National Infrastructure Protection Plan

Overview

March 2006

Prepared By:

Infrastructure Protection Office
Preparedness Directorate

Homeland Security

Vision

The United States will forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructure and key assets from terrorist attack.

The National Strategy for Homeland Security
July 2002

Homeland Security

HSPD-7 Requirements

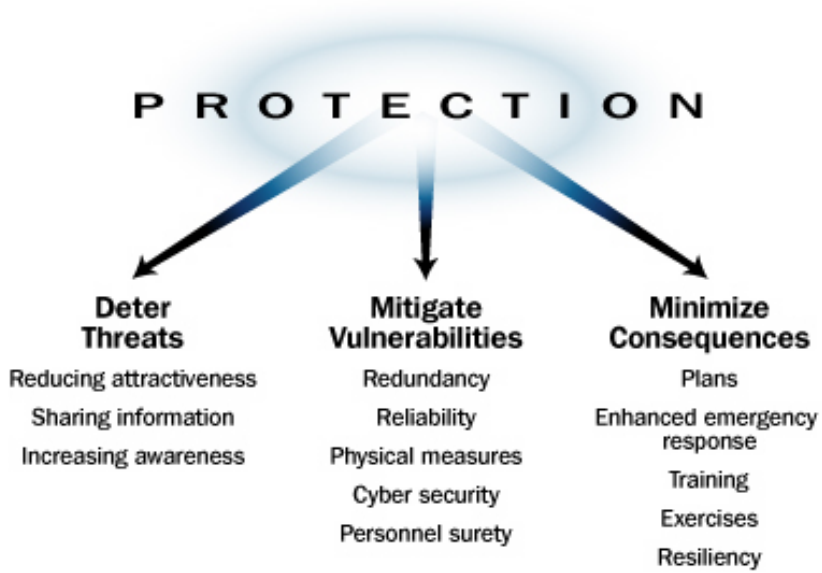
Directs the development of a National Infrastructure Protection Plan (NIPP)

The NIPP is a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources (CI/KR) Protection to outline national goals, objectives, milestones, and key initiatives. The Plan includes the following elements:

- A strategy to identify, prioritize, and coordinate CI/KR protection, including how DHS intends to work with Federal departments and agencies, State and local governments, the private sector, foreign countries, and international organizations;
- Descriptions of activities which: define and prioritize, reduce the vulnerability of, and coordinate CI/KR protection;
- A summary of initiatives for sharing CI/KR information and for providing CI/KR threat warning data to State and local governments and the private sector; and
- Coordination and integration, as appropriate, with other Federal emergency management and preparedness activities

NIPP Goal

Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and enabling national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.



Homeland Security

NIPP Value Proposition

The success of the partnership for CI/KR protection depends on articulating the mutual benefits to government and private sector partners. This value proposition:

- Enables Federal, State, local, tribal and private sector security partners to clearly understand the national CI/KR protection priorities
- Provides CI/KR protection planning, information sharing, risk management, resource coordination, and program implementation processes
- Is intended to be used as a framework for coordinating CI/KR protection efforts across sectors and security partners

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
Key Resources	Commercial Facilities	DHS
	Government Facilities	DHS
	Dams	DHS
	Commercial Nuclear Reactors, Materials, & Waste	DHS

Sector-Specific Agencies (SSAs)

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

Homeland Security

Major NIPP Theme: Roles and Responsibilities

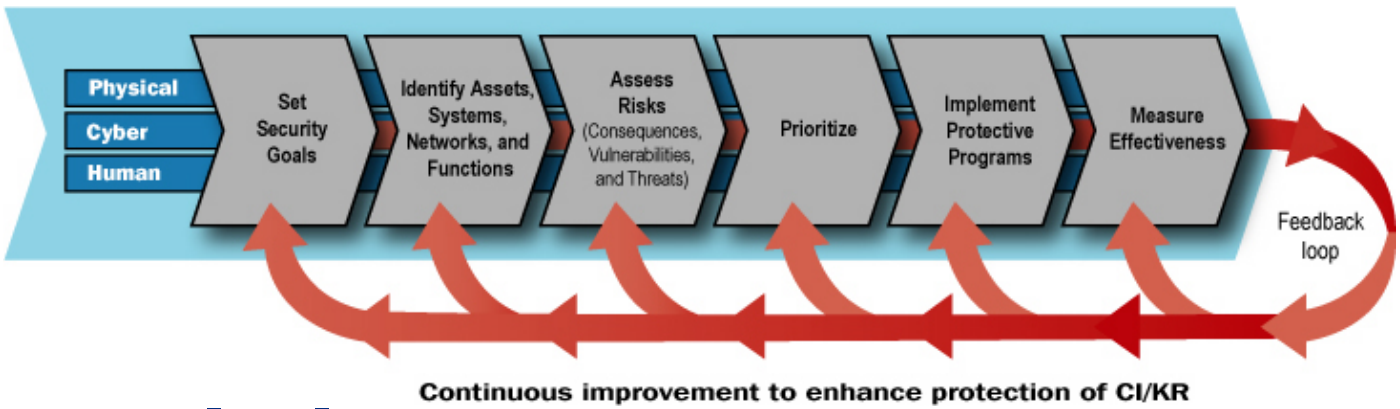
Security Partners:

