National Infrastructure Protection Plan (NIPP)

Impact on Protection & Resiliency
Merrick E Krause
Office of Infrastructure Protection
18 Mar 09
National Infrastructure Protection Plan

Strategic Context for Infrastructure Protection & Resiliency Planning

- Dynamic threat environment
  - Natural Disasters
  - Terrorists
  - Accidents
  - Cyber Attacks

- Complex problem requiring a National plan & framework
  - 18 Sectors, from asset-focused to systems to networks
  - Outside regulatory space
  - Vast majority privately owned
  - Nearly all are within State and local jurisdictions

- Updated early 2009 based on inputs & lessons since 2006

“All Hazards” – natural & manmade incidents
National Infrastructure Protection Plan

- Comprehensive plan & unifying structure for government and private sector to improve protection and resiliency of CIKR
- Steady-state risk management and incident management framework
- Drives IP’s activities and guides
  - Other Federal agencies and departments
  - State, local, tribal, and territorial governments
  - CIKR owners and operators
### 18 Sectors & Sector-Specific Agencies

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

- **Roles & responsibilities** – since terrorist attacks & certain natural disasters have a National-level impact, it’s incumbent upon the Federal Government to provide leadership and coordination.

- **DHS coordinates the overall national effort to enhance CIKR protection and resiliency through the implementation of the NIPP**.

- **Sector-Specific Agencies (SSA) lead activities in each of 18 CIKR Sectors and develop and implement Sector-Specific Plans (SSPs)**.
Risk Management Framework

- The NIPP describes processes to
  - Set Goals and Objectives
  - Identify Assets, Systems, and Networks
  - Assess Risk (Consequences, Vulnerabilities, and Threats)
  - Prioritize
  - Implement Protective Programs & Resiliency Strategies
  - Measure Effectiveness

Continuous improvement to enhance protection of CIKR
Assessing Risks & Prioritization

“Risk” = Threat + Vulnerabilities + Consequences

HITRAC
Homeland Infrastructure Threat & Risk Analysis Center

NISAC
National Infrastructure Simulation and Analysis Center

Protection

Manage Risks

Deter Threats

Mitigate Vulnerabilities

Minimize Consequences
Sector-Specific Plans (SSPs) are designed to tailor the NIPP risk management framework to each CIKR sector. They address each sector’s unique characteristics and risk landscape. Sector-Specific Agencies partnered with Sector Coordinating Councils and Government Coordinating Councils to develop these plans. SSPs were released in May 2007 and underwent annual reviews in 2008 and 2009. They are scheduled for a triennial review with reissue in 2010.
Sector Partnership Model

- Critical infrastructure protection & resiliency – shared responsibilities of Federal, State, local, tribal, and territorial governments, regional coalitions, and the owners and operators of America’s CIKR
  - NIPP outlines roles & responsibilities
  - NIPP describes information sharing environment & communications
Cross-Sector Coordination

18 Critical Infrastructure Sectors

- Agriculture/Food
- Banking & Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments & Icons
- Nuclear
- Postal & Shipping
- Transportation Systems
- Water

- Regional Consortium Coordinating Council
- Cross-Sector Cybersecurity Working Group
- CIKR Cross-Sector Council
- State, Local, Tribal, and Territorial Government Coordinating Council
- Federal Senior Leadership Council (FSLC)
National Response Framework
CIKR Support Annex

- CIKR Annex provides a *bridge* between the steady-state critical infrastructure protection and National Response Framework’s (NRF) incident management doctrine
- Addresses recommendations of the Hurricane Katrina after-action
Complex Resiliency Collaboration

Federal Agencies

DHS

FEMA

Other DHS Components

Other Rsch Cntrs

IP

S&T

Universi Programs

IGD

NIPP Public Sector Partners

18 Sector-Specific Agencies & Government at all levels

NIPP Regional Partners

NIPP Partners

18 Sectors with # Assets Per

NIPP Private Sector Partners

Simplified for discussion …
RUN A SIMULATION OF OUR PRODUCTIVITY IF WE LOST HALF OUR WORKFORCE TO A PANDEMIC.

SHOULD I ASSUME WE LOSE THE PRODUCTIVE PEOPLE OR THE PEOPLE WHO ASK OTHER PEOPLE TO RUN PANDEMIC SIMULATIONS?

TRY BOTH WAYS.

OKAY. I'M DONE.
National Infrastructure Protection Plan (NIPP)

Impact on Protection & Resiliency

Merrick E Krause
Office of Infrastructure Protection
18 Mar 09
Homeland Security Act of 2002 established Assistant Secretary for Infrastructure Protection, responsible for assessing vulnerabilities of critical infrastructures & key resources (CIKR) and developing a comprehensive national plan.


Homeland Security Presidential Directives (HSPD) provide policy guidance in the areas of incident management, critical infrastructure protection, and National preparedness.

Hurricanes in 2005 through 2008 affirmed IP’s mission & central role in preparedness and resiliency planning.

National Infrastructure Protection Plan

- Build a safer, more secure, and more resilient America
  - … by preventing, deterring, neutralizing, or mitigating the effects of terrorists to destroy, incapacitate, or exploit our Nation’s CIKR
  - … to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency

“Risk” – Threat + Vulnerabilities + Consequences

- Deter Threats
- Mitigate Vulnerabilities
- Minimize Consequences
NIPP Triennial Review Process

- Process began May 2008 and involved other Federal departments, agencies, and the private sector
- Working sessions held with Sector-Specific Agencies, Partnership for Critical Infrastructure Security, and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTGCC)
- Two Federal Register Notices with opportunity for public review/comment in June and October
- Homeland Security Council Critical Infrastructure Protection Policy Coordination Committee concurrence received 12/23
Summary of Most Significant Revisions

- Incorporation of partnership concept throughout plan
- Metrics section focuses on outcome based metrics, simplifies metrics approach
- Developments in programs, approaches, and tools used to implement the NIPP risk management framework
- Updates on information-sharing mechanisms
- CIKR mission integration in State & local fusion centers
- Cybersecurity & international appendixes enhanced
- CIKR protection-related education, training, outreach, and exercise programs expanded
- Evolution of FEMA’s National Response Plan to the National Response Framework (NRF)
Overview of Key Changes

- NIPP improvements do not change underlying 2006 policy
- 2009 NIPP integrates the concepts of resiliency and protection and broadens the focus of NIPP-related programs and activities to the all-hazards environment
- Changes reflect suggestions and comments …
  - Release of Sector Specific Plans in 2007
  - New HSPDs, National Homeland Security Strategy, legislation
  - Establishment of Critical Manufacturing as 18th Sector
  - Designated Education a subsector of Government Facilities
  - Formed Regional Consortium Coordinating Council
  - Released Chemical Facility Anti-Terrorism Standards