



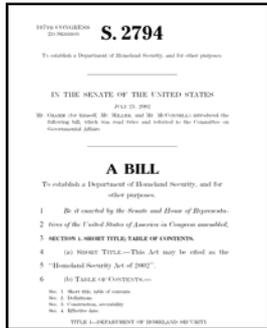
***Industry & Government Perspectives on the  
State of Global Maritime Awareness***

***The DHS Infrastructure Perspective***

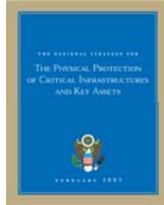
September 15, 2009

***Global Maritime Information Sharing Symposium  
National Defense University  
Ft. McNair, Washington, DC***

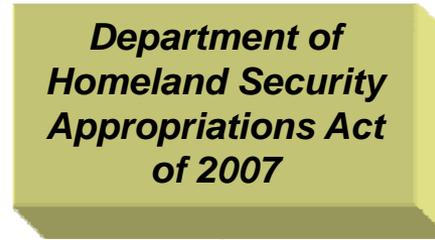
# Strategic Drivers



The Homeland Security Act of 2002 established an Assistant Secretary for Infrastructure Protection, responsible for assessing vulnerabilities of key resources and critical infrastructures and developing a comprehensive national plan. In 2006, P.L. 109-295, Section 550 directed the regulation of high risk chemical facilities.



National strategies for Homeland Security, Cyber Security, and Physical Protection of CIKR provided high-level goals and priorities for the Office of Infrastructure Protection.



The DHS Appropriations Act of 2007 charged IP with creating a chemical security regulatory program. The Appropriations Act of 2008 also requires Ammonium Nitrate regulations.



The 2005 / 08 hurricanes affirmed IP's important mission and central role in preparedness.



HSPDs provide inter-related and focused policy guidance in the areas of incident management, critical infrastructure protection, and national preparedness.

