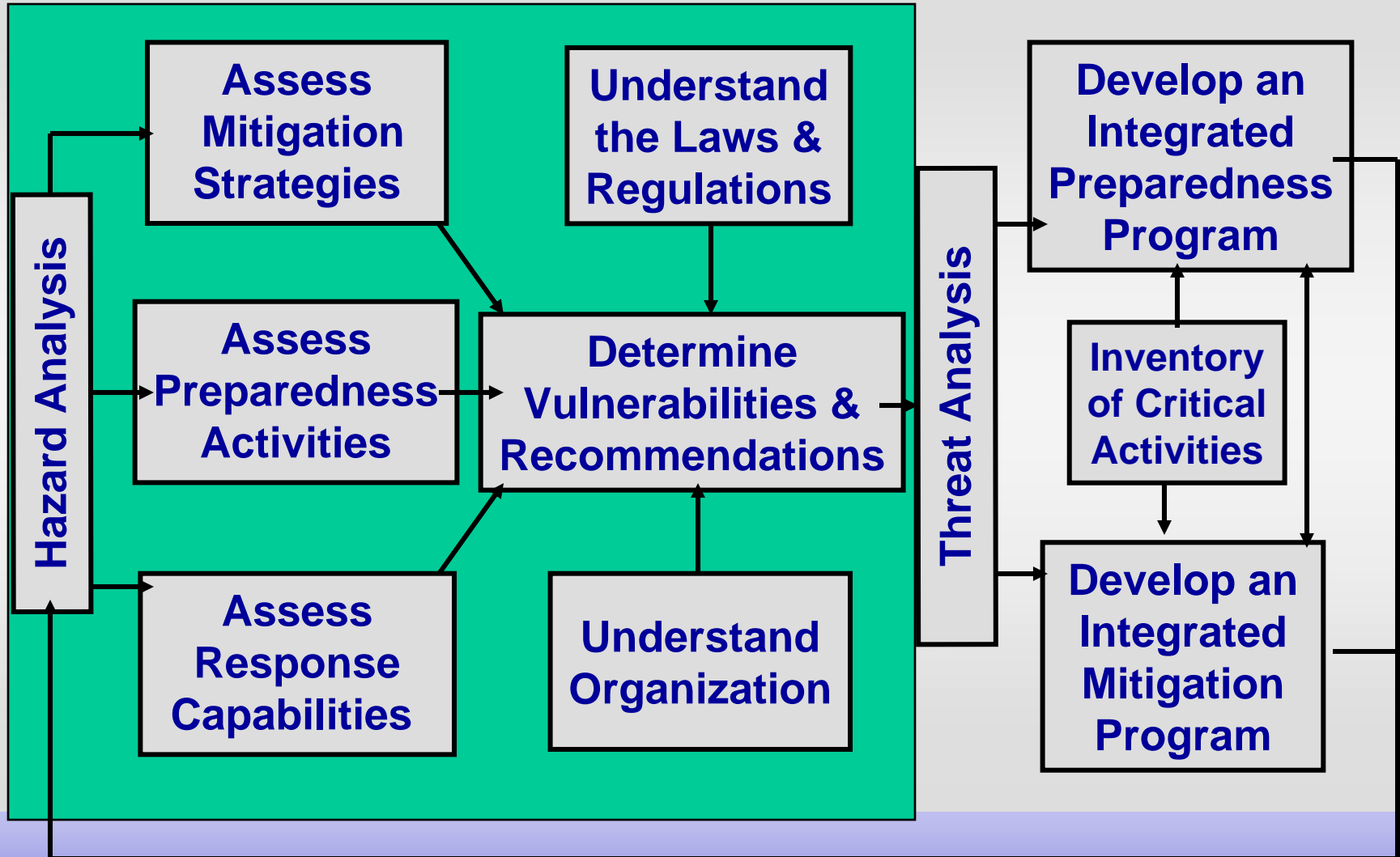
- Objectives
  - Ensure The Continuity Of The Mission/Operation
  - Protect People, Infrastructure and Resources
- Understand Which Locations, Nodes, Networks, And Elements Are Critical To The Mission
  - Identify Single Point Vulnerabilities (SPV)
  - Not Everything Is Critical
- Look At The Critical Elements For Vulnerabilities And Recommend Solutions
- The Three-Phase Process:
  - Phase I: Establish the Minimum Critical Infrastructure (MCI)
  - Phase II: Data Collection to Identify MCI Vulnerabilities
  - Phase III: Analyze and Prioritize Vulnerabilities

# PHYSICAL ATTACK



- **Explosives**
- **Gun/Ballistic**
- **Sabotage**
- **Vandalism**
- **IT systems**
  
- **Radiological**
  - **Dirty Bomb**
  - **Man portable low yield**
  - **Tactical (artillery, aircraft)**
  - **Strategic**
  
- **Biological**
  - **Anthrax**
  - **Smallpox**
  - **Dengue Fever**
  - **Equine Encephalitis**
  - **Ebola**
  
- **Chemical**
  - **Nerve (Sarin, VX, GX)**
  - **Blood**
  - **Choking**
  - **Blister**

# A FRAMEWORK FOR ASSESSMENT



# FACILITY SYSTEM INTERACTIONS



Damage Mechanisms:

**WEAPONS & ATTACKS**

Facility Systems:

Delivery

**PROTECTION FUNCTION**  
• EMP  
• Structure  
• Security  
• NBC

Penetration

**CRITICAL COMPONENTS**  
• **Support Function**  
• Operation Function  
• Personnel

System Defeat

**PROTECTION FUNCTION**  
• Damage Control & Recovery (Int & Ext)

Functional Defeat:

