



# State Energy Assurance Guidelines

## Overview and Use

**Blue Sand Exercises**  
Indianapolis, Indiana  
June 7, 2005

**Jeffrey Pillon**, Chair, NASEO Energy Data and Security Committee; &  
Chair Staff Subcommittee, NARUC Ad Hoc Committee on Critical Infrastructure

**Don Milsten**, Senior Associate NASEO

# Emergency Preparedness and Response



**Protecting Critical Infrastructure**

# Protecting Critical Energy Infrastructure

- Defining Critical Infrastructure
- Components of Critical Infrastructure Protection
- Protection of Sensitive information
- Diversification of Energy Sources and increased efficiency



# Cyber Security

- Work to defend against, detect, and react to cyber attacks.
- Examine the physical security of control systems and the locations of servers and backup capability.
- Promote awareness of cyber & communication threats and mitigation techniques



# Responding to an Energy Emergency

- Communications and Assessment – who talks to who, when about what.
  - Internal Communications
  - External Communications
- Response -- who does what, when.
- Energy Emergency Assurance Coordinators



Citgo Refinery in Lemont, Illinois  
August 2001

# Purpose of the Guidelines

Provide state energy and emergency officials with tools for understanding and reviewing how their jurisdictions respond to energy outages and how to improve the energy emergency plans that guide this response.

The Guidelines are a compilation of information from many state energy and emergency officials who have experienced and responded to energy emergencies.

## Response -- What Questions Should you Ask?

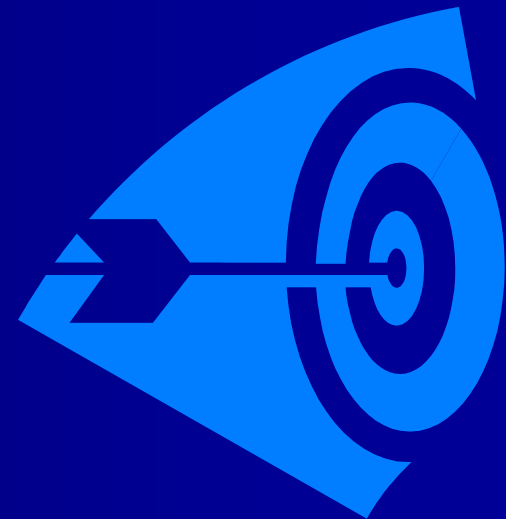
- Is there a shortage and how long might it last?
- What geographic areas are effected?
- What specific energy types are effected?
- How short is supply compared to demand?
- What are the possible consequences of the shortage and interdependencies?
- Who should be contacted and in what order?
- What energy providers should respond - how and how quickly?

# How Does a State Proceed from Asking Questions to Providing Answers?

- The Guidelines:
  - Discuss major planning issues
  - Suggest Crisis Management Strategies
  - Encourage Pre-Crisis Preparation
  - Emphasize Good Data Collection and Analysis
  - Identify Possible Response Actions

# Key Elements for Success

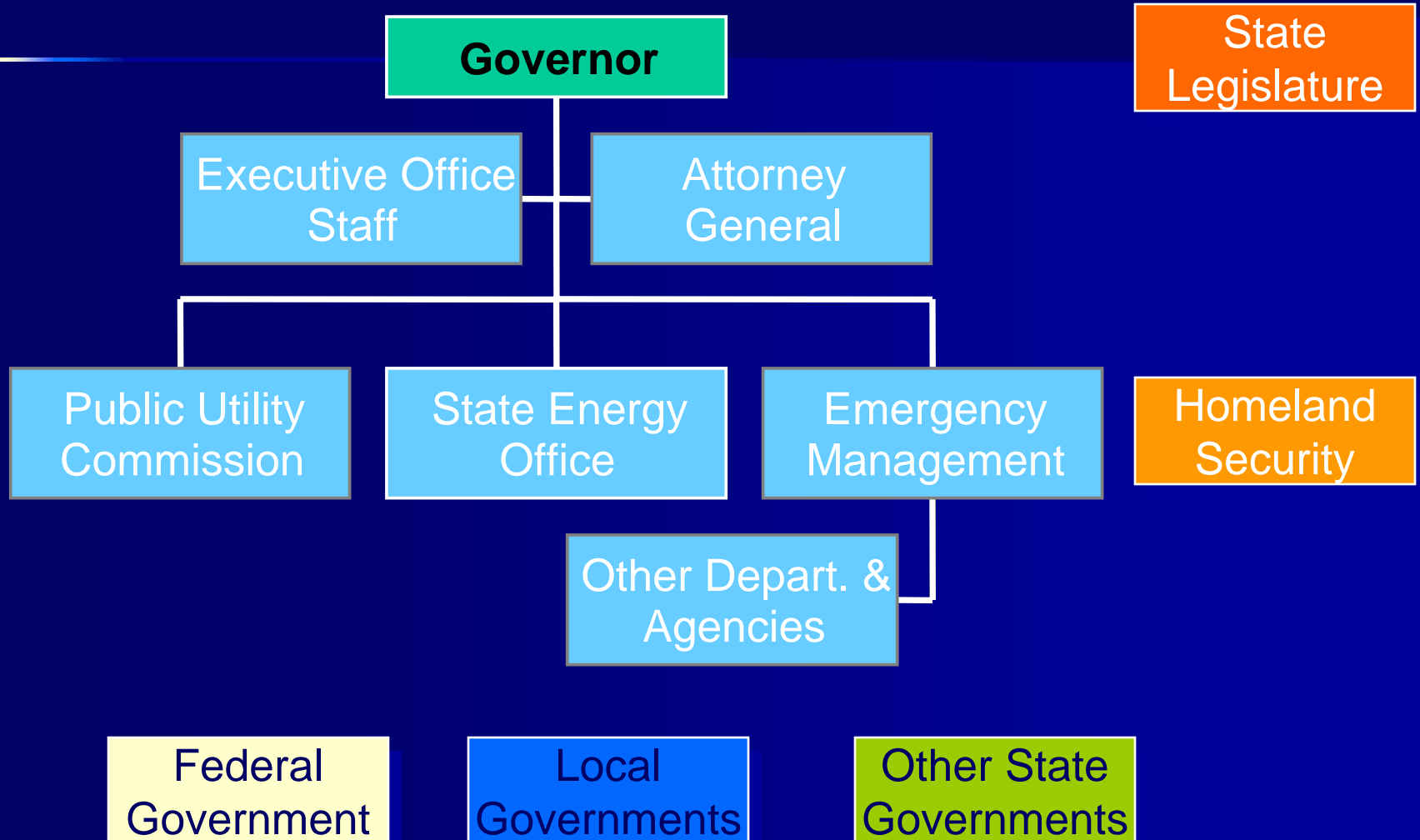
- Communication and Coordination across all jurisdictions, sectors and professions.
- Building Relationships
- Developing Public/Private Partnerships
- Use existing structures, programs and build off what has worked