*HSPD-7: drives the NIPP*

*HSPD-19: drives the Office of Bombing Prevention's activities*

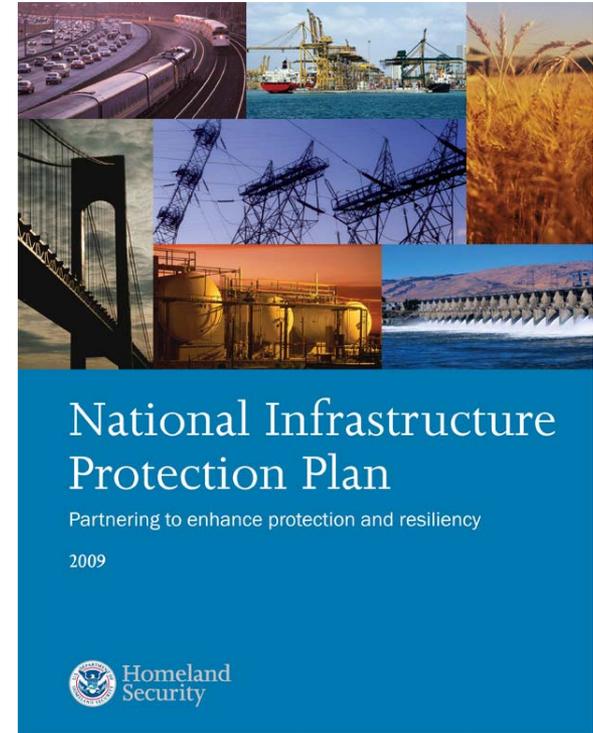


**STAKEHOLDER INTERACTION**

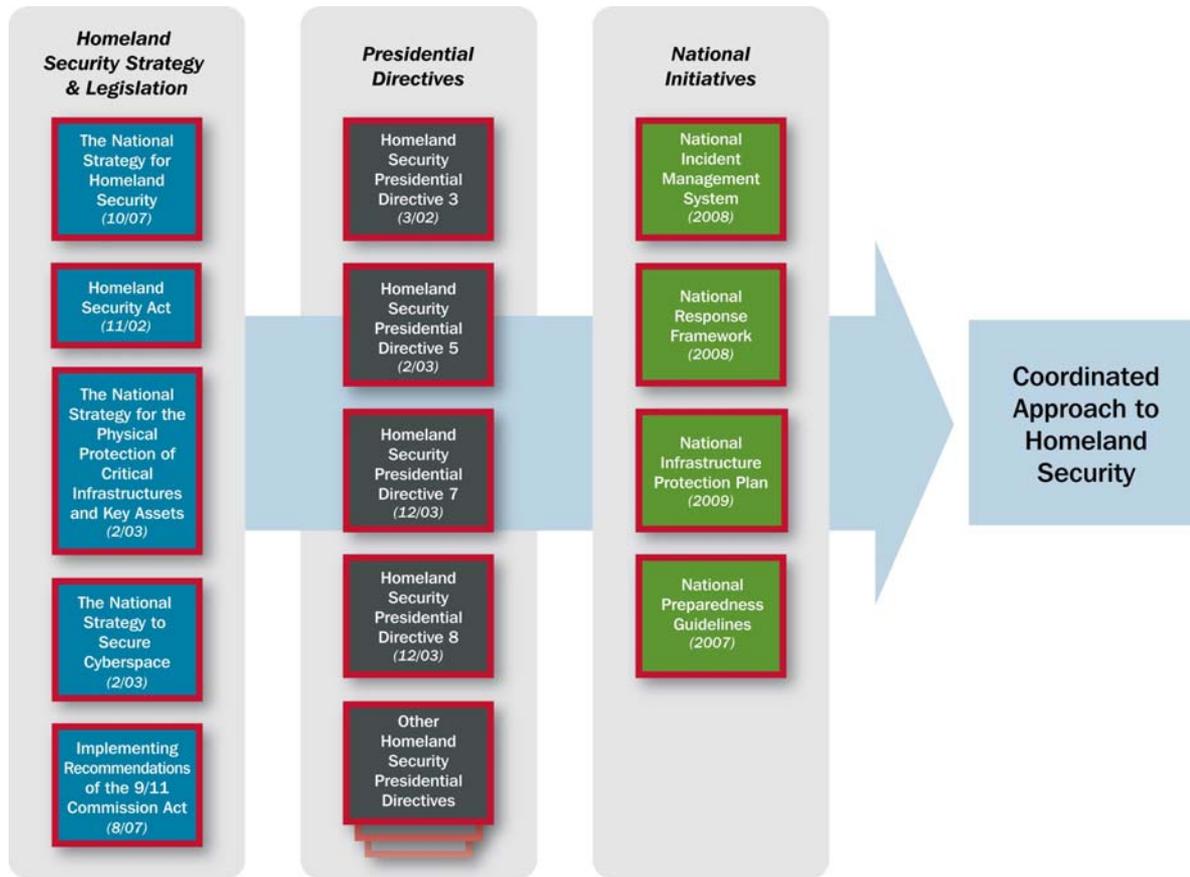


# National Infrastructure Protection Plan (NIPP)

- ▶ A comprehensive plan and unifying structure for the government and the private sector to improve protection and resiliency of critical infrastructure and key resources (CIKR), including
  - Partnership model & information sharing
  - Roles & responsibilities
  - Risk management framework
  - Authorities
  - Integration with other plans
  - Building a long-term program
  - Providing resources & prioritizing investments
- ▶ Contributes to both steady-state (non-incident) risk management and incident management
- ▶ Drives IP's programs & activities, guides those of
  - Other Federal agencies and departments
  - State, local, tribal, and territorial governments
  - CIKR owners and operators



# Homeland Security Strategic Framework



The NIPP is a key component of the Nation's all-hazards homeland security framework.

