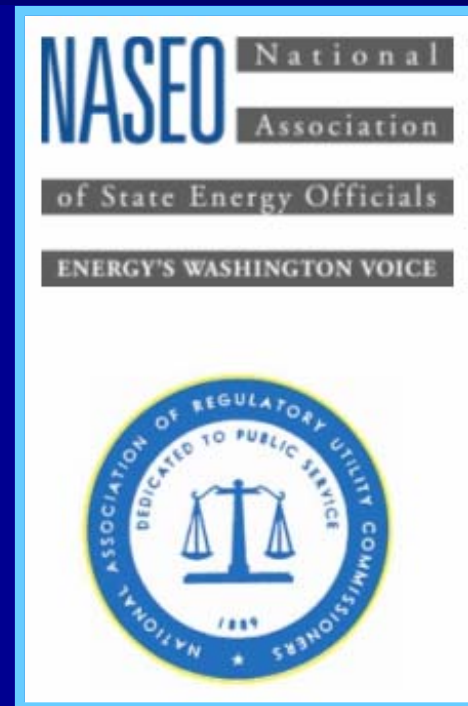


**Building Resiliency Into Energy Assurance Planning**  
**Denver, Colorado**  
*April 22-23, 2007*

# ***Energy Assurance*** **Guidelines for States**

**Jeffrey Pillon**, Chair,  
Energy Data & Security Committee  
National Association of State Energy Officials,

**David Terry**, Stateline Energy LLC



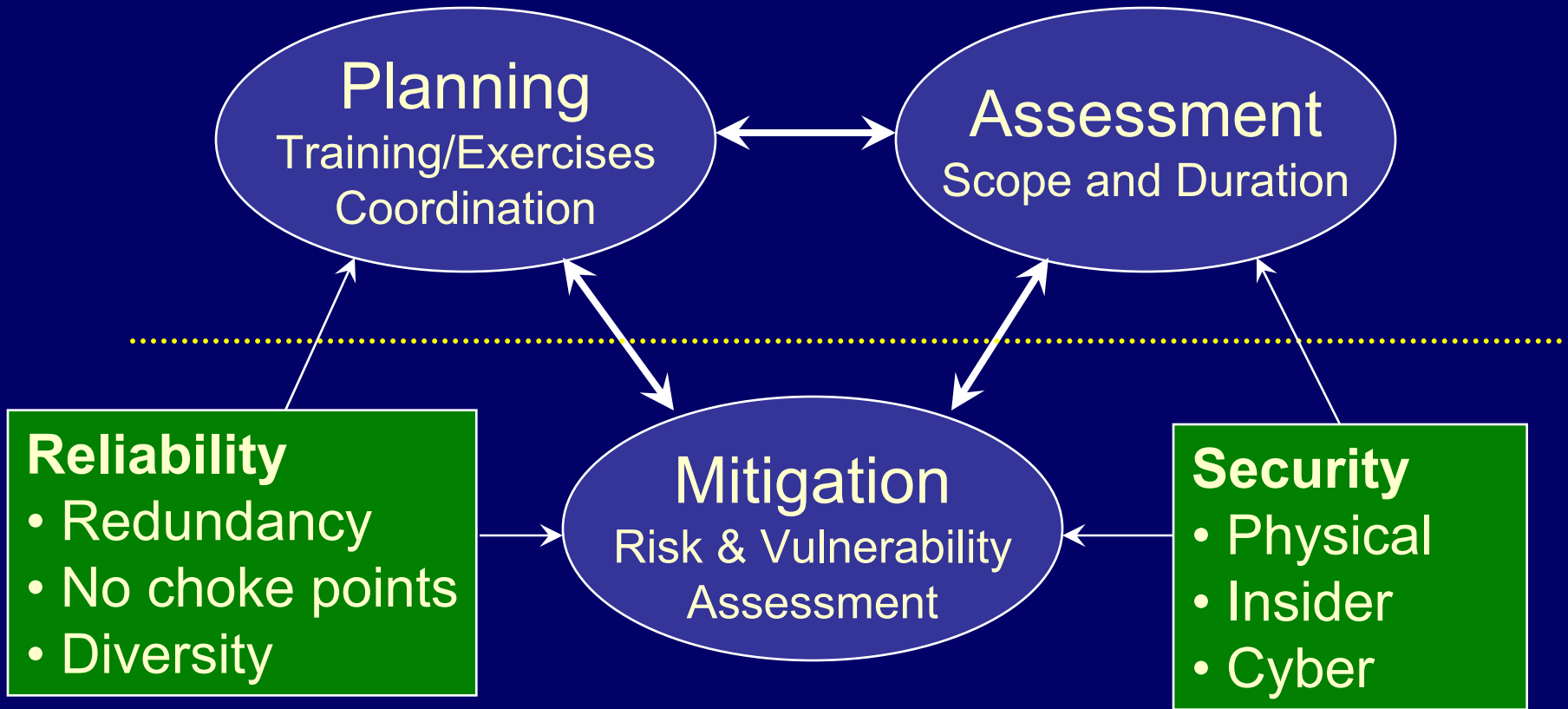
# What is Energy Assurance?