## Define and Clarify Organizational Relationships and Responsibilities

- Legal Authority
- Relationship of Legal Authority to a State's Emergency Plan
- The Relationship Among State Agencies and Federal, and Regional Authorities
- Energy Assurance Planning for Utilities

# State Energy Emergency Organizations



# Principal Strategies for Managing an Energy Disruption/Shortage

- A. Assessment – What Going On
- B. Stages of an Energy Emergency
- C. Energy Emergency Response Matrix
- D. Severity of an Energy Emergency
- E. Understanding a State's Energy Profile & Vulnerabilities
- F. Important Elements to Consider in Designing Emergency Response Measures

## Response Measures considering:

### **A. Electricity**

- Generation, Transmission, Local Distribution, Restoration, Mutual Aid Agreements, Restructuring

### **B. Natural Gas**

- Pipelines, Local Distribution Companies, Restoration, Deregulation

### **C. Petroleum**

- Gasoline, Distillate, Propane

# Public Information

1. Public Information Programs and Objectives
2. Functions of a Public Information Program Coordination
3. Operational Considerations
4. Data and Information Acquisition and Dissemination
5. Equipment Requirements

# Additions to Version 2 of the Guidelines

- Section II – NARUC on Critical Infrastructure
- Section III – NARUC Inventories
- Section IV – Energy Emergency Assurance Coordinators Web Site
- Section V – Natural Gas Shortage Response
- Section V – RTO/ISO Emergency Response
- Appendix F – Petroleum Fuel Set-Aside

# Questions About the Guidelines?

**From Planning to Use:  
Dealing with a  
Real Emergency**

# The Consequences



**September 11, 2001**

## **World Trade Center/Pentagon**

- 2,800 Deaths
- Economic Impact: \$83 billion

**April 19, 2001**

## **Oklahoma Bombing**

- 168 Deaths
- 675 Injured



# The Consequences-At Home



2001

## Anthrax-Laden Mail

- 5 Deaths
- 22 Injured
- Remediation Costs: \$41.7 million



# The Consequences-All Hazard



May 14, 2003

## Marquette, Michigan Flood

- Economic Impact: \$102 million
- Evacuees: 1,900
- Lost Roads, Bridges (9), Dams (3)
- Idled Coal Mines