- **Department of Homeland Security:** Management of the Nation's CI/KR protection framework and overseeing NIPP implementation
- **Sector-Specific Agencies (SSAs):** Implementation of the NIPP and guidance for development of Sector-Specific Plans (SSPs)
- **Other Federal Departments, Agencies, and Offices:** Implementation of specific roles designated in HSPD-7 or other relevant statutes and executive orders
- **State, Territory, Local, and Tribal Governments:** Development and implementation of a CI/KR protection program as a component of their overarching homeland security program
- **Private Sector Asset Owners and Operators:** CI/KR protection, coordination, and cooperation

Major NIPP Theme: NIPP Risk Management Framework

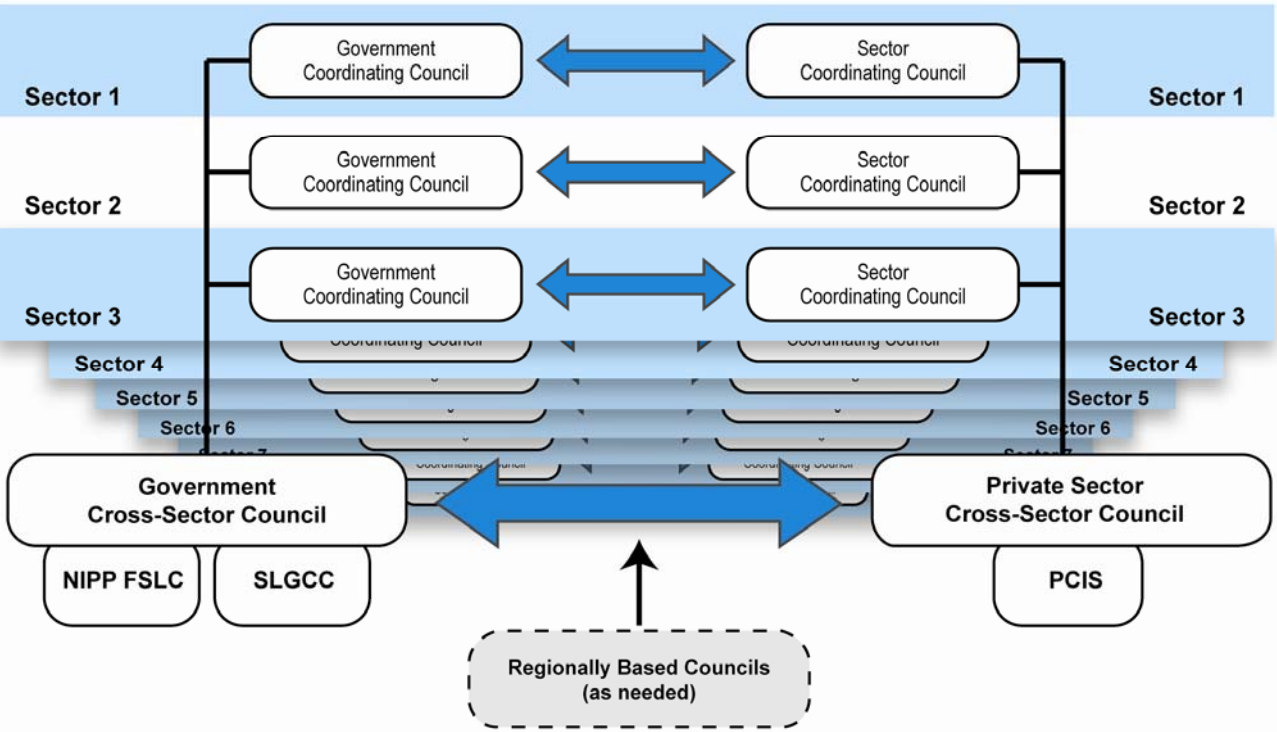
The NIPP and supporting Sector-Specific Plans (SSPs) describe the processes to:

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



Homeland Security

Major NIPP Theme: Sector Partnership Model



Provides the framework for security partners to work together in a robust public-private partnership.

