

Energy Assurance & the National Infrastructure Protection Plan

Jeffrey Pillon, Chair, NASEO
Energy Data & Security Committee

NASEO Energy Outlook Conference
Washington, D.C.
February 2006

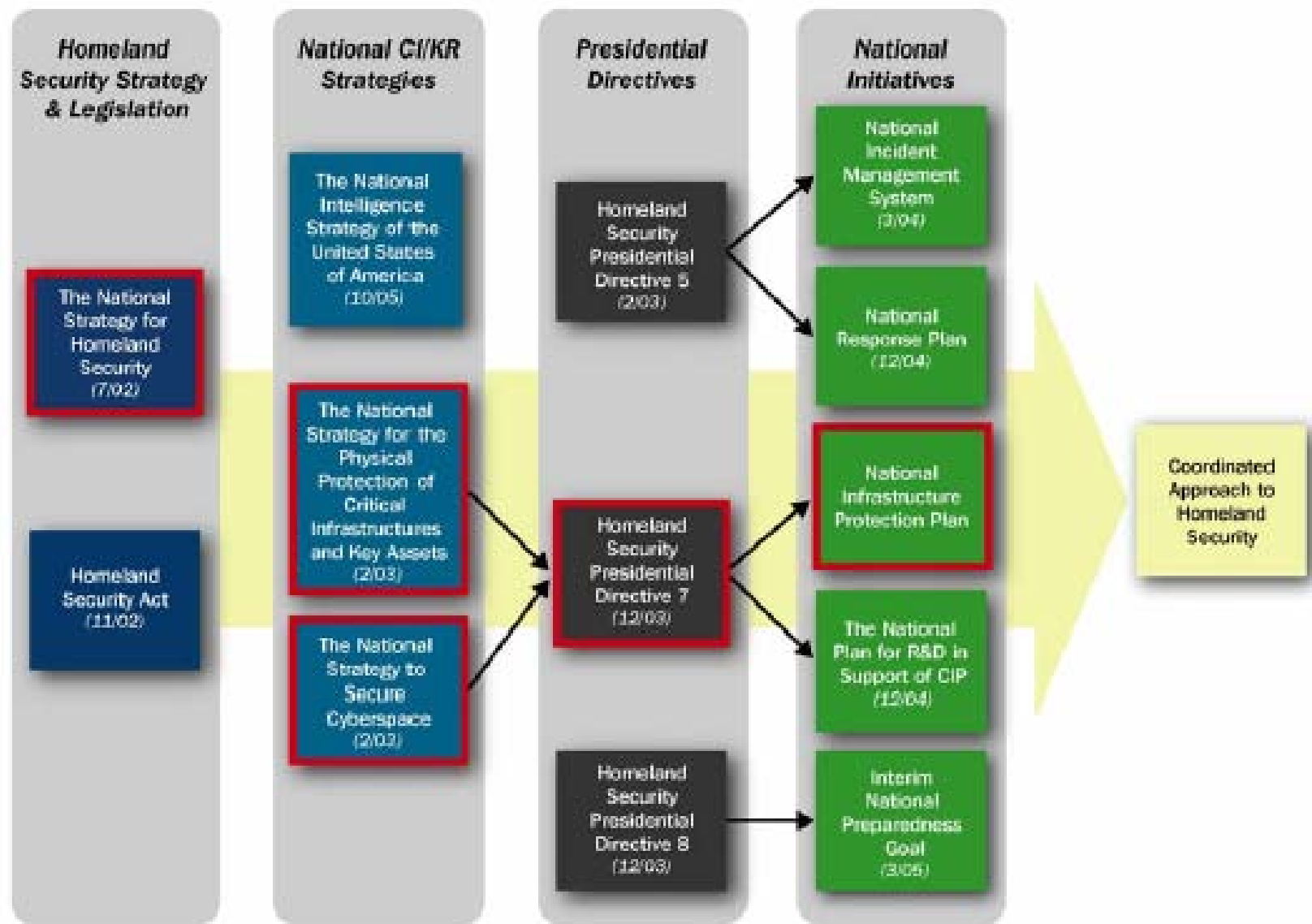


Figure 5-1: National Framework for Homeland Security

Partnership Model

The kind of true partnership that protecting the homeland requires means that we not only share information but also responsibility. It means that we not only exchange expertise but also expect accountability. It means that our partners must bear a part of the security burden as well as become part of the security solution.