June 8, 1953

## Genesee County, Michigan F5 Tornado

- 116 Dead
- 785 Injured



# The Consequences-All Hazard

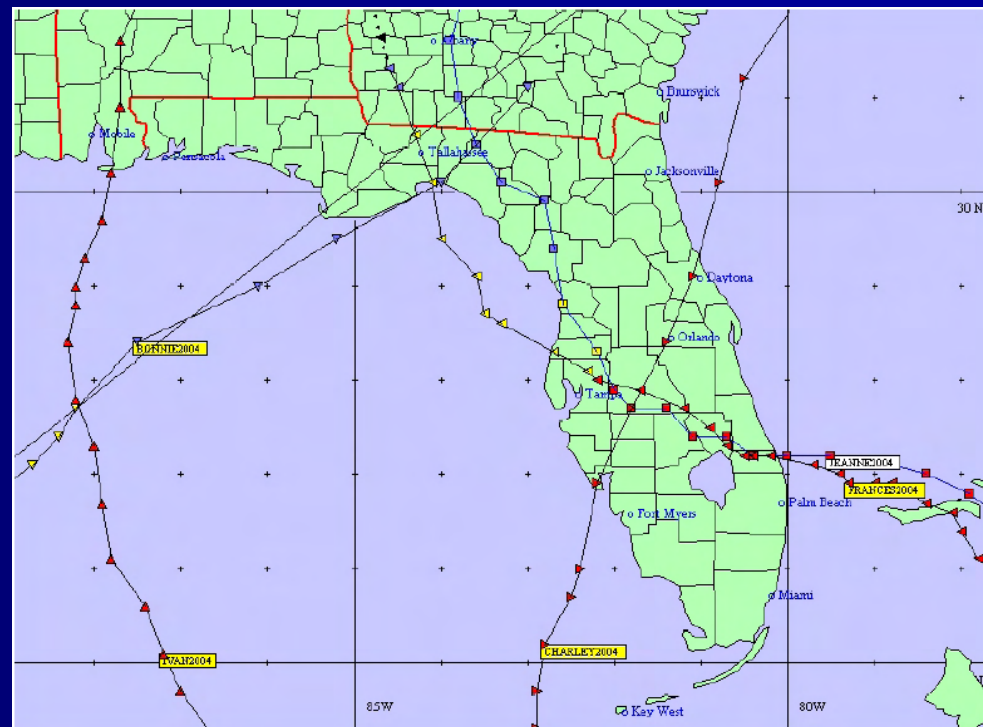


## August 2003 Power Outage

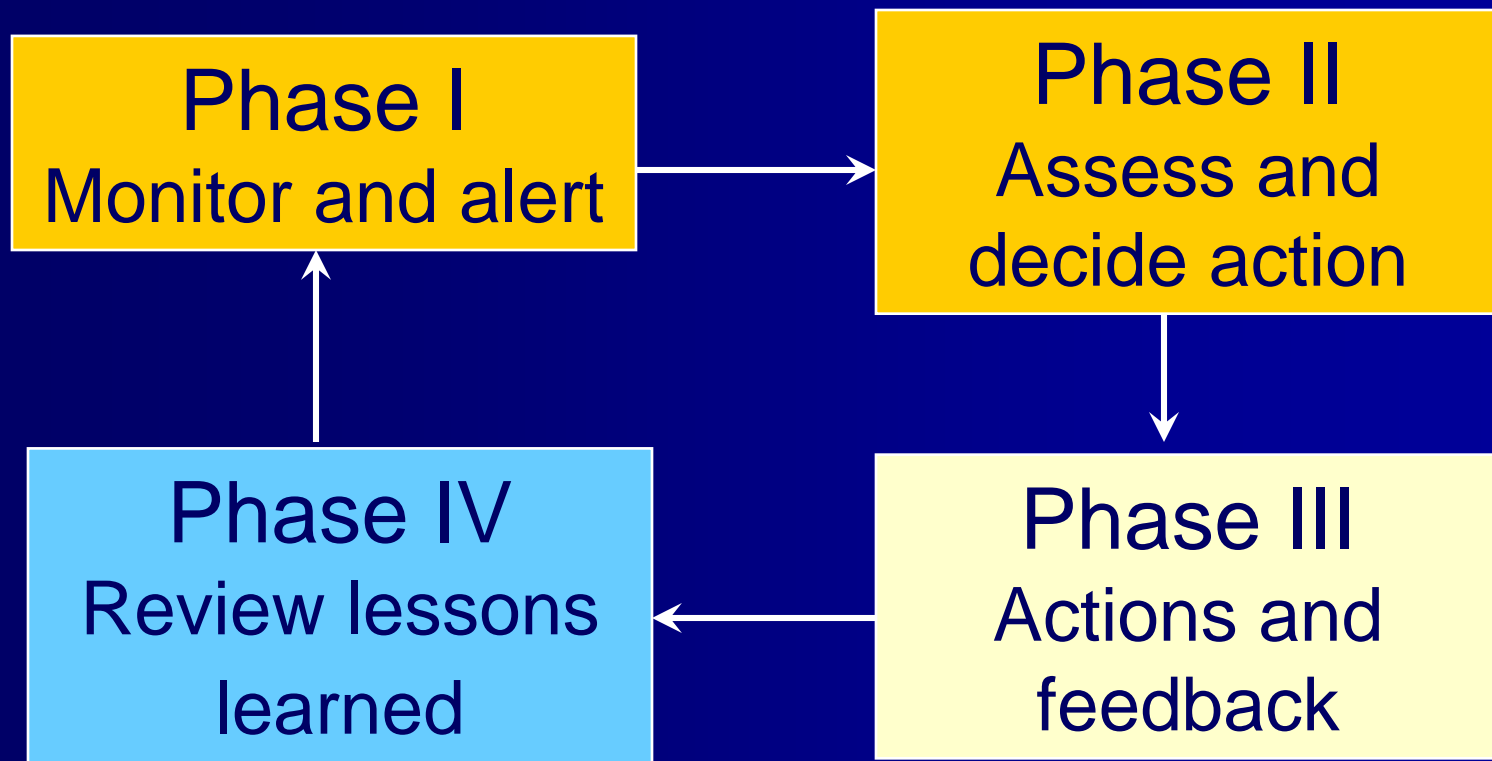
- National Economic Impact: \$7-10 billion
- 56 Automotive Plants Idled
- 11 million gasoline gallons lost from refinery
- 50 million Americans without power
- Gasoline hoarding, pricing, and long lines.

# The Consequences-All Hazard

- Florida Hurricane Season 2004
  - 4 Major Hurricanes



# The Four Phases of an Energy Emergency



## Phase I -- Monitor and Alert

- Mechanisms are needed to monitor and make assessments:
  - What is the nature/cause of the problem?
  - How big is the problem?
  - How long might it last?
  - Who is effected, where, and how?
  - Who needs to be informed?