Homeland Security

Critical Infrastructure Partnership Advisory Council

The DHS Secretary established the Critical Infrastructure Partnership Advisory Council (CIPAC)

- Creation of the CIPAC stems from requirements of the Homeland Security Act of 2002 and HSPD-7, from congressional guidance, and from recommendations put forth by private sector advisory councils
- Created to facilitate more effective coordination of Federal infrastructure protection programs with CI/KR activities of the private sector and of State, local, territorial, and tribal governments
- Unlike other advisory councils, the CIPAC role is not strictly advisory in nature, but will engage in the wide range of activities required by the CI/KR protection mission
- Pursuant to Section 871 of the Homeland Security Act of 2002, the DHS Secretary has exempted the Committee from the Federal Advisory Committee Act (FACA) to allow the Department to work more collaboratively with private sector and other CI/KR owners and operators

Homeland Security

Major NIPP Theme: Information Sharing and Protection

The NIPP uses a network approach to information sharing that:

- Enables secure multidirectional information sharing between and across government and CI/KR owners and operators at all levels.
- Provides mechanisms, using “need to know” protocols as required, to support the development and sharing of strategic and specific threat assessments, incident reports and threat warning, impact assessments, and best practices.
- Allows security partners to assess risks, conduct risk management activities, allocate resources, and make continuous improvements to the Nation’s CI/KR protective posture

DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information (PCII) Program, to ensure that CI/KR information is properly safeguarded

Homeland Security

Major NIPP Theme: Providing Resources for the CI/KR Protection Program

Resources must be directed to areas of greatest priority to enable effective management of risk.

The NIPP resource allocation process describes:

- The integrated risk-based approach that will be used to determine how CI/KR protection programs will be prioritized and funded
- How State- and local-level CI/KR protection efforts will be supported through DHS and other CI/KR protection Grant Programs
- How all of these investments, coupled with appropriate incentives, support collaboration among security partners to enhance CI/KR protection

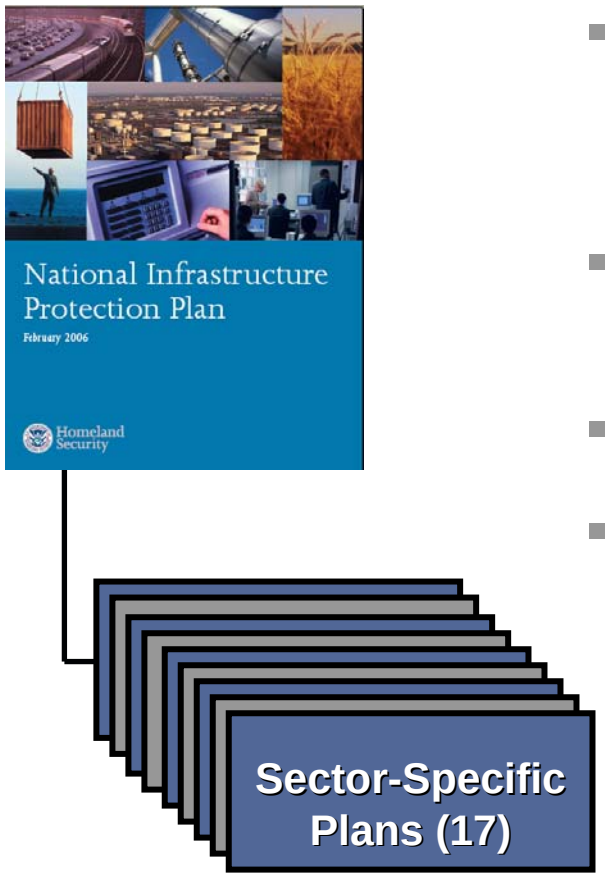
NIPP Development & Coordination

The NIPP was developed as a collaborative process between DHS, SSAs, State, local, and private sector security partners

Review and comment process included broad distribution of the NIPP across all sectors and at each level of government and the private sector and the public to obtain individual comments and input

- Draft NIPP Base Plan was distributed to the following Security Partners:
  - **Federal Government**
    - DHS; Sector-Specific Agencies; HSPD-7 Departments & Agencies; Government Coordinating Councils
  - **State, Local, Territorial, and Tribal Governments**
    - Homeland Security Advisors; State Administrative Agents and Emergency Managers
  - **Advisory Councils**
    - National Infrastructure Advisory Council; National Security Telecommunications Committee; Homeland Security Advisory Committee
  - **Private Sector Partners**
    - Sector Coordinating Councils; Private Sector Security Partners

Sector-Specific Plans (SSPs) Content



- SSPs 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
- SSPs are annexes to the NIPP Base Plan
- Finalized SSPs are to be submitted to DHS within 180 days after the NIPP is issued by the Secretary of Homeland Security