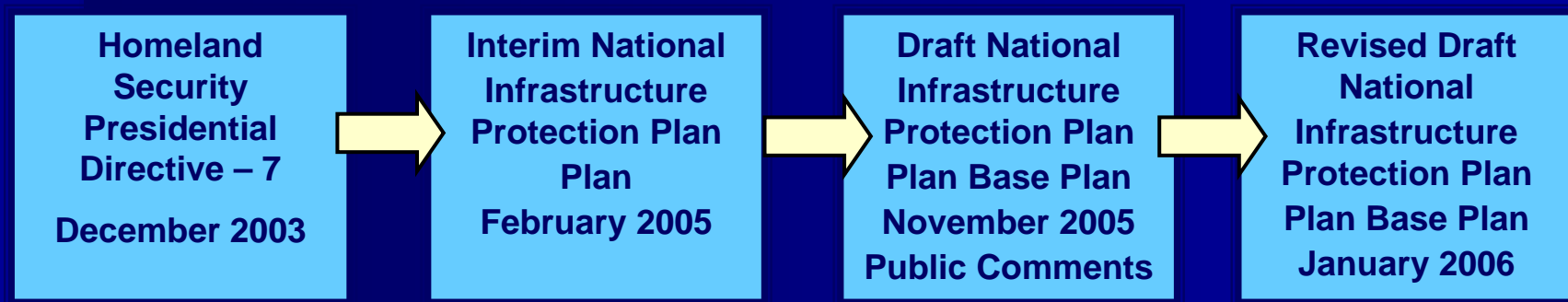
*Michael Chertoff , Secretary
U.S. Department of Homeland Security*

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
- DOE is the Lead Sector Specific Agency
- State, local and tribal governments will have a role in implementation



Federal Sector-Specific Agencies & Assigned Sectors

- **Department of Agriculture**

- Agriculture, food (meat, poultry, egg products)

- **Department of Health and Human Services**

- Public health and healthcare; Food (other than meat, poultry, egg products)

- **Environmental Protection Agency**

- Drinking water and wastewater treatment systems

- **Department of Energy**

- Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)

- **Department of Treasury**

- Banking and finance

- **Department of the Interior**

- National monuments and icons

- **Department of Defense**

- Defense industrial base

- **Department of Homeland Security**

- Information technology
- Telecommunications
- Chemical
- Transportation systems
- Emergency services
- Postal and shipping
- Dams
- Government facilities
- Commercial facilities
- Nuclear reactors, materials, and waste