## Phase II -- Assessment and Action

- Inform Policymakers
- Identify Options
- Determine if and when actions might be appropriate and needed
  - Actions behind the scenes and at the industry level
  - Public Actions
- Use the Energy Emergency Assurance Coordinators Contact to help assess the situation

## Phase III -- Actions and Feedback

- How quickly can actions be implemented?
- What is the appropriate legal authority?
  - What are the limitations?
- “Voluntary conservation should be preferred to mandatory measures whenever possible. Any mandatory response should be phased in, beginning with the least stringent measures, with rationing reserved for only the most severe shortage.” (NGA)

## Phase IV – Lessons Learned

- Update contingency plans and responses.
- Assure material regular review.
- Provide for periodic training/exercises.
- Assure internal state government coordination and communication.
- Assure external coordination/communication
  - Energy industry,
  - Governments.

# Recommended Actions

## Voluntary

- **Monitor Supply (no shortage)**
  - Attention to rumors, reports, national and regional events
  - Monitor, alert, coordinate
  - Issue public advisories as needed
- **Moderate shortage**
  - Seek input from stakeholders regarding potential mandatory actions
  - Give special attention to supporting private sector recovery efforts
  - Coordinate with advisory committees, other stakeholders
  - Conduct risk analysis, notify Governor of impending energy emergency

# Recommended Actions

## Mandatory

### ■ Severe Shortages

#### ■ State of Disaster

- Responsibility usually falls to state & local EMA, sometimes PUC

#### ■ Declaration of Energy Emergency

- SEO or PUC should coordinate with EMA and federal agencies as appropriate:

- DOE, FEMA, DOT

#### ■ Recommend mandatory actions

- (e.g., driver hour waivers, usage management)

# What Happens?

## Natural Gas Emergency

- **Local Distribution Companies (LDC)**
  - Initiate PUC-approved gas service curtailment plans to protect essential human services.
- **PUC**
  - Monitors supply and infrastructure status.
- **Random Outages**
  - LDCs handle random pipeline cuts due to contractor digging and similar events.
  - Reports made to PUC.

# What Happens?

## Electric Emergency

- PUC
  - Monitors for outages and emergencies.
  - Examples:
    - Storm, transmission and distribution, generation capability, interconnections, equipment failure.
- Utilities
  - Institute “Emergency Electrical Procedures”
  - Know what should be exempt from rotating blackouts.
  - Coordinate with area Security Coordinator Regional Transmission or Independent System Operator.
  - Restoration, reports.

# What Happens?

## Petroleum Emergency

- **SEO/PUC**
  - Monitors area prices and other factors for signs for shortage.
  - Receives informal reports from associations regarding product allocations.
  - Evaluates and makes recommendations to governor.
  - Coordinates with industry.
  - Convenes advisory committee and stakeholders as needed
    - Develop recommended mandatory actions.
    - Implement, administer, and monitor.
- **Industry**
  - Attempts supply enhancement.
  - Repairs and restoration as needed.
  - Initiates alternative delivery options

# What Happened?

## Petroleum Disruption Scenario

- Supply Management
  - Increase supply
    - EPA waivers
    - Increase petroleum imports
    - Driver hour waivers
    - Jones Act waivers
    - Use of SPR
  - Manage limited supply
    - Only if supplies are allocated
      - Local approval for delivery options
      - Priority end users
      - State set asides

# What Happened?

## Petroleum Disruption Scenario

- **Demand Restraint**
  - **Voluntary first, followed by mandatory actions, as needed**
  - **Public information programs to reduce use**
    - Ridesharing
    - Carpool parking lots
    - Vehicle maintenance (e.g., oil change, tire pressure, etc.)
    - Telecommuting
  - **Mandatory programs**
    - Alternate date purchases
    - Extended date purchases
    - Lower speed limits
    - Fuel switching

# **Energy Assurance Protecting Critical Infrastructure & Interdependencies**

**Integrating Critical Energy  
Infrastructure Protection and  
Emergency Response Plans into an  
Energy Assurance Plan**

# Key Definitions

## Critical Infrastructure

*Physical assets related to:*

1. The generation, transmission of electricity
2. The exploration, production, processing, storage, and delivery of natural gas.
3. The exploration, production, refining, storage and delivery of petroleum products.

## Energy Assurance

1. Reducing the vulnerability of critical infrastructure from all types of risk
2. Hastening post-shortage recovery through:
  - Multiple energy sources.
  - Redundant delivery and consumption systems.

# Integrating Response and Infrastructure

*Can you protect  
Infrastructure  
without a response  
plan?*

If you do, then you may  
have:

1. Downstream conflicts.
2. No way to relate the level of threat to the level of risk.
3. No way to mitigate the impact of shortage.

*Can you develop a  
response plan  
without attention to  
infrastructure?*

If you do, then you may:

1. Overlook essential shortage impacts.
2. Incorrectly assess vulnerability.
3. Recommend inadequate response measures.

# I. Identification of Critical Assets

- 1) State governments do not own or control much, if any, physical energy assets.
- 2) How much does government need to know about physical/cyber assets?
- 3) Who in State Government has this Responsibility?
- 4) For emergency planning:

Knowing about major assets abets preparedness and the state's ability to respond.

## II. Threat Environment

*Threat has many meanings in emergency preparedness.*

- Deliberate attacks caused by people (e.g. terrorists, criminals, hackers, delinquents, employees)
- Natural attacks caused by nature (e.g. tornados, floors wildfires)
- Accidental attacks caused by technological failure (e.g. pipeline failure, chemical spills, nuclear, or biological)

## III. Policies and Procedures

### 1. Traditional components of energy planning:

- Refining policies.
- Understanding procedures.
- Providing training.
- Making post-action assessments.