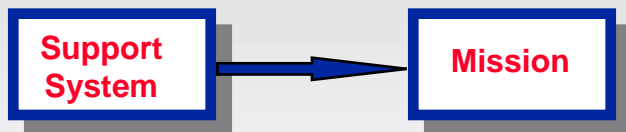
**DAMAGE EFFECTS**  
• Mission Defeat  
• Downtime  
• % Degradation

Critical Function Failure

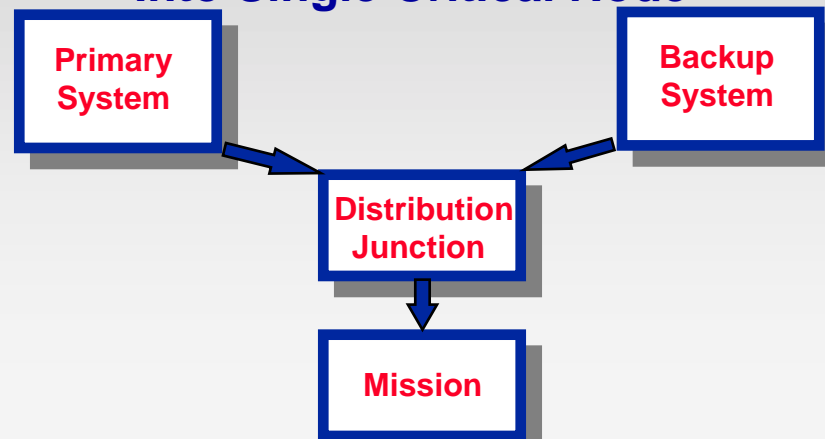
# COMMON SYSTEM VULNERABILITIES



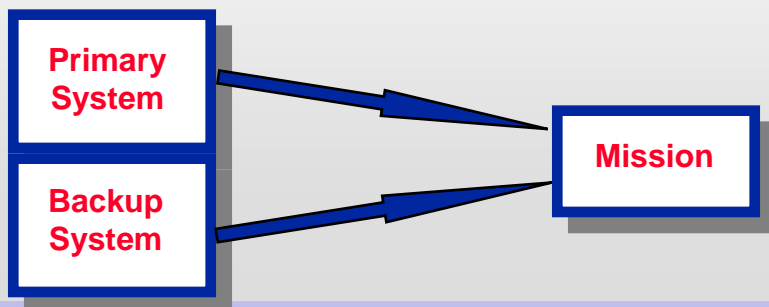
## No Redundancy



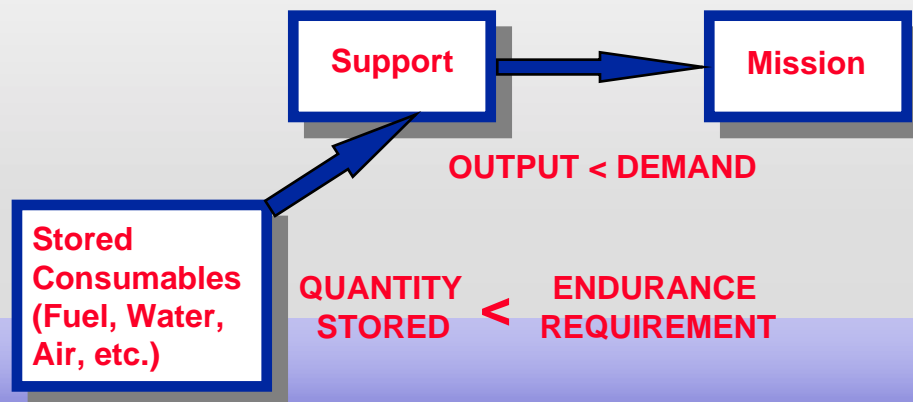
## Redundant Systems Feed Into Single Critical Node



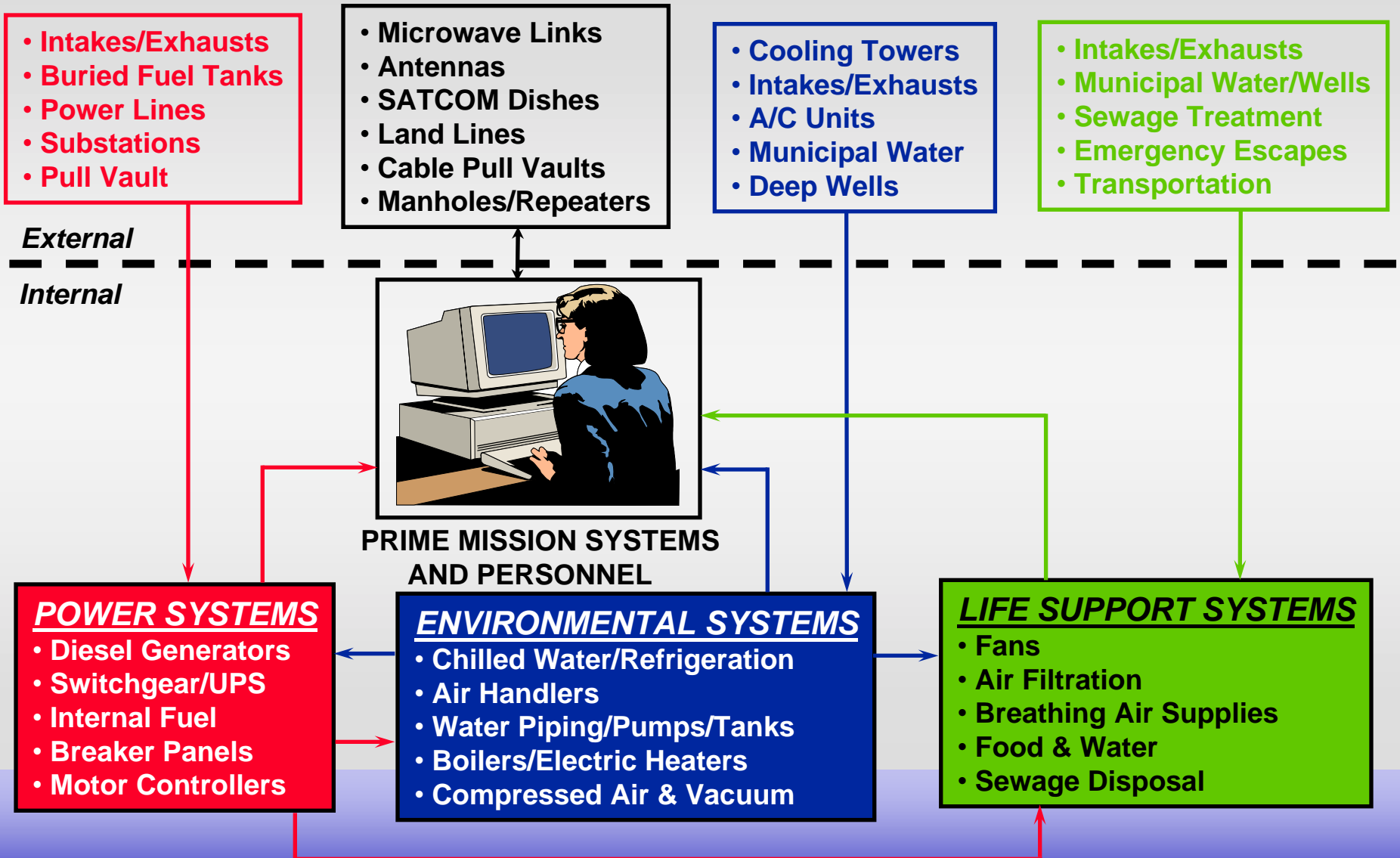
## Critical Components of Redundant Systems Collocated