Homeland Security

Next Steps

- **Finalize the NIPP Base Plan**
  - Based on review/comment by HSC Policy Coordination Committee, Deputies Committee, Principals Committee, and DHS Leadership (Deputy Secretary and Secretary) reviews
- Achieve **Final Approval and Sign-off** on the NIPP Base Plan
- Finalize **NIPP Campaign Plan & Rollout Strategy**
- Coordinate with and support SSA efforts to finalize the SSPs
  - **SSPs are due 180 days from the final signature on the NIPP Base Plan**
- **Implement the Risk Management Framework** nationally and across all CI/KR Sectors

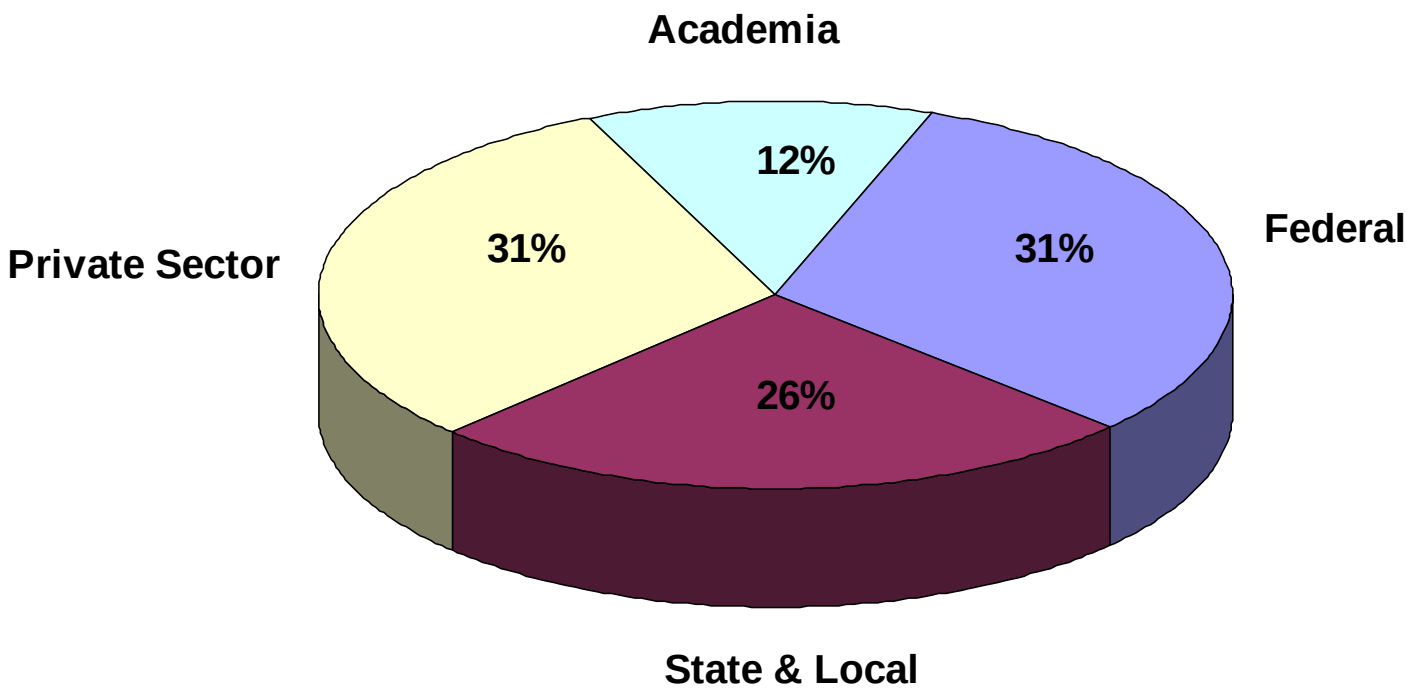
Homeland Security

NIPP Comments Process

- **Nearly 10,000 comments** received and adjudicated
  - First Round: nearly 6500 comments from more than 300 individuals
  - Second Round: nearly 3000 comments from more than 200 individuals

- Timeline
  - Draft 1: Released November 2, 2005
  - Draft 2: Released January 20, 2006
  - **Final: Secretarial approval and HSC coordination – March/April 2006**

NIPP Comments Received from Security Partners



Homeland Security

Comments: Themes and Resolution

- **All Hazards Considerations – Strengthened the linkage between the NIPP and incident management**
- **Goals & Objectives – Additional information on the "value proposition" and "end state" for private sector participation**
- **Roles and Responsibilities – Formed the State and Local Homeland Security Coordinating Council to provide State and local participation in the partnership model**
- **Risk Tools & Criteria – Strengthened the risk management framework, including:**
  - **Detail on assets, systems, networks, and functions**
  - **Greater flexibility for SSAs to utilize a top down/bottom up approach**
- **Information Protection – Strengthened information sharing and protection to include the "information sharing life-cycle"**
- **Resource Allocation – Clarified the resource process and annual reporting requirement**