### 2. All viable energy emergency plans should be updated regularly to:

- Assure that contemporary policies are included.
- Acquaint all responders with how response and mitigation systems are designed to work.

## IV. Physical Security – Lack of Physical Security Increases Risk

### What Can Government Do?

1. Work with energy providers
2. Use existing natural gas pipeline safety rules.
  - Continue to work with the industry to assure that these rules are followed.
3. Use rules pertaining to the reliable delivery of electricity.
4. Knowledge of petroleum structure enhances the ability to respond and provides effective mitigation:

## V. Operations Security

1. **State program developers are should not need extensive knowledge of energy company operations security.**
  
2. **What should they know?**
  - Security is in place
  - Energy companies train personnel in its implementation.
  - How to ask questions and insist on site specific security measures.
  - Public Utility Commissions may include operational security requirements in a Certificate of Convenience and Necessity, or other rules, for those energy entities regulated by the state.
  - **Industry can assist state emergency responders by increasing their knowledge about operations security process and practice.**

## VI. Cyber System Network Architecture

- 1. Understand the nature of electronic information and management platforms.**
  - Use proprietary systems if possible as mass market systems increase risk.
  
- 2. States may wish to have their own information technology specialists work with the energy industry and the federal government to improve such systems, thus increasing energy assurance.**
  - Have knowledge of current information networks and their operating characteristics (architecture).
  - PUC may wish to consider rules for improved information system architecture and adequate penetration testing.

## VII. Consequence Analysis

1. Consequence analysis: Means understanding downstream effects of an energy disruption.
  - How many people could be killed and injured?
  - How large would the economic impact be?
2. Wide-spread energy outages, such as the power failure in the Midwest and Northeast during the summer of 2003: Show need to consider consequences.
3. Plans should contain sufficient information about energy infrastructure and operations
4. To project possible shortage impacts.

# Vulnerability Assessment

- Identify and characterize vulnerabilities related to specific assets or events
- Look for exploitable situations and consider actions that could be taken by insiders
- Level of vulnerability depends on existing countermeasures
- The perspective has shifted to include low probability high consequence events

# Risk Assessment

- Asset, threat, and vulnerability assessments are combined and evaluated to give a complete picture of the risks as well as the risks to each asset
- Risk = consequence x threat x vulnerability  
                    (step 1)           (step 2)           (step 3)
  - C = damage level -loss of life, physical, economic
  - T = likelihood of attack
  - V = probability of a successful attack
- Approximates the probability of an unwanted event

# Protective Measures

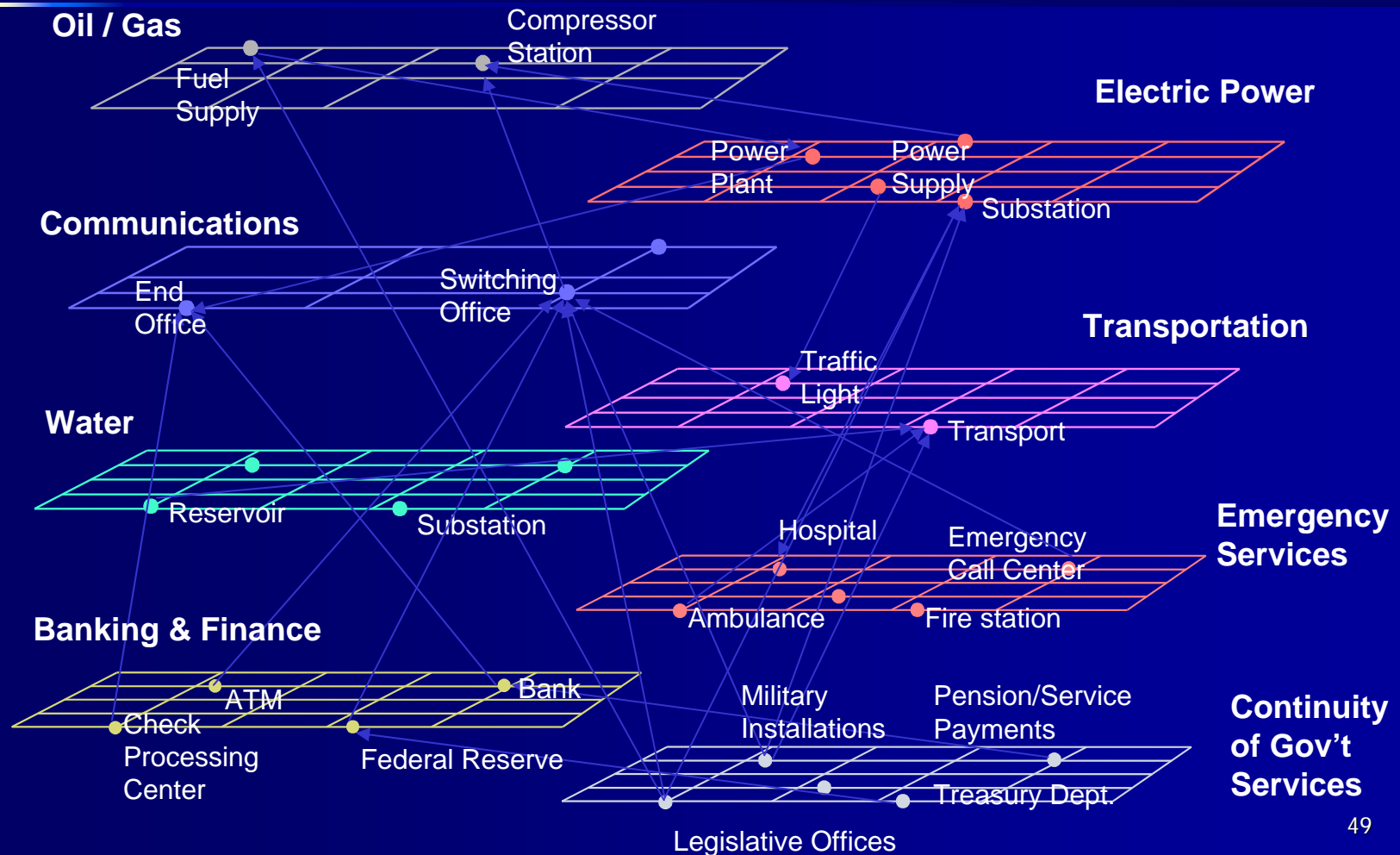
- Constant monitoring of changes in assets, threats and vulnerabilities allows:
  - Organizations to more effectively manage new risks in a timely manner, and for a longer period of time.
- Organizations develop a risk-aware culture
- Identify actions that might be taken at different threat levels: e.g., yellow, orange , red.
- What are the recommended industry standards?