## All Hazards Approach

- Sabotage/Terrorism
- Civil Disturbance
- Flooding
- Natural Disasters
- Infrastructure Failures
- Public Health Emergencies



# Emergency Preparedness and Response



**Protecting Critical Infrastructure  
and Enhancing Resiliency**

# Prevention and Response

## I. Energy Emergency Preparedness

- Because you can't protect everything, being ready to rapidly respond can minimize the consequences

## II. Critical Infrastructure Protection

- Reducing Risk and Vulnerabilities



# Ten State Actions to Assure Energy Emergency Preparedness

1. Make sure you and your staff are prepared and trained to meet the needs of policy makers.
2. Know your state's energy profile and Interdependencies.
3. Know the geography and demography of your energy infrastructure.
4. Know your key government and industry contacts.
5. Maintain a good working relationship with the private and public sector contacts.
6. Be prepared to work with the media.
7. Know the legal authorities which support your response.
8. Understand how you can effectively respond (increasing supply, reducing demand and other actions).
9. Maintain an alternative budget for emergencies.
10. Keep your energy assurance plan up to date.

# Energy Assurance Guidelines

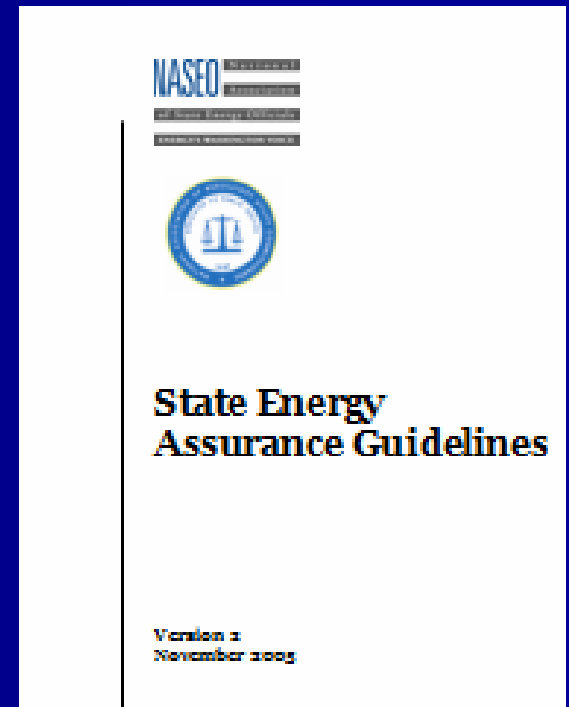
Provide states with tools for reviewing how their jurisdictions respond to energy disruptions and how to improve energy emergency plans.

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

**Find the Guidelines online at:**

**<http://www.naseo.org/EnergyAssuranceGuidelines/>**

**Version 3 now under development**



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

- The Guidelines:
  - Discuss major planning issues
  - Suggest Crisis Management Strategies
  - Help Identify Levels of Shortage
  - Encourage Pre-Crisis Preparation
  - Emphasize Data Collection, Analysis and Consequence Assessment
  - Identify Possible Response Actions

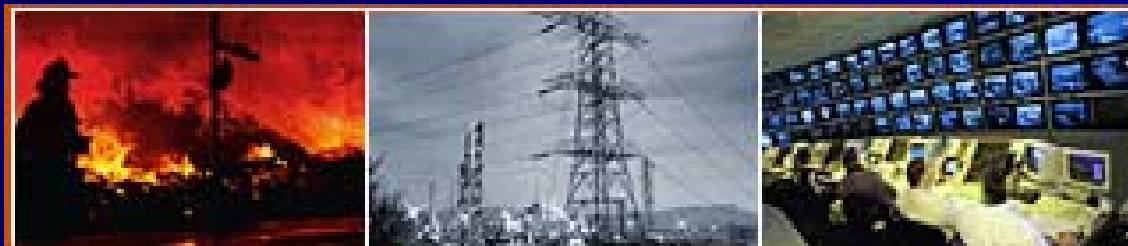


U.S. DEPARTMENT OF  
**ENERGY**

- **Office of Electricity Delivery and Energy Reliability**
  - Lead Department for energy emergency response ESF-12
  - Principal Coordinator for State and DHS on energy issues
  - Coordinates with Industry, NARUC, NASEO, NCSL, NGA, PTI
- **Functions**
  - Energy emergencies support & management duties
  - Encourages partnerships
  - Works with states directly
  - Assesses critical assets
  - Provides technical expertise
  - Provides leadership for policy and analysis

# Energy Emergency Assurance Coordinators (EEAC)

- Points of contact for States, DOE and industry in event of and energy emergency.
- Provide assessment, notification, news and updates on actions taken.
- Primary and secondary contact for each sector (petroleum, electricity, natural gas) from each state
- Midwest and Western EEAC Regional Calls
- Website: <https://www.oe.netl.doe.gov/isernet/login.aspx>





Logged in as: Jeffrey Pillon  
9:11:14 AM

[Logout](#)

Search:

[EEAC \(States\)](#)

[Orientation & Exercises](#)

[Outages & Curtailments](#)

[Energy Security Blog](#)

[Security Awareness](#)

[Bulletin Board](#)

[GIS Data](#)

[Change Password](#)

[Home](#)

## EEAC (States)

The EEAC system is a restricted-access communications network for key State-level personnel to exchange information and coordinate with each other and the Department of Energy during energy emergencies. EEAC members have access to the following communications tools to facilitate information exchange and coordination related to energy emergency issues:

### [EEAC Member List](#)

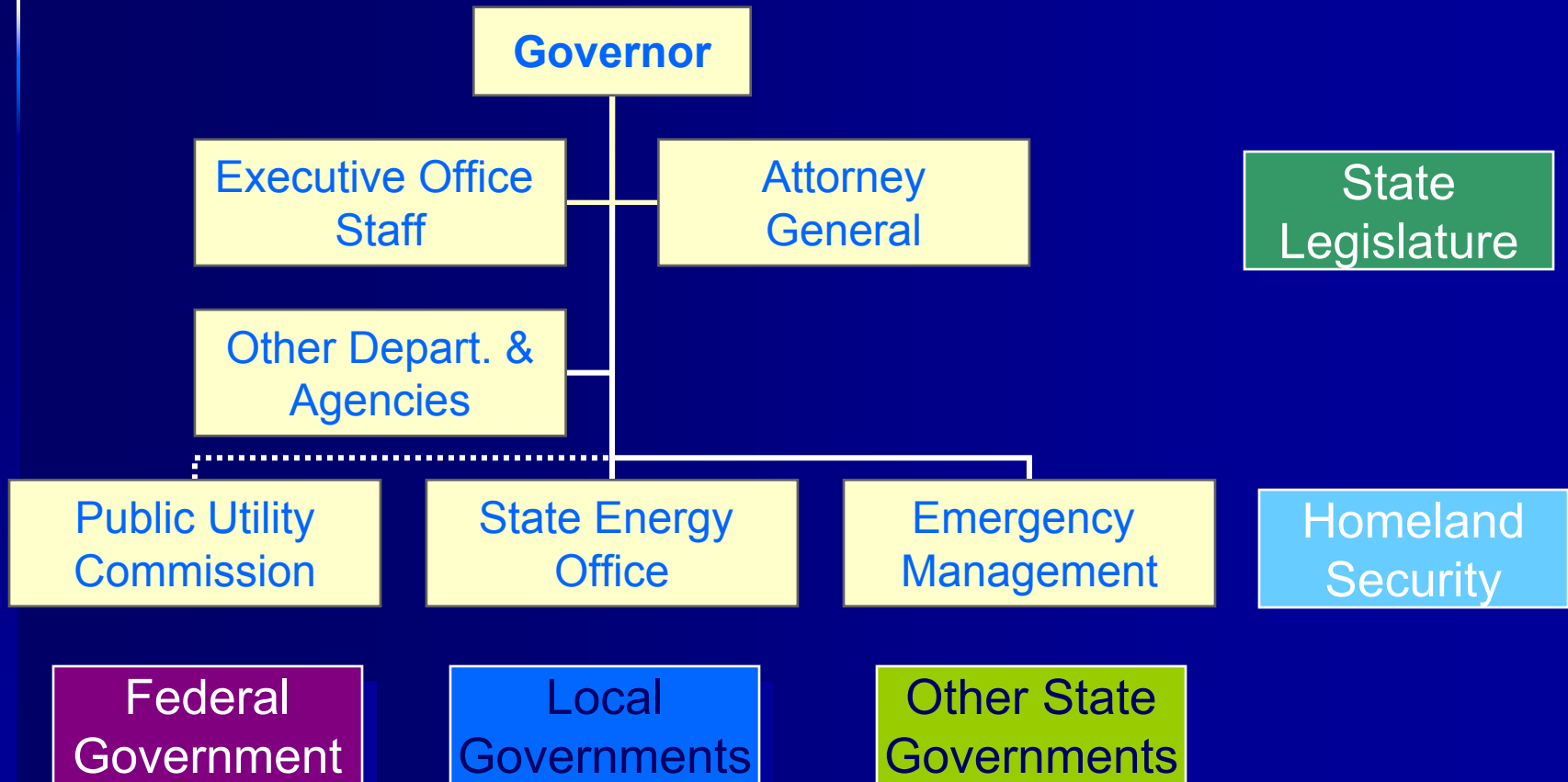
The Member List page allows EEAC users to filter the EEAC database and create customized lists of EEAC members. For example, by using the filters on the Member List page, a user can easily generate a list of all EEAC members in Florida, Georgia, and South Carolina. The user can then send an email to these EEAC members or pull up their contact information. Click here to use the Member List.

Welcome to the Energy Emergency Assurance Coordinators (EEAC) System Web Site!

Sponsored by the National Association of State Energy Officials (NASEO) and the National Association of Regulatory Utility Commissioners (NARUC) in partnership with the Office of Electricity Delivery and Energy Restoration / Infrastructure Security and Energy Reliability Division of the U.S. Department of Energy.