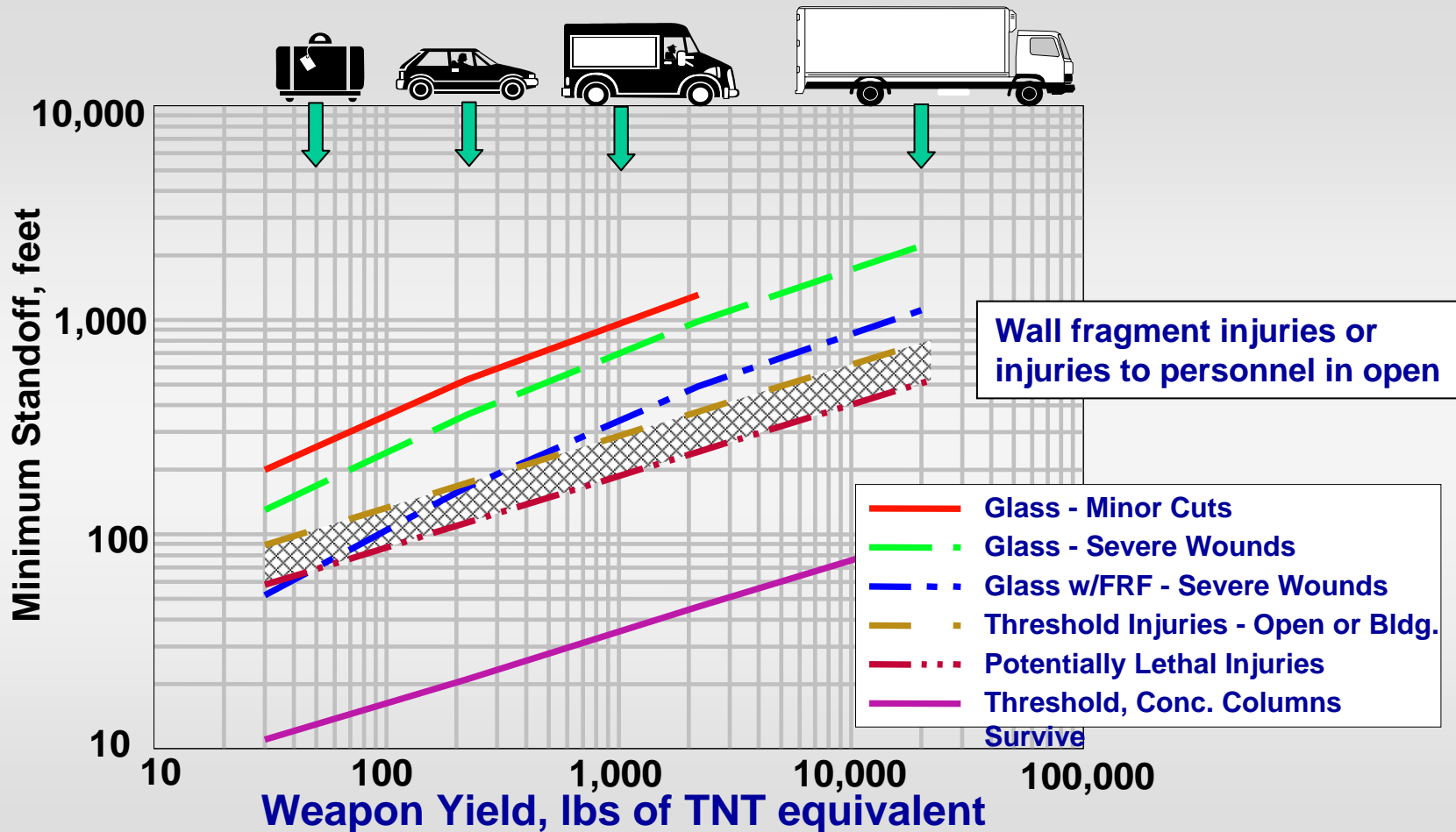
## Inadequate Capacity or Endurance in Post-Attack Environment