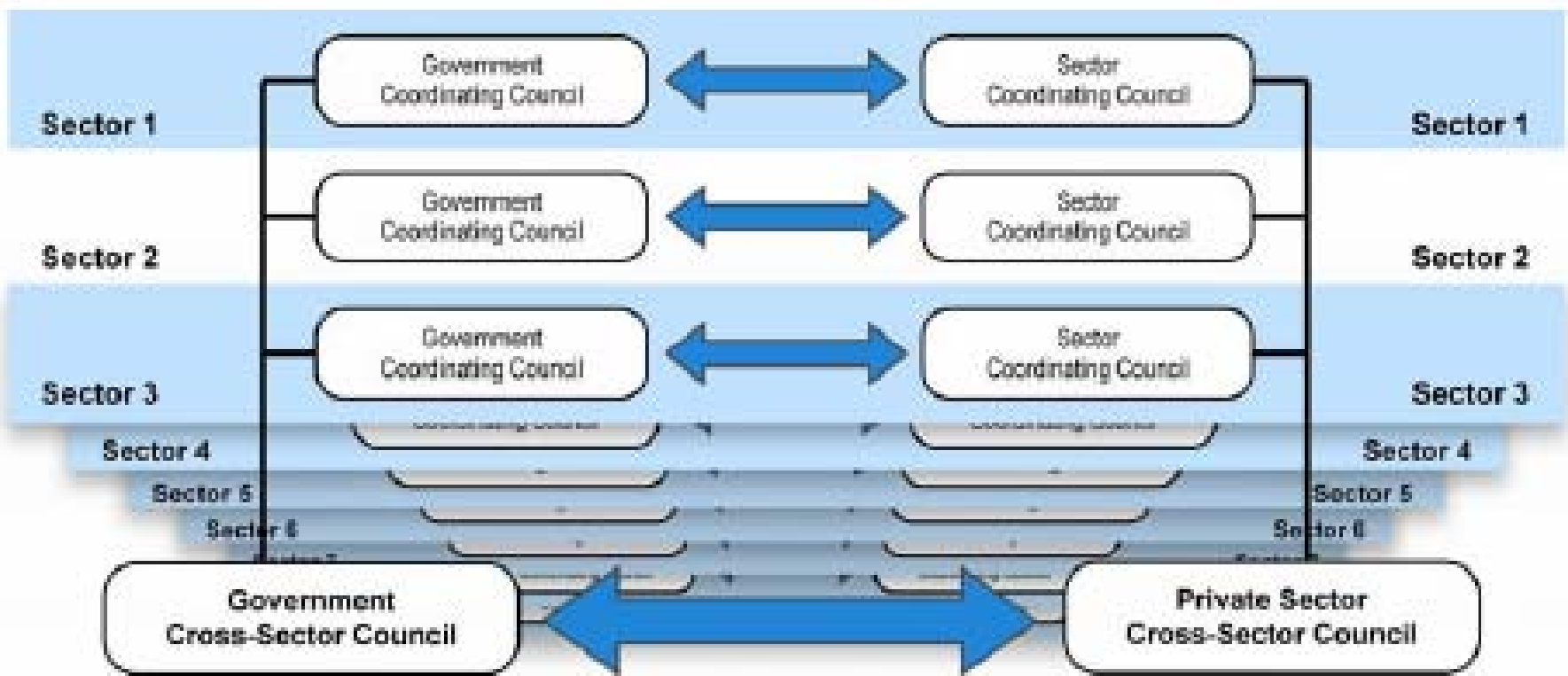
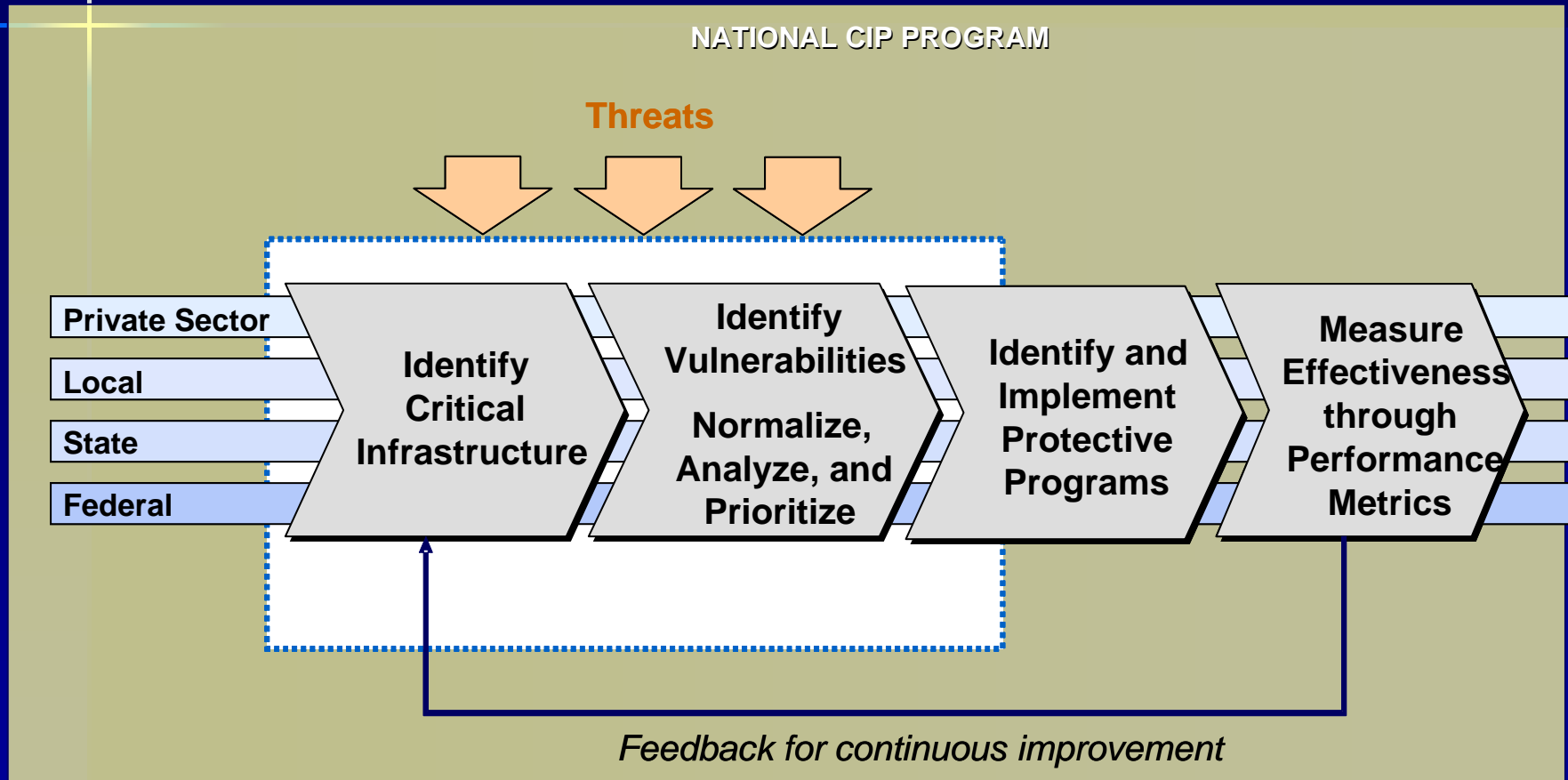