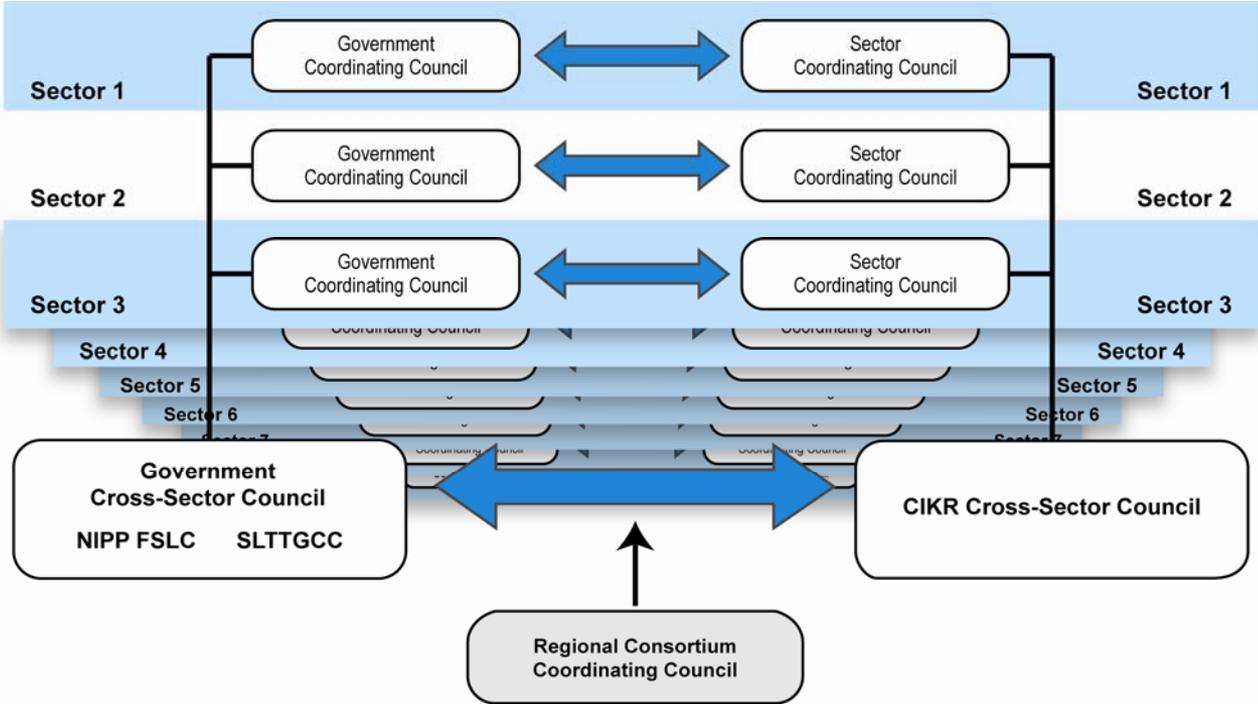
# Designated Sectors & Lead Agencies from HSPD-7

- ▶ DHS coordinates the overall national effort to enhance CIKR protection and resiliency through the implementation of the NIPP
- ▶ Sector-specific agencies lead the activities in each of 18 sectors and develop and implement Sector-Specific Plans
- ▶ DHS leads 11 of the sectors
- ▶ IP leads six of these sectors

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security <i>Office of Infrastructure Protection</i>	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
<i>Office of Cybersecurity and Communications</i>	Information Technology Communications
<i>Transportation Security Administration</i>	Postal and Shipping
<i>Transportation Security Administration United States Coast Guard</i>	Transportation Systems
<i>Immigration and Customs Enforcement, Federal Protective Service</i>	Government Facilities

# Sector Partnership Model

- ▶ Critical infrastructure protection and resiliency are the shared responsibilities of Federal, State, local, tribal, and territorial governments, regional coalitions, and the owners and operators of the Nation's CIKR
- ▶ NIPP outlines their roles & responsibilities
- ▶ Also describes the information-sharing environment and communications



Council functions include comprehensive planning, methodology development, risk assessment, protective programs & resiliency strategies, incident management, training, exercises, identification of R&D requirements

# Coordination and Information Sharing

## GOALS

- Enhance situational awareness and maximize ability of government and private sector security partners at all levels to
  - assess risks,
  - respond to emerging threats,
  - and coordinate programs and processes
- Lead, integrate, and coordinate implementation of NIPP
- Facilitate development and ongoing support of security partner governance and coordination structures

# Partnership Structures

*Overarching  
Framework*



*CIKR Owners &  
Operators*



*Government  
Counterparts*



*CIKR Initiatives Integration Using  
Existing Regional Coalitions*



# Networked Information Sharing



# CIKR ISE Implementation

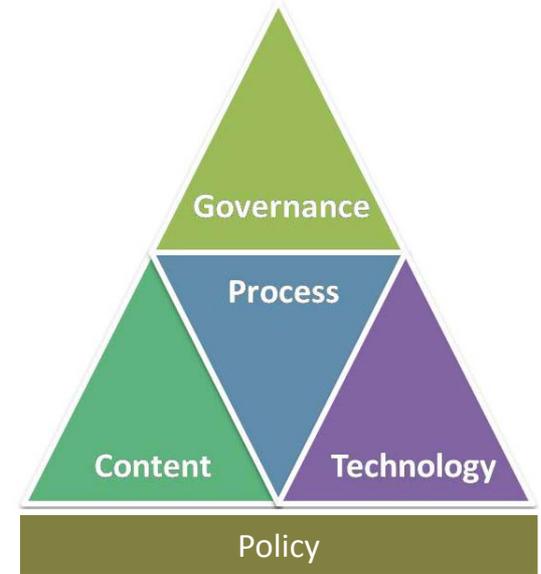
- Information Sharing for the CIKR Information Sharing Environment (ISE) involves the mission-driven processes that support homeland security:

- Situational awareness,
- Preparedness, and
- Recovery for all hazards.