# Protection of Sensitive Information

IF you are going to handle sensitive Information

- How will it be used, to determine what?
  - Do you really need it?
  - Who will, and will not, have access?
  - Can you legally protect from disclosure?
  - What happens if a person that has access to the information discloses it, are their consequences?
  - How will you physically protect the information?
  - Will the private sector providers of the information trust you?
- Is the information exempt from disclosure under your Freedom of Information Act or Sun Shine Laws, if not how can it be legally be protected from disclosure?

# Interdependent Infrastructures



# Interstate and National Coordination

- **DOE Office of Electricity Delivery and Energy Reliability**
  - Lead federal agency for energy response
  - Principal Coordinator for State and DHS on energy issues
  - Coordinates with Industry, NARUC, NASEO, NCSL, NGA
- **Functions**
  - Energy emergencies support & management duties
  - Encourages partnerships
  - Works with states directly
  - Assesses critical assets
  - Provides technical expertise
  - Provides leadership for policy and analysis

# Identification of Sector Initiatives

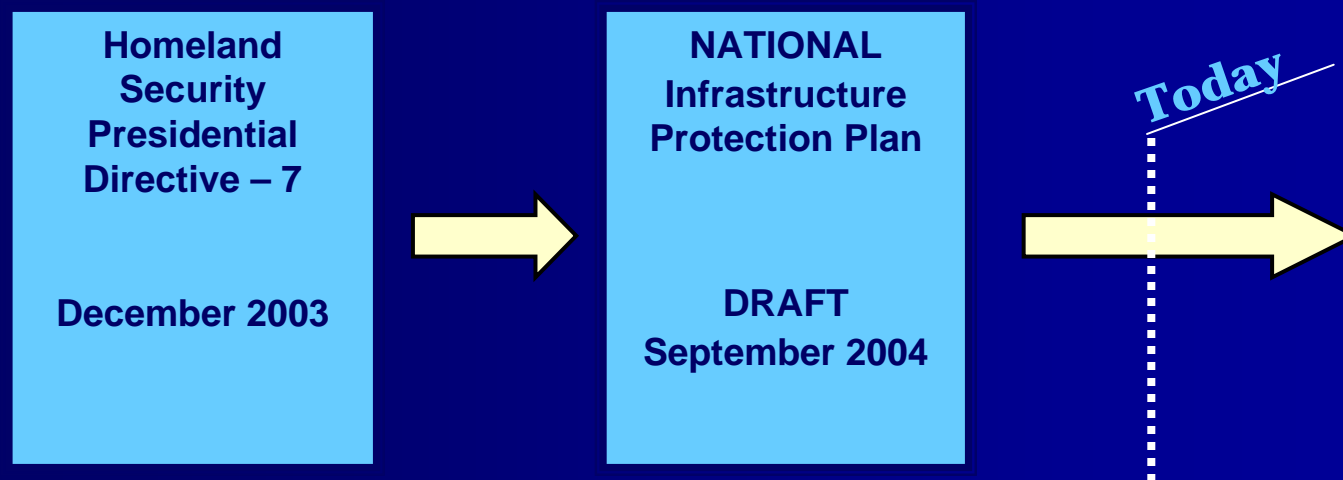
- EPA's funding Water Risk & Vulnerability Assessment
- The DOT's Office of Pipeline Safety Adoption of Industry Standards and self certification subject to audit
- NRC's enhanced security measures for Nuclear Power plants
- InfaGuard Cyber Security
- DHS Protective Measures
- Coast Guard Post Security Initiative
- Utility Cost Recovery of Security Investment
- NERC's Mandatory Cyber Security Standards
- Work by Public and Private Sector Associations
- Private Sector Security Guidelines and Actions
  - Subcommittees include private sector participation
  - Companies not directly involved one on one meeting held