Figure 4-1: Sector Partnership Model

Protecting Critical Energy Infrastructure and Building 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
- Protect of sensitive information
- Build partnerships Public/Private Sectors, Federal, state, local and tribal governments.

Working Towards a National CIP Program



New first step is in draft base plans to include setting Security Goals

Risk is defined by three factors

- **Consequence:** The range of loss or damage that can be expected from a successful attack;
- **Vulnerability:** The characteristic of, or flaw in, an asset, system, or network's design, location, security posture, or operation that renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional Acts, mechanical failures, and natural hazards, and
- **Threat:** The likelihood that a particular target, or type of target, will suffer an attack or incident. In the context of risk from terrorist attack, threat likelihood is based on the analysis of the intent and the capability of the adversary.

Consequences Includes

- **Health Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact:** Direct and indirect effects on the economy (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from unavailability of product or
- **Psychological Impact:** Effect on the public's morale and confidence in national economic and political
- **Governance Impact:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure the public's health and safety, and carry out national security-related missions.

Examples of Other Federal Agencies and Private Sector Initiatives

- 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
- DHS Protective Measures
- Coast Guard Port Security Initiative
- EPA's funding Water Risk & Vulnerability Assessment
- NERC's Mandatory Cyber Security Standards
- API Security Guidelines
- Other Industry guidance

Aligning State and Urban Area Homeland Security Strategies with the National Preparedness Goal

July 22, 2005

National Priorities Overarching Priorities

- Implement the National Incident Management System and National Response Plan
- Expanded Regional Collaboration
- Implement the Interim National Infrastructure Protection Plan (NIPP)

Capability-Specific Priorities

- Strengthen Information Sharing and Collaboration capabilities
- Strengthen Interoperable Communications capabilities
- Strengthen CBRNE Detection, Response, and Decontamination capabilities
- Strengthen Medical Surge and Mass Prophylaxis capabilities

How to apply the NIPP Priority to the State and Urban Area Homeland Security Strategy Update:

States and Urban Areas should consider how they will fulfill the following roles:

- Build a Statewide critical infrastructure protection program that implements the risk management framework outlined in the NIPP.
- Engage all relevant intergovernmental coordination points (e.g., Federal, State, regional, tribal, local) to ensure a comprehensive approach to critical infrastructure protection across all appropriate levels of government and across both public and private sectors.
- Develop strategies for the protection of CI/KR assets not on the Federal list, but which are of concern to the State or Urban Area.
- Incorporate cyber security protection efforts across all sectors of CI/KR.



Questions?

Thank you for your attention

For more information contact:

Jeffrey Pillon

E-mail: jpillo@michigan.gov