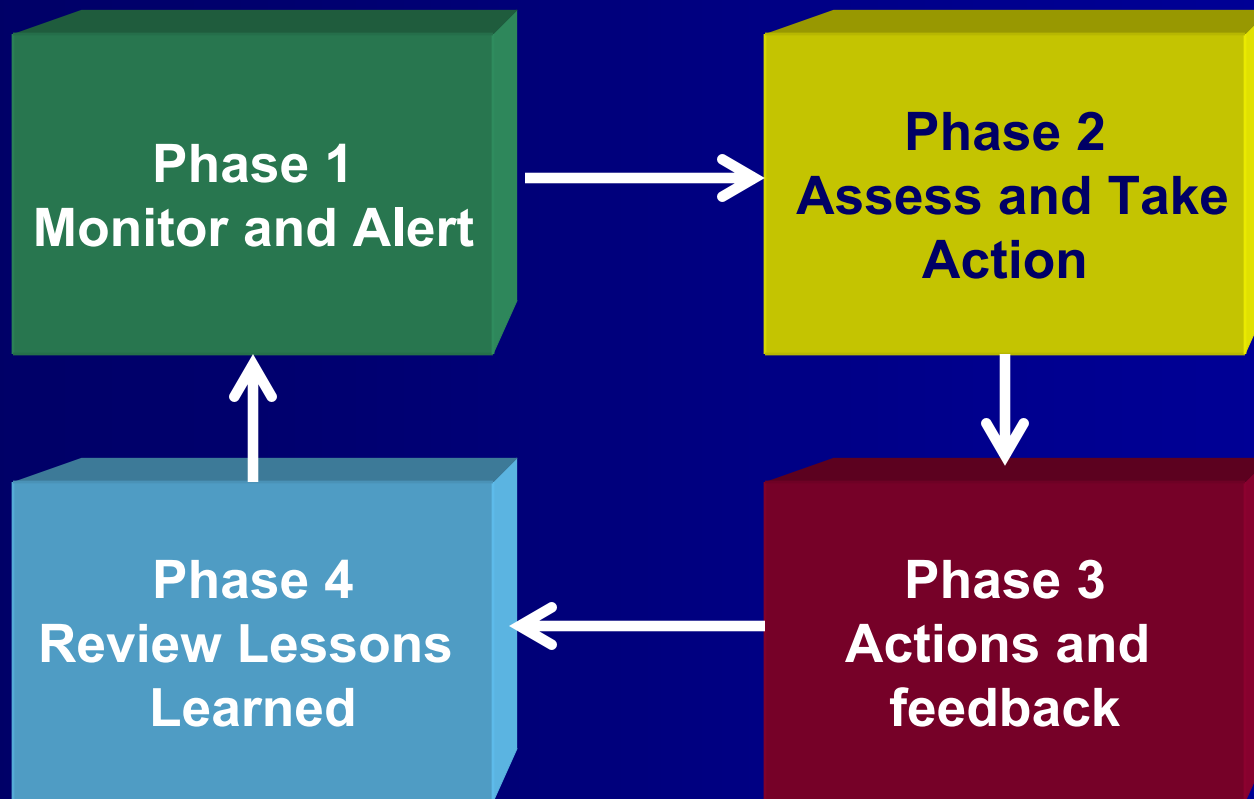
For **urgent issues** related to an energy emergency contact the DOE Emergency Operations Center at **(202) 586-8100**.

# State Energy Emergency Organizations



Note: See NARUC-NASEO Paper  
On State Organizational Issues

# The Four Phases of an Energy Emergency



# 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

- **Recommend mandatory actions**
- **State of Disaster**
  - **Responsibility usually falls to state &**
  - **local emergency management agency (EMA), sometimes PUC**
- **Declaration of Energy Emergency**
  - **SEO and/or PUC should coordinate with**
  - **State EMA and federal agencies as appropriate:**
    - **DOE, FEMA, DOT**
    - **(e.g., pipelines and driver hour waivers)**

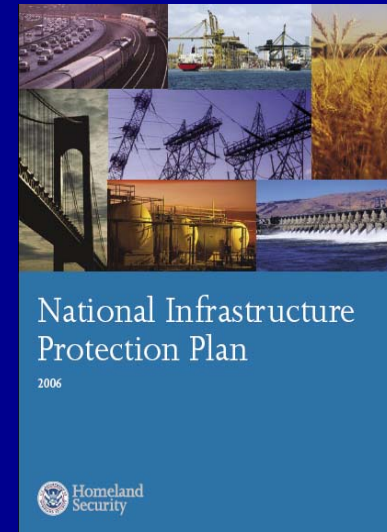
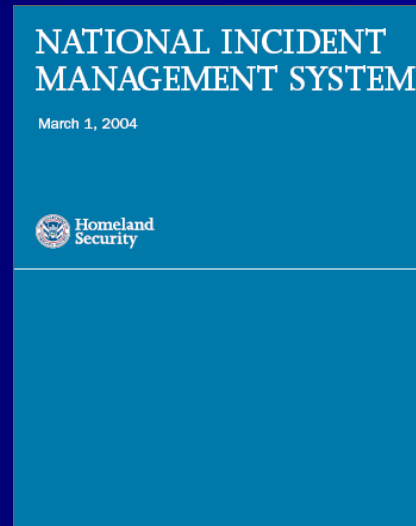
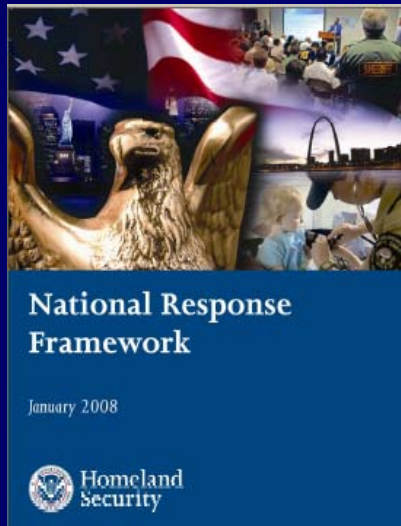
# Local, State & Federal Plans need to be Integrated and Coordinated