# UTILITY SUPPORT SYSTEMS



# EXPLOSIVES ENVIRONMENTS



**Key concerns are glass shards and structural collapse**



# ASSESSMENT TOOLS



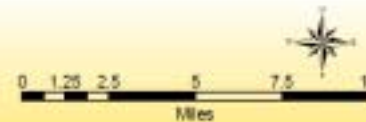
A screenshot of a software application window titled "UTD\_Demo - ArcMap - ArcView". The interface is divided into several sections. On the left, there is a vertical sidebar with the UTD INC. logo at the top and a list of regional buttons: US, East, Central, West, and Regional. The main central area displays a map of the Eastern United States, with state boundaries and major cities like Detroit, Cleveland, Columbus, Washington, and Charlotte marked. Above the map is a standard ArcView toolbar with various navigation and tool icons. To the right of the map is a vertical column of buttons for different assessment types: North, South, East, West, Front Entrance, Deck, Telecom, CAD Drawing, Energy Management, Interior Fly Through, and Video. At the bottom of this column is a "Close Form" button. On the far right, there are two image panels. The top panel shows four small photographs of building exteriors from different perspectives. The bottom panel shows a detailed architectural floor plan of a building, with various rooms and structural elements highlighted in different colors.

# GIS FACILITY INFORMATION

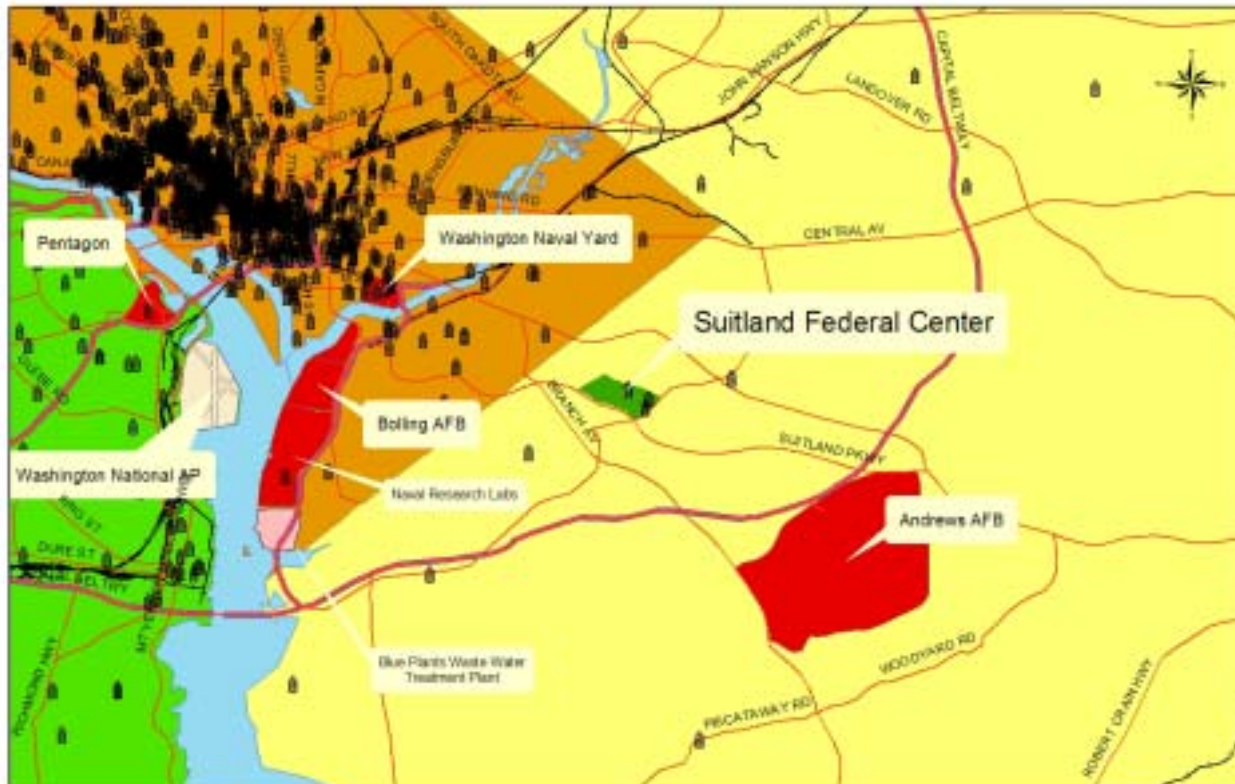


## 10 Mile Campus Buffer

Census Bureau - Sulland Federal Center



# GIS FACILITY INFORMATION

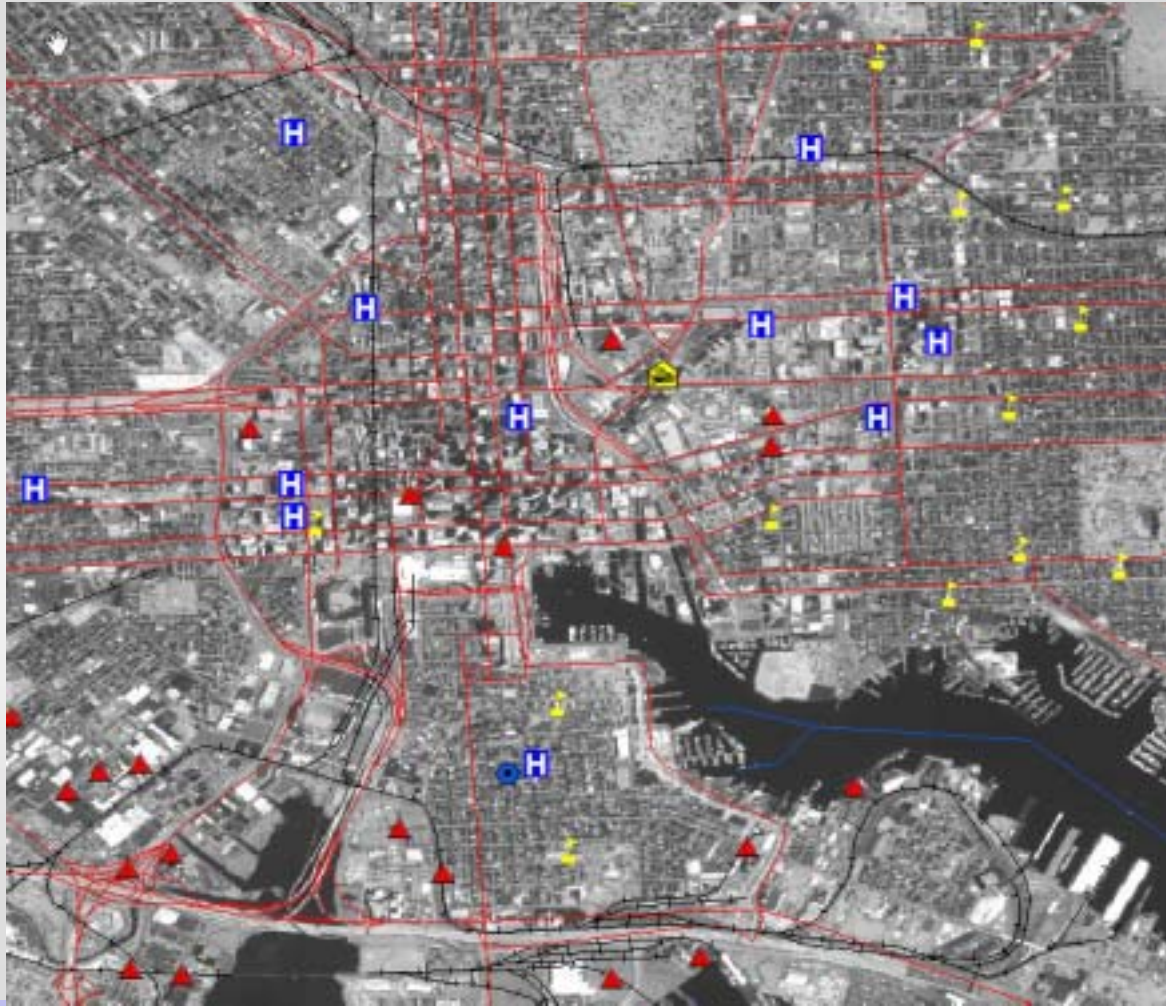


## Public and Federal Buildings

Census Bureau - Suitland Federal Center



# GIS FACILITY INFORMATION

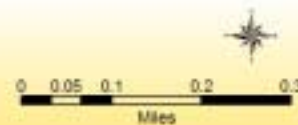


# GIS FACILITY INFORMATION

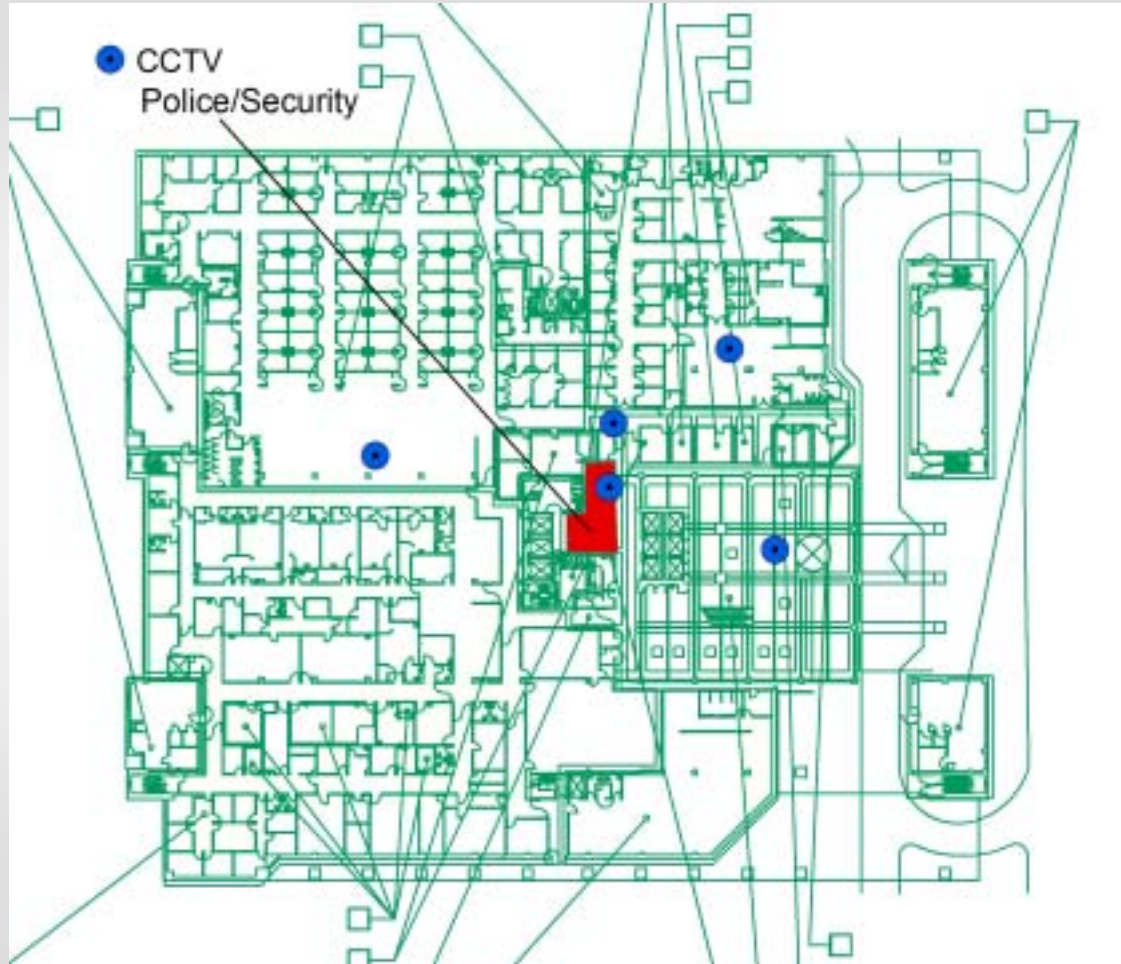


## Suitland Federal Center Imagery

Census Bureau - Suitland Federal Center



# GIS FACILITY INFORMATION



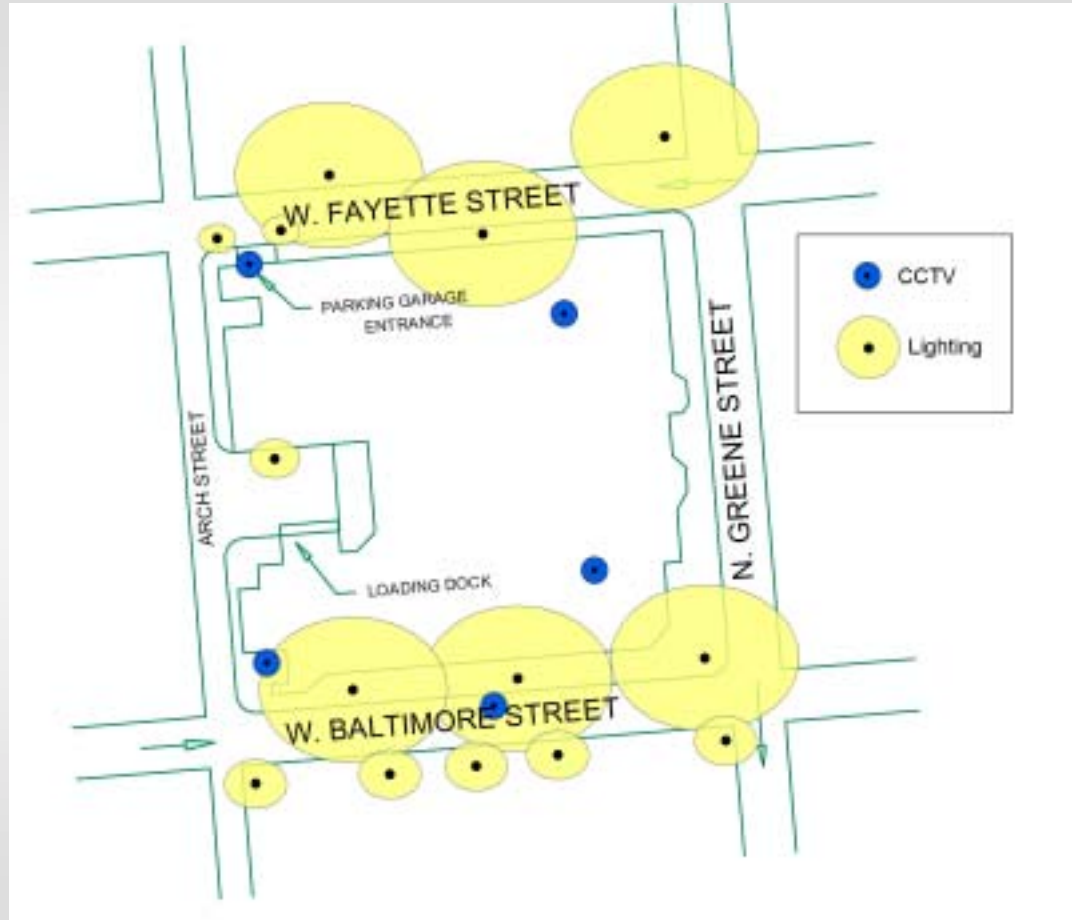
- Security with no Alternate Site, Off Main Lobby