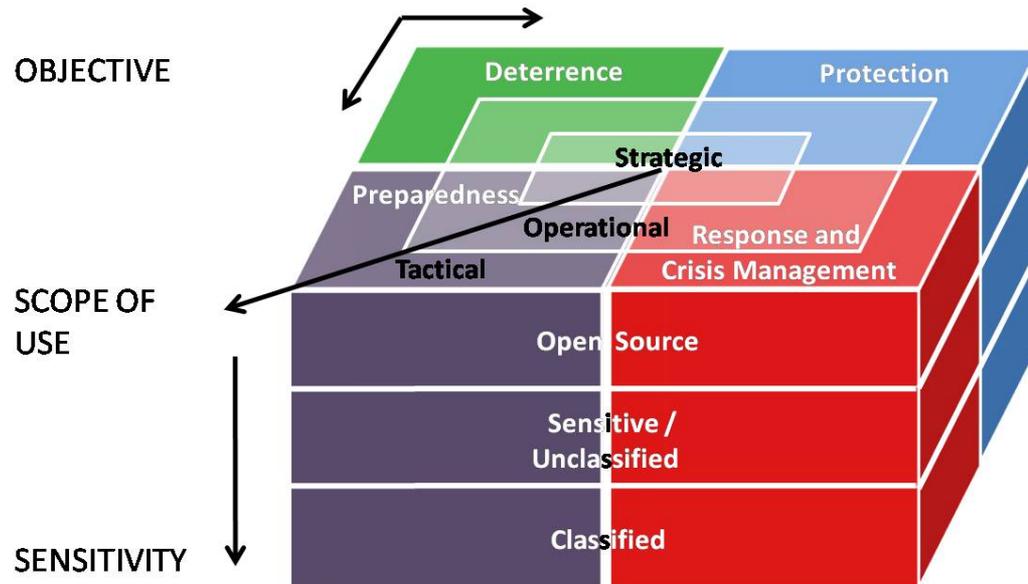
- To implement the CIKR ISE effectively, information sharing is divided into four key components:

- Policy / Governance** – the foundational construct that defines the roles, responsibilities and processes for the sector.
- Content** – formalized process that defines information that is required and generated by sector members.
- Process** – core, enhanced and external capabilities that define how a sector shares information.
- Technology** – HSIN or similar information sharing platforms that enable sector communication and coordination.

- Additionally, information sharing requirements are collected to address any gaps in the four components and to ensure effective and robust information sharing