# Critical Energy Infrastructure Protection

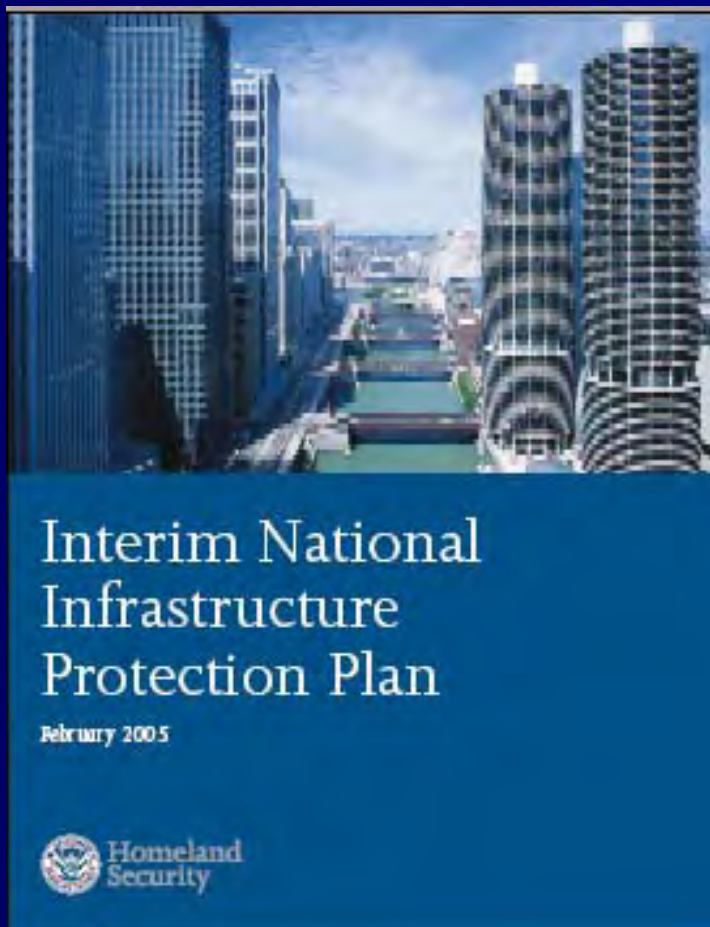
## *Where is the federal government going?*

**National Infrastructure Protection Plan (NIPP)** is a *mechanism* for establishing a dynamic, integrated, National CIP Program that reduces vulnerability of CI/KR to terrorist attacks and other hazards through:

- Identification of CI/KR threats and assets
- Assessment and prioritization of vulnerabilities
- Development, implementation of protection programs



# Interim National Infrastructure Protection Plan -- February 2005



- **Goal 1:** Protect CI/KR against plausible and specific threats
- **Goal 2:** Long-term reduction of CI/KR vulnerabilities in a comprehensive and integrated manner
- **Goal 3:** Maximize efficient use of resources for infrastructure protection
- **Goal 4:** Build partnerships among Federal, State, local, tribal, international, and private sector stakeholders to implement CIP programs
- **Goal 5:** Continuously track and improve national protection