# GIS FACILITY INFORMATION



- Interior Loading Dock, Warehouse, Mailroom

# GIS FACILITY INFORMATION



- **CCTV Blind Spots, Vehicle Control**

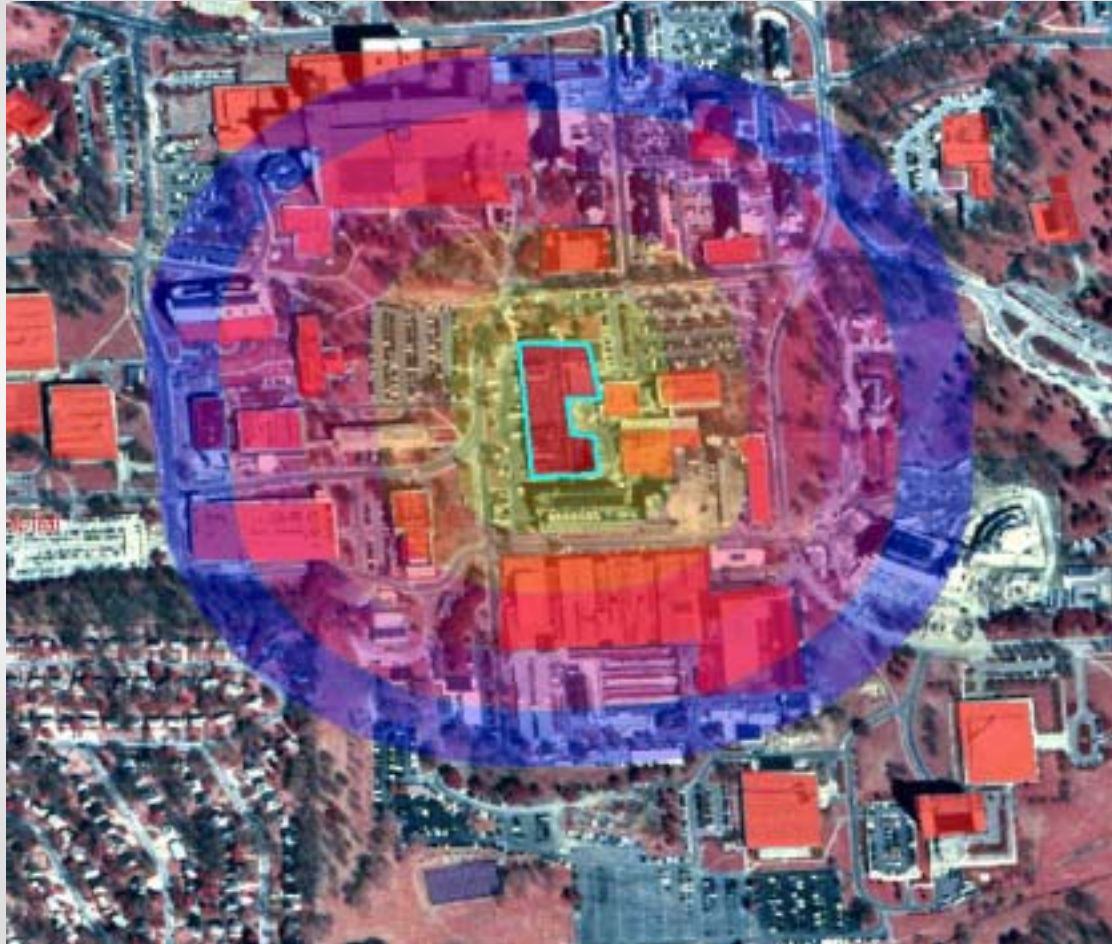
# GIS FACILITY INFORMATION



# GIS FACILITY INFORMATION



# GIS FACILITY INFORMATION



# GIS FACILITY INFORMATION



## Census Bureau Imagery

Census Bureau - Suitland Federal Center



# GIS FACILITY INFORMATION



# CAFM FACILITY INFORMATION



# CAFM FACILITY INFORMATION



CAFM02 (c) 1996-2002 CAFM Incorporated. Licensed to UTD

File Edit CAD Help

PLANNING PROJECTS ASSESSMENT PROPERTY UTILITIES MAINTENANCE

Conditions & Codes Security

Owner: VA | General Info | Project List

Project: BOSTON2002 | Item No.: 4 | User ID: CAFM | Team: | Date: 08/24/2002

Site Name: CLINICAL ADDITION | GPS Lat: | Long: |

Fac./Asset: 100 | Name: SURGERY

Location ID: 102 | Use: DAY SURGERY WAITING | Pr./El: |

Attributes: LAND | Cat: Physical Security | Sub-Cat: Lock and Key Control

Benchmark -> Facilities have established proper key control and accountability practices.

Questions



Best Practice

Observation: 1 Does not meet | Classification: C | Mitigation: | Threat: | Organization: |

Scope: | Priority: 1 | Est. Cost: \$1,500.00

Directory: DEMOPROJ | Fix File: | Dwg File: |

VA\_BOSTON.dwg | 1001-A1.dwg



# VFA FACILITY INFORMATION



VFA Facility - practice - Microsoft Internet Explorer

**vfa Asset Data**    Asset Data    Funding Analysis    Project Planning    Reports    My Account  
Import    Custom Links    Help    Logout

UTD Region / A University / Buildings

View    List    Save    Delete    Print

|                    |                           |                      |                                  |
|--------------------|---------------------------|----------------------|----------------------------------|
| Campus:            | A University              | Use:                 | A3. Fire                         |
| Name:              | Firehouse                 | Construction Type:   | D Business and Personal Services |
| Blg No.:           | 101a                      | Date Constructed:    | 1945                             |
| St Address:        | Canal St                  | Date Renovated:      |                                  |
| Cost Model:        | Fire Station Single Story | Architect:           |                                  |
| Stories:           | 1                         | Historical Category: | [none selected]                  |
| Gross Area:        | 120.000                   | Facility Type:       | Building                         |
| Replacement Value: | \$10,300,000              | Campus Map Coord:    |                                  |
| PCI:               | 0.00                      |                      |                                  |