- National Response Framework (NRF)
  - Emergency Support Function (ESF) 12 Energy
  - Critical Infrastructure and Key Resources Support Annex
- National Incident Management System (NIMS)
- National Infrastructure Protection Plan
  - Energy Sector Specific Plan
  - Transportation Sector Specific Plan for Pipelines
- Continuity of Operation Plans (COOP) State and Local Governments

Federal Government COOP, COG, plans shall be integrated with the emergency plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, to promote interoperability and to prevent redundancies<sup>15</sup> and conflicting lines of authority. Homeland Security Presidential Directive/HSPD-20

# Overarching National Strategies

- **National Response Framework (NRF)**
  - <http://www.fema.gov/emergency/nrf/>
- **National Incident Management System (NIMS)**
  - <http://www.fema.gov/emergency/nims/>
- **National Infrastructure Protection Plan (NIPP)**
  - <http://www.dhs.gov/nipp>



# Planning for Interdependencies in Response & Protection

- Examine in-state industry interdependencies.
- Look at state level and interstate interdependencies.
- Focus on regional interdependencies.
- Coordinated Planning
- Round out with national connections.
- Energy is comprised of systems and a systems perspective is needed.



# Guidelines Appendices

- Appendix A - NASEO's Quick Guidelines: Ten Things You Should Know
- Appendix B - Additional Information Pertaining to Federal Agencies
- Appendix C – Federal Energy Emergency Actions
- Appendix D – Monitoring Fuel Supplies
- Appendix E – Essential Pre-Crisis and Background Information for State Energy Emergency Responders
- Appendix F – Petroleum Fuel Set-Aside
- Appendix G – Diversification of supply and improved efficiency (underdevelopment)
- Appendix H – Pandemic Planning (underdevelopment)
- Appendix I – Cyber Security for Energy System (underdevelopment)

# How do you build resiliency into emergency preparedness, planning, & response?

- How would you define resiliency in the context of energy emergency response actions?
- What are the types of emergency response actions that can be taken to improve resiliency in the context of planning?
- Can the speed and effectiveness of the response reduce consequences?

## **Part II. Protecting Critical Energy Infrastructure and Enhancing Long-Term Resiliency**

- Defining critical energy infrastructure and Key Assets
- Assessing risk, vulnerabilities, criticality and the nature of the threat
- Identifying Protective Measures
- Developing investments that build resiliency
  - Diversification of energy sources
  - Build redundant systems to enhance reliability
  - Increased efficiency
  - Development of Smart or Intelligent Power Grid
- Protection of sensitive information
- Build partnerships Public/Private Sectors, Federal, state, local and tribal governments.

# HSPD-7 Designated Sectors & Agencies

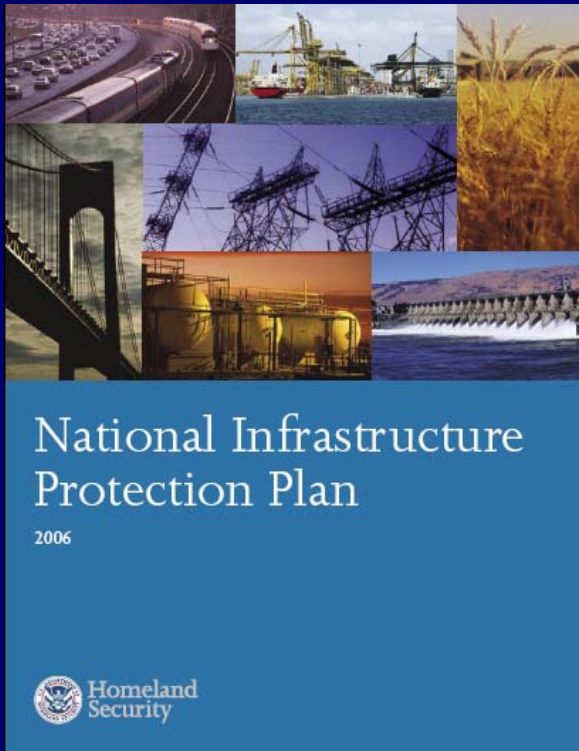
Critical Infrastructure Sectors	Agriculture, Food	USDA
	Public Health, Healthcare, Food	HHS
	Drinking Water, Water Treatment	EPA
	Defense Industrial Base	DoD
	Energy	DOE
	Banking and Finance	TREAS
	National Monuments & Icons	DOI
	Transportation Systems	DHS
	Information Technology	DHS
	Telecommunications	DHS
	Chemical	DHS
	Emergency Services	DHS
	Postal and Shipping	DHS
	Manufacturing (New)	DHS
Key Resources	Commercial Facilities	DHS
	Government Facilities	DHS
	Dams	DHS
	Commercial Nuclear Reactors,	DHS

Sector-Specific Agencies (SSAs)

DHS is responsible for coordinating the overall national effort to enhance protection of CI/KR across Sectors

# Protecting Critical Infrastructure

## NIPP Base Plan June 2006



[www.dhs.gov/nipp](http://www.dhs.gov/nipp)

- Incorporates extensive State, local, and private sector input
- Expands risk management framework:
  - Risk framework is based on threat, vulnerability, and consequences
  - Focuses on assets, systems, networks, and functions
- Strengthens information sharing and protection to include the “information sharing life-cycle”
- Forms the State and Local Homeland Security Coordinating Council
- Establishes a “steady-state” of security across critical infrastructure/key resource (CI/KR) sectors

# Risk Assessment

**Risk is a function of  
[Consequence x Threat x Vulnerability]**



## DETAILS OF JFK AIRPORT TERROR PLOT CODE-NAMED THE CHICKEN FARM

By Homeland Security NTARC News | June 3, 2007



They met at the Gertz Plaza Mall, a small shopping center in the Jamaica section of Queens, one day last July.