# CIKR ISE Content Environment

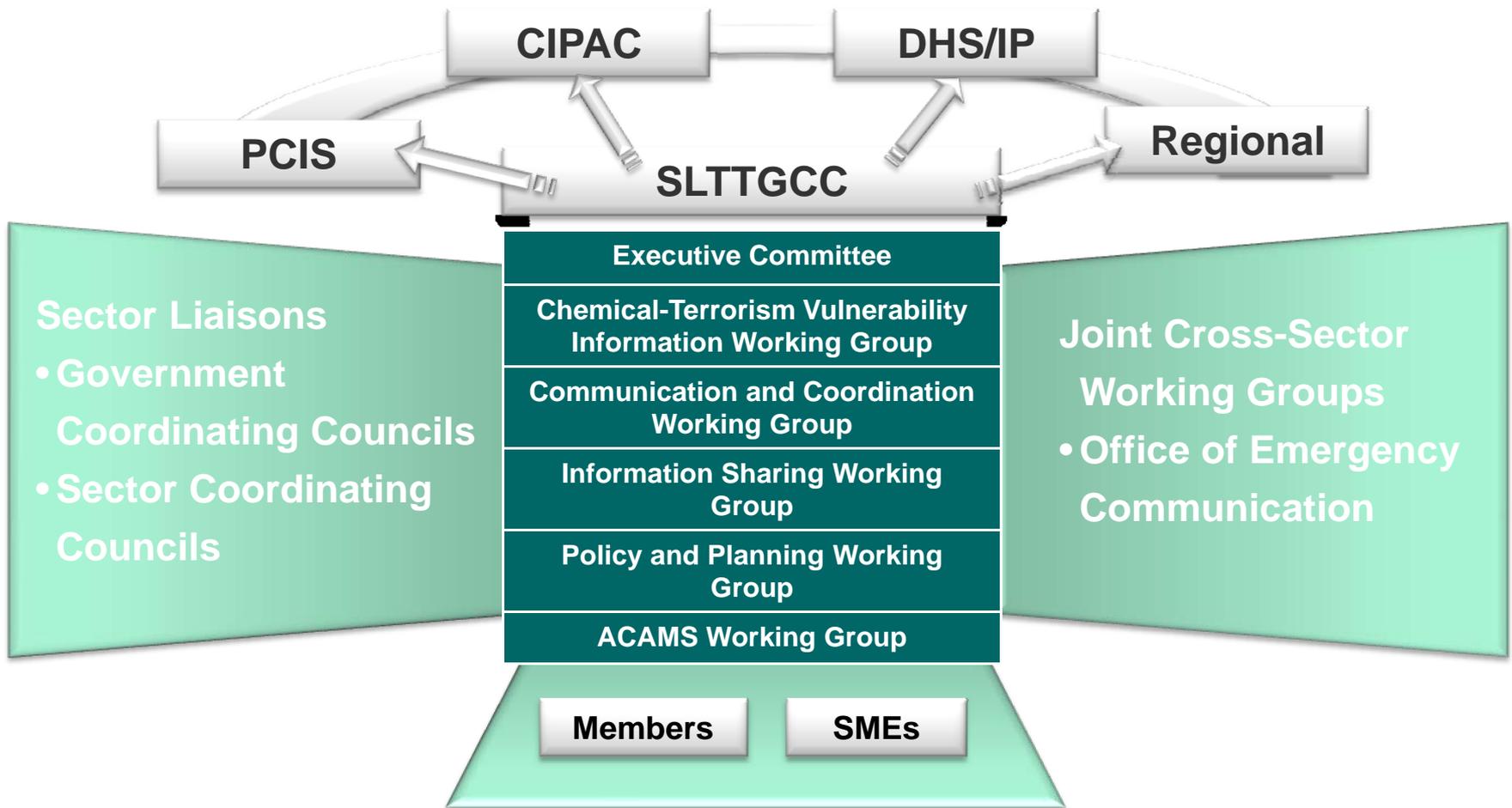


---

*The CIKR Content Environment ensures information vital to the operations of CIKR infrastructure is seamlessly provided to owners and operators in a form that is useful.*