Estimation

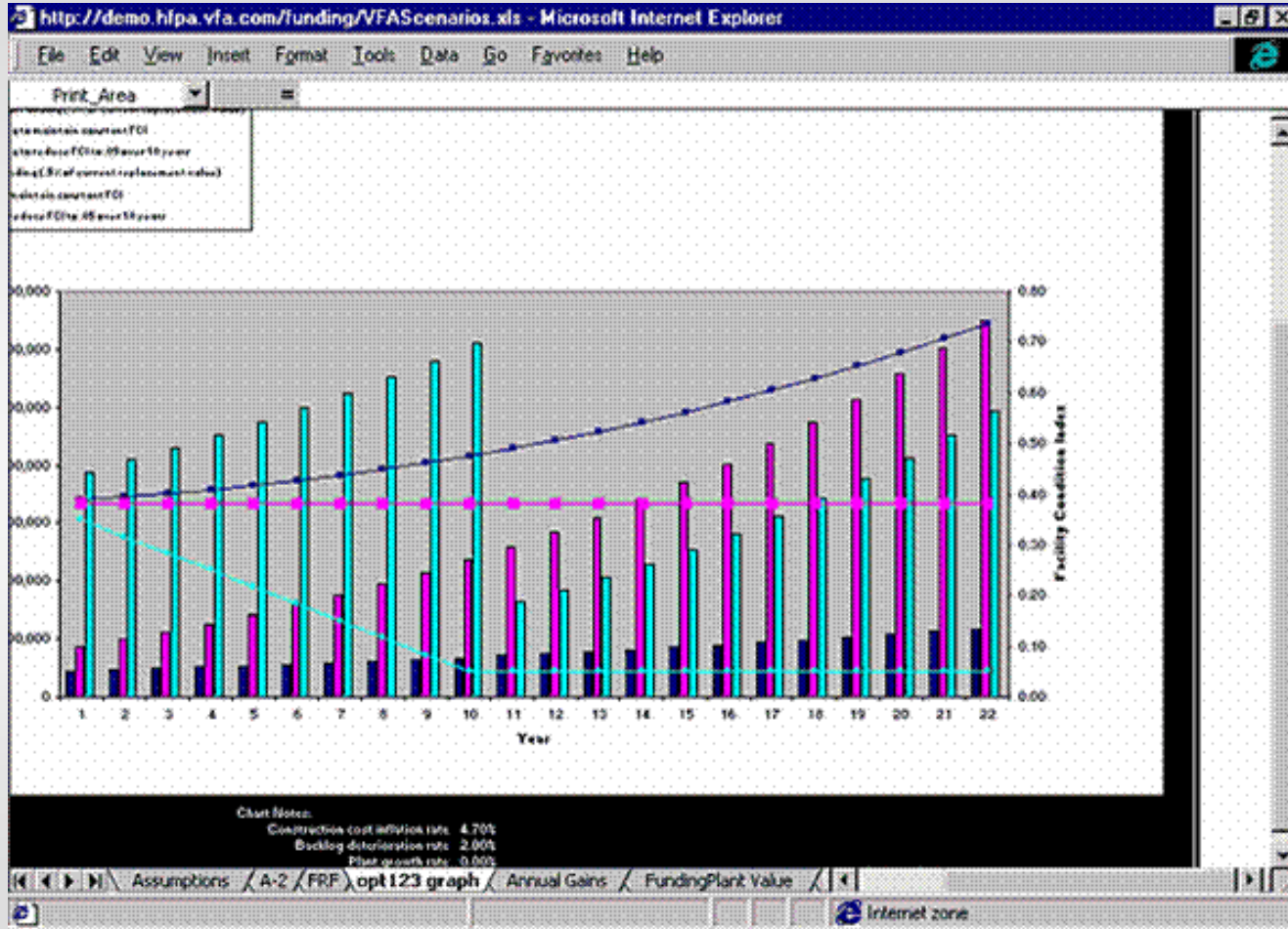
U.S. Means State: [none selected]

Description

| System Lifecycles |        |             |             |
|-------------------|--------|-------------|-------------|
| Uniform Category  | % Used | % Deficient | Valid as of |
|                   |        |             |             |

Building: Firehouse.    1 of 1    Internet

# VFA FACILITY INFORMATION



# EMERGENCY MANAGEMENT



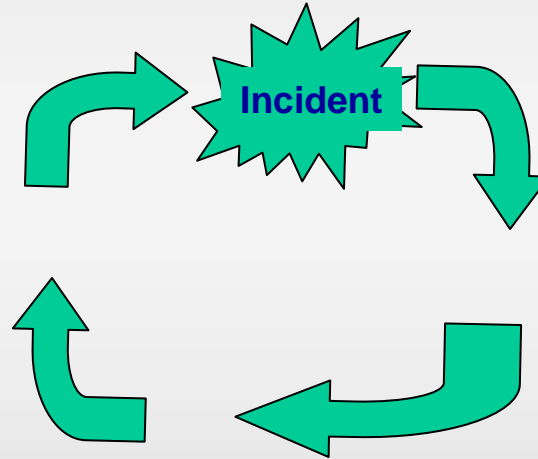
**Preparedness**--activities that prepare for an effective response to an emergency



**Mitigation**--activities that eliminate or reduce the effects of a disaster



**Response**--Immediate activities that occur during and immediately following a disaster.



**Recovery**--longer-term activities to return all systems to normal, or near normal

# EMERGENCY MANAGEMENT



**Response:** activities that occur during and immediately following a disaster to prevent further loss of life or property

**Organizational  
Response**

**Local  
Response**

## Typical Response Activities

Emergency Alert  
Evacuation  
Accountability  
Notification  
Damage Control  
Hand-off Procedures  
Continuity of Opns.  
Family Support  
Survivor Support

Emergency Dispatch  
Incident Command  
Fire Fighting  
Search & Rescue  
On-Scene Security  
Emergency Medical  
Ambulance Support  
Hospital Support  
Mortuary Support

Emergency Comms.  
Bomb Disposal Spt.  
HAZMAT response  
Decontamination Spt.  
Emergency Utilities  
Engineering Spt.  
Law Enforcement Spt.  
Public Affairs

# EMERGENCY MANAGEMENT



**Mitigation:** activities that eliminate or reduce the adverse effects of a disaster

**Risk  
Avoidance**

**Risk  
Reduction**

## Typical Mitigation Tools

### Tool

### Examples

|                     |   |
|---------------------|---|
| Limit Access        | Vehicle Entry Control/Barriers          |
| Structural Measures | Façade hardening, window film           |
| Public Information  | Flood plain maps, awareness & education |
| Replace Property    | Flood Insurance                         |

# SUMMARY



- **Conduct a Vulnerability Assessment**
- **Evaluate Risk, Mission Continuity, Recoverability**
- **Develop/update Emergency Response and Disaster Management Plans**
- **Conduct Table Top and Full Scale Exercises**