Russell Defreitas was a retired cargo worker allegedly trying to put together a team to mount a terrorist attack on Kennedy Airport.

Buckeye Pipeline Company  
12" Petroleum Product Pipeline  
Use of the Petroleum  
Infrastructure as a vehicle for an  
attack.

# Consequence

Consequence analysis should address both direct and indirect effects of a terrorist attack or natural disaster

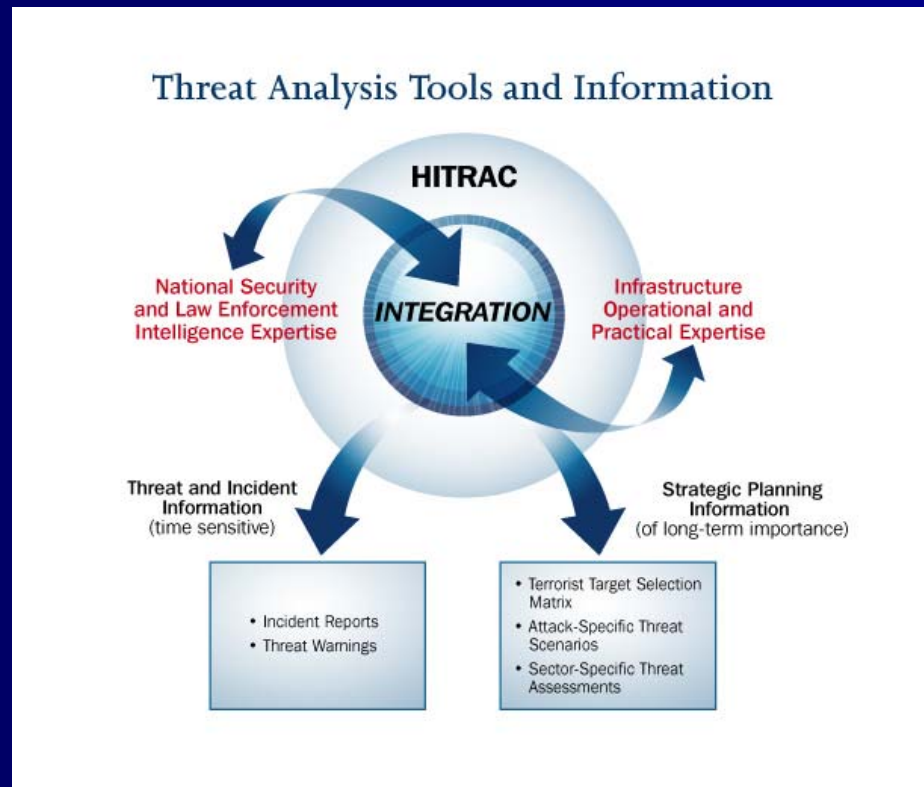
Under the NIPP, DHS works with SSAs and other security partners to examine the inherent characteristics of assets, systems, or networks to identify “worst-case” consequences

Consequences that are considered for the national-level comparative risk assessment can be divided into four main categories, which include:

- Human Impact
- Economic Impact
- Impact on Public Confidence
- Impact on Government Capability



# Threat



Threat is the likelihood that a particular asset, system, or network will suffer an attack or an incident

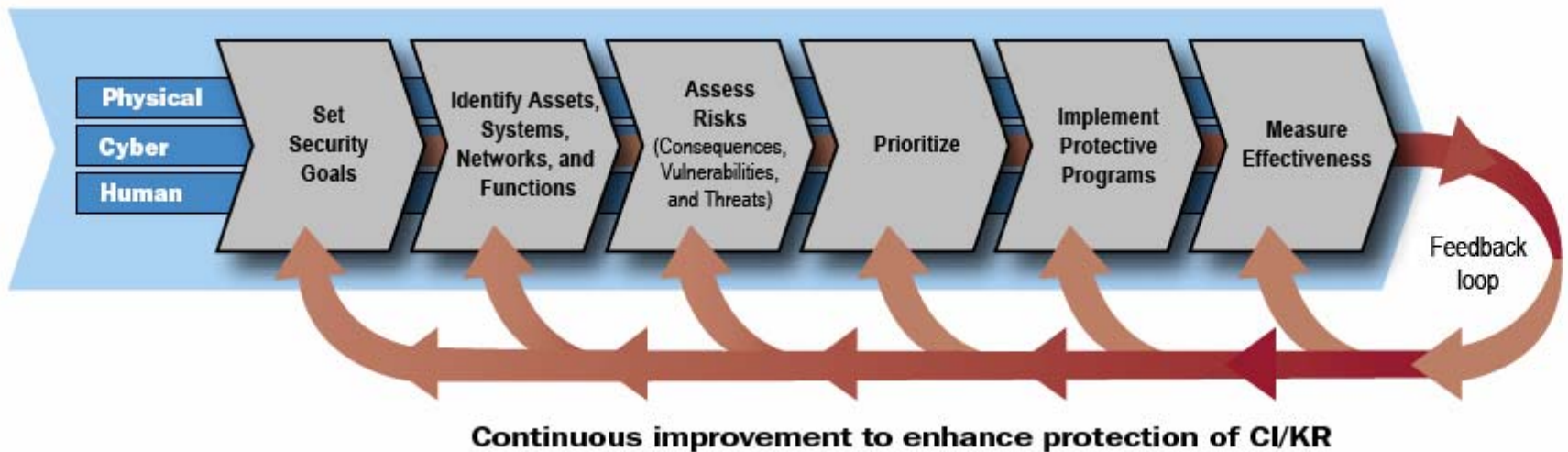
- In the context of risk from terrorist attack, the estimate of threat is based on the analysis of the intent and the capability of an adversary
- In the context of risk from a natural disaster or accident the likelihood is based on the probability of occurrence