---

# SLTTGCC Role in the Sector Partnership



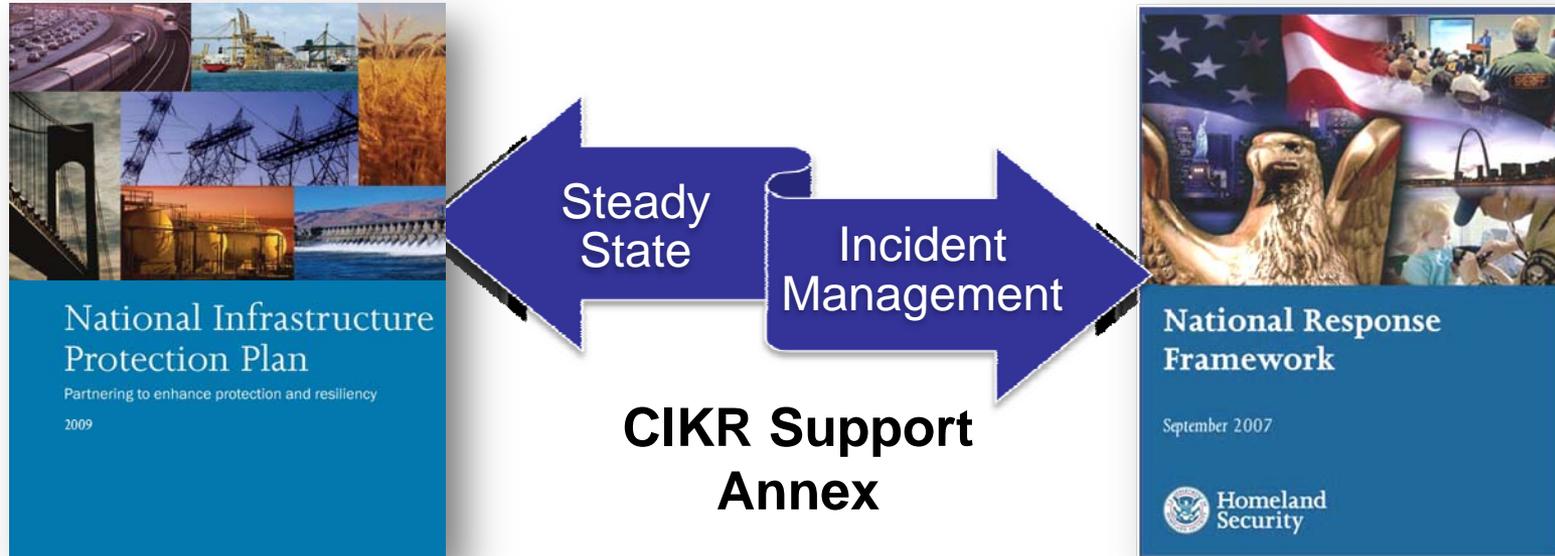
# Regional Coalitions

- The Regional Consortium Coordinating Council (RCCC):
  - Is the final component of the NIPP partnership structure
  - Formed in 2008 to serve as the focal point for coordination with DHS and CIKR sectors
  - Engages existing organizations as a powerful force multiplier to implement CIKR protection and energize grassroots activities

**“Specific regional initiatives range in scope from organizations that include multiple jurisdictions and industry partners within a single State to groups that involve jurisdictions and enterprises in more than one State and across international borders.”**

***- National Infrastructure Protection Plan***

# NRF CIKR Support Annex



- Provides the bridge between the NIPP “steady-state” approach for CIKR protection and the NRF incident management doctrine
- Addresses recommendations of the Hurricane Katrina after-action review

# NIPP – NRF : The Full Spectrum of Incident Management

**Pre-Incident**



**Incident**



**Post-Incident**



**Prevention**

**Preparedness**

**Response**

**Recovery**

**Mitigation**

# NRF Coordination Structure



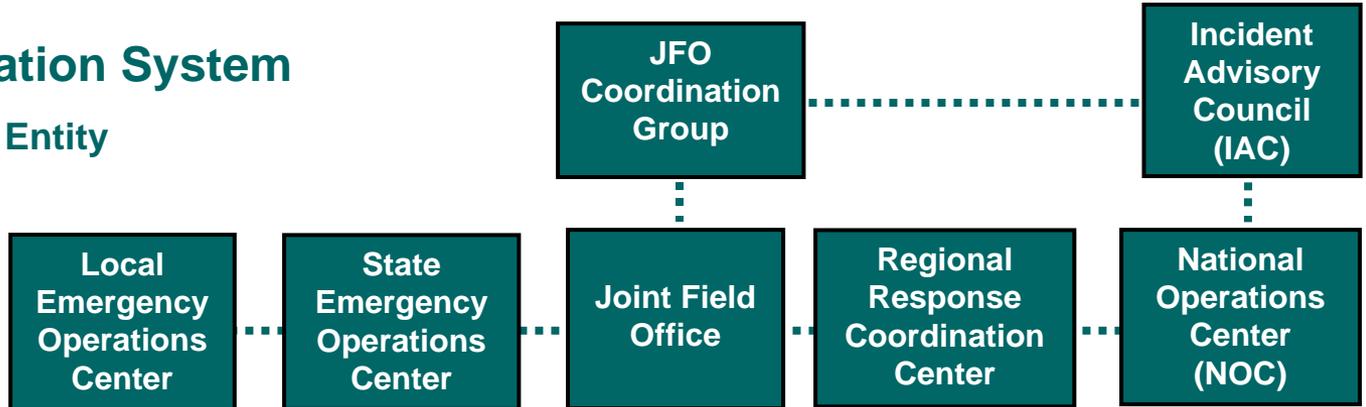
## Multiagency Coordination System

### Multiagency Coordination Entity

- Strategic coordination

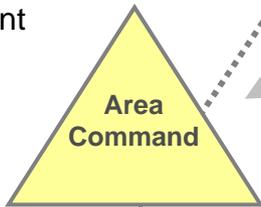
### Multiagency Coordination Centers/EOCs

- Support and coordination



## Incident Command

- Directing on-scene emergency management



An **Area Command** is established when needed due to the complexity or number of incidents.

**Role of regional components** varies depending on scope and magnitude of the incident.

**The NRF includes slight variations of the base structure for *terrorism response* and *Federal-to-Federal support***

# Major CIKR Concerns/Issues

- Access and Credentialing
- Evacuation and re-entry plans and routes
- Status of
  - Electricity
  - Water
  - Telecommunications
  - Roads
- Resource and supply confiscation



# Questions?

September 15, 2009

***Global Maritime Information Sharing Symposium  
National Defense University  
Ft. McNair, Washington, DC***