# Working Towards a National CIP Program

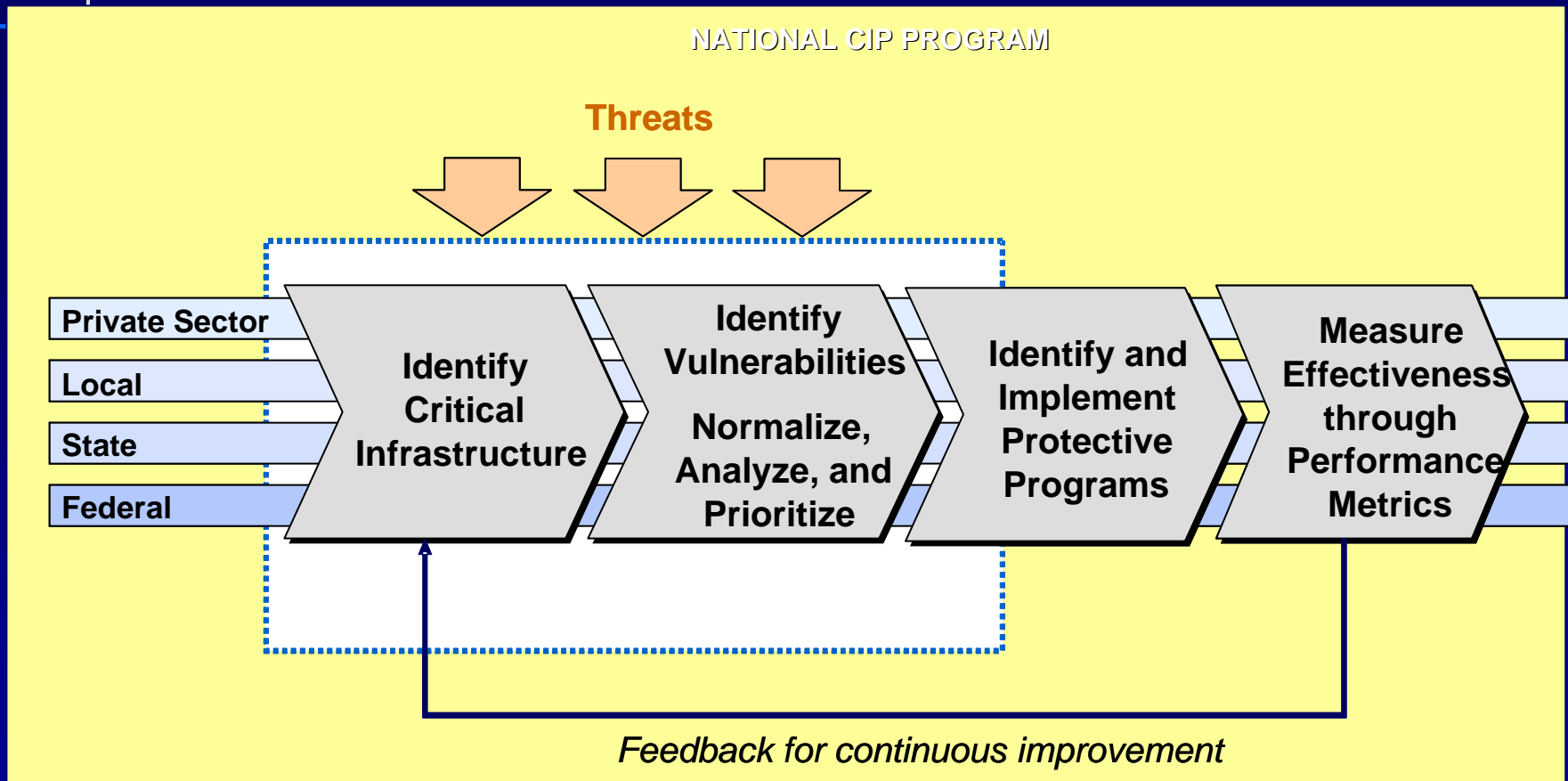
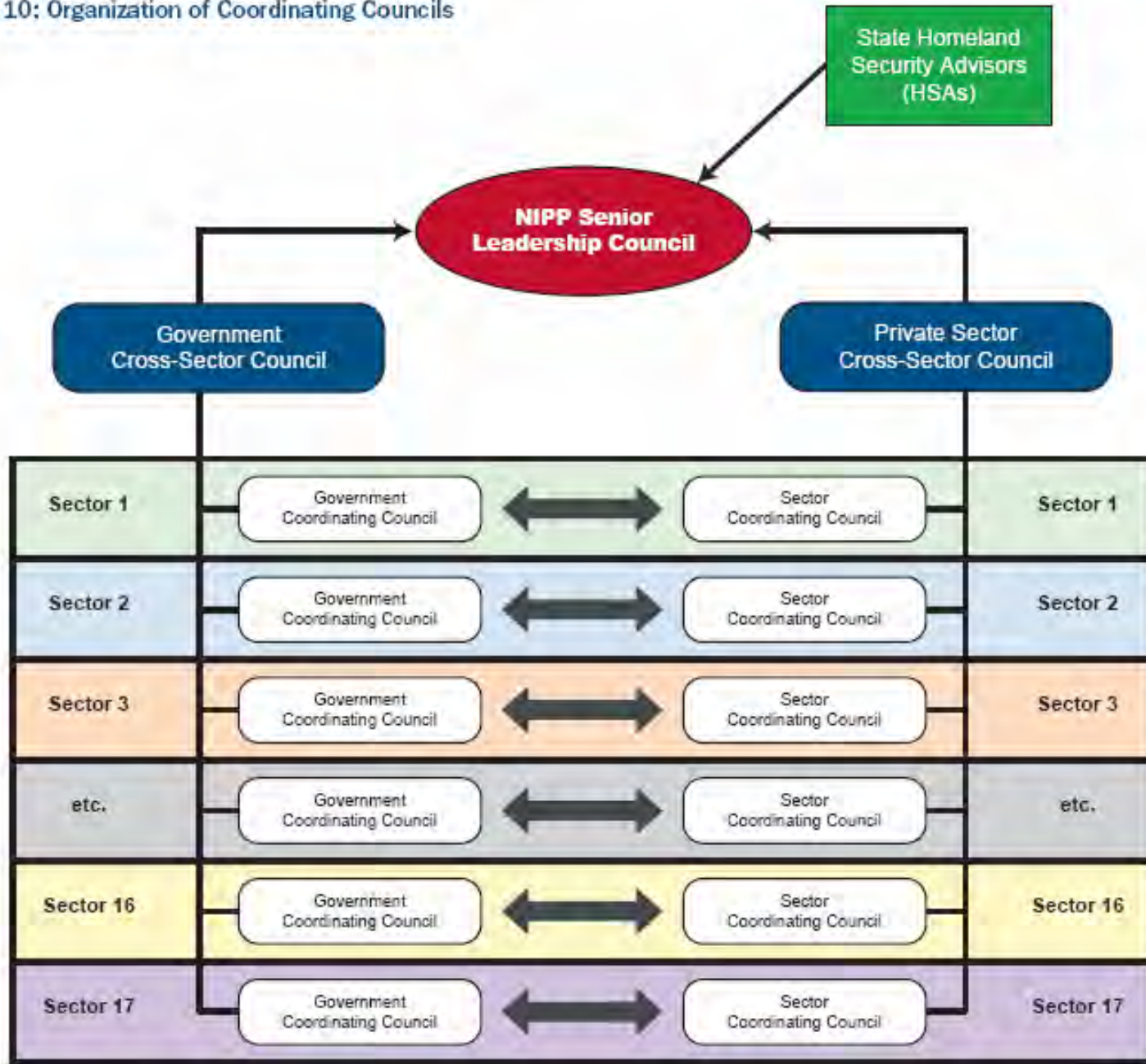


Exhibit 10: Organization of Coordinating Councils



# Questions?

Thank you for your attention  
For more information contact:

**Jeffrey Pillon**

E-mail: [jpillo@michigan.gov](mailto:jpillo@michigan.gov)

**Donald Milsten**

E-mail: [donmilsten@naseo.org](mailto:donmilsten@naseo.org)