# Vulnerability

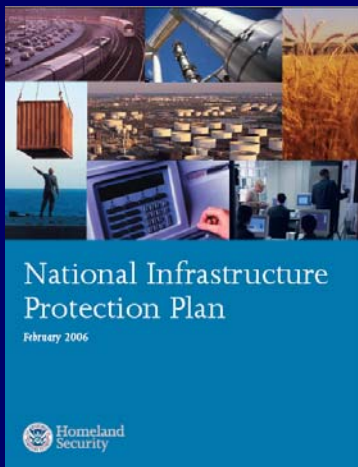
- Visible vs. not visible
- Widely know about vs. unknown
- Easy vs. difficult to protect perimeter
- Public vs. restricted access
- Security measures / standards adopted
- Inherent redundancy & resiliency
- Speed of response
- Exploitable situations available to insiders
- Cyber security

# The NIPP and Supporting Sector-Specific Plans (SSPs) describe the processes to:

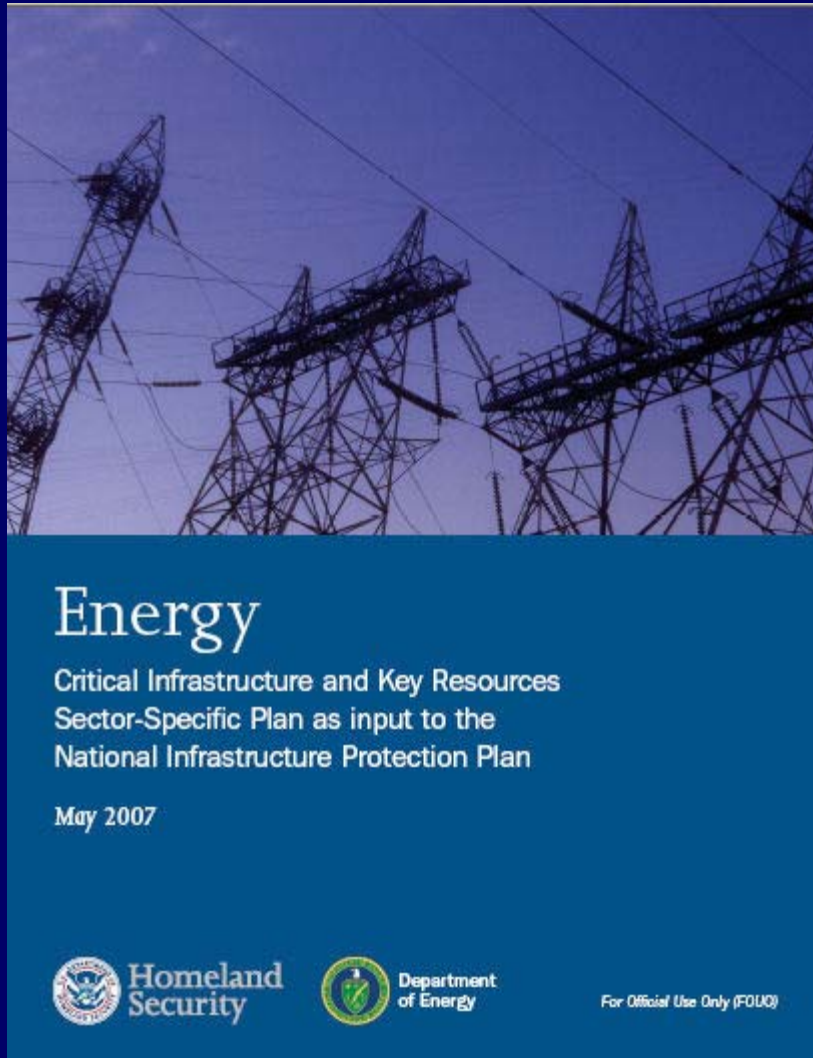
- ✓ Set Security Goals
- ✓ Identify Assets, Systems, Networks, and Functions
- ✓ Assess Risk (Consequences, Vulnerabilities, and Threats)
- ✓ Prioritize
- ✓ Implement Protective Programs
- ✓ Measure Effectiveness



# Sector-Specific Plans (SSP)



- SSP detail the application of the NIPP risk management framework in each of the 17 CI/KR sectors
- Sector-Specific Agencies partner with their sector to develop the individual SSP
- SSP are annexes to the NIPP Base Plan
- SSP complete and available on HISN (1/2 FOUO)



- Approved May 2007
- Collaborative effort between the SCC and GCC and DOE (Federal, state, local government and energy sector participants)
- Available on Homeland Security Information Network (HSIN)
- For Official Use Only, Redacted Version available at link below.
- 106 Pages

<http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf>

# Energy SSP -- Select Milestones

## Now Underway

- Continue discussions with industry on approaches and protocols for information and data collection during energy-related emergencies.
- Submit to DHS examples of risk/vulnerability assessment methodologies currently being used in the Energy Sector. Work with DHS to identify gaps and to improve approaches to meet the NIPP Base Plan criteria.
- Work to support private sector and state and local efforts to refine their risk-based protective programs and activities.
- Develop guidelines for energy emergency and security planning for State and local governments.
- Continue and expand upon previously held joint exercises and training with energy security partners and other interdependent sectors focused on potential natural and terrorist events.

# Examples of Federal Agencies & Private Sector Initiatives

- The DOT's Pipeline & Hazardous Materials Safety Administration adoption of Industry Standards and self certification subject to audit
- Buffer Zone Protection Plans
- NRC's enhanced Nuclear Power plant security
- Coast Guard Post Security Initiative
- NERC's Mandatory Cyber Security Standards
- API Security Guidelines
- Other Industry guidance

# So can you protect everything from everything?

# NO

- You need good energy emergency preparedness to rapidly respond to disruptions so as to minimize the consequences and allow for a more rapid recovery.
- By making investments now in planning, training and exercises, and by making investment in infrastructure, in the long term, the time to recovery systems can be reduced.

# How can Government and the Private Sector work together to enhance the resiliency of the energy sector?

- There are a variety of mid- to long-term opportunities to address resiliency, what are they?
- Do actions to improve resiliency generally have characteristics that require regional or multi-state planning or actions?
- In the context of energy assurance planning, what types of resiliency actions are your state involved in?

# A Framework for Defining Resilience

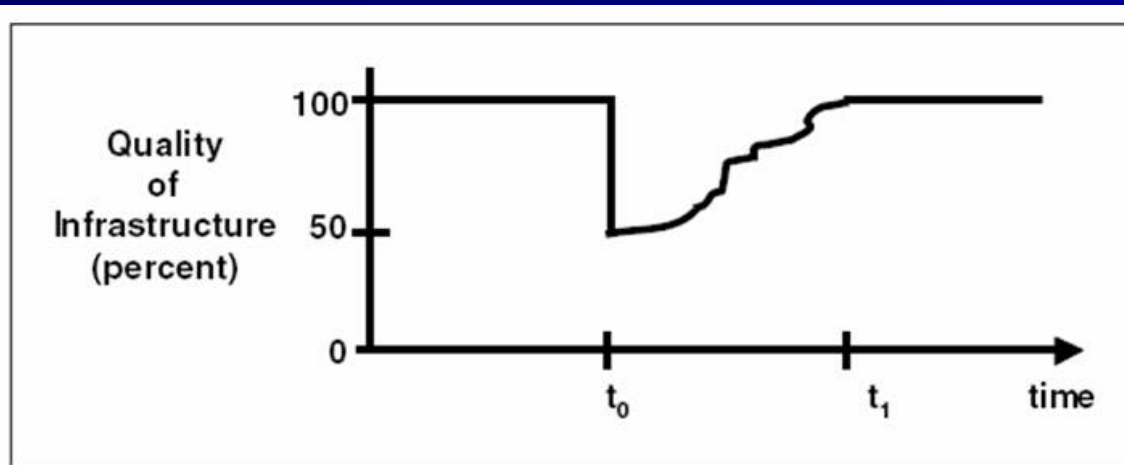


FIGURE 3 Measure of seismic resilience—conceptual definition. Source: Bruneau et al., 2003.

For a community, loss of resilience,  $R$ , can be measured as the expected loss in quality (probability of failure) over the time to recovery,  $t_1 - t_0$ . Thus, mathematically,  $R$  is defined as:

$$R = \int_{t_0}^{t_1} [100 - Q(t)] dt$$

# Resilience results from a sustained commitment to four factors

- **Robustness**
  - The ability to operate or stay standing in the face of disaster
- **Resourcefulness**
  - skillfully managing a disaster once it unfolds
- **Rapid Recovery**
  - The capacity to get things back to normal as quickly as possible after a disaster
- **Learning lessons**
  - Having the means to absorb the new lessons that can be drawn from a catastrophe

# Intersecting Stakeholder Interest

## Public/Private Sector Partnerships



In 2004 Osama bin Laden enunciated a policy of “bleeding America to the point of bankruptcy.”

Source: Homeland Security Advisory Council, Critical Infrastructure Task Force Report, January 2006



For more information contact:

Jeffrey Pillon

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

Phone: 517-241-6171

David Terry

E-mail: [dterry@statelineenergy.org](mailto:dterry@statelineenergy.org)

Phone: 703-395-1076

