NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience*

PNT Advisory Board Meeting

December 4, 2013

Homeland Security

Table of Contents

NIPP 2013: Partnering for Critical Infrastructure Security and Resilience

Strategic Drivers

President Obama announced two policies related to critical infrastructure security and resilience in February, 2013:

Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive 21:
Critical Infrastructure Security and Resilience

"The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure that are vital to public confidence and the Nation's safety, prosperity, and well-being."

– Presidential Policy Directive (PPD) 21

NIPP Vision

Vision: *A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened*

Security: *Reducing the risk to critical infrastructure caused by natural and manmade physical and cyber threats*

Resilience: *The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions*

Shared Goals

- *Assess and analyze critical infrastructure threats vulnerabilities and consequences to inform risk management*
- *Address multiple threats through sustainable efforts to reduce risk; account for costs and benefits of security investments*
- *Enhance critical infrastructure resilience; minimize the adverse consequences of incidents…as well as effective responses…*
- *Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making*
- *Promote learning and adaptation during and after exercises and incidents*

Critical Infrastructure Today

Ensuring the security and resilience of critical infrastructure in the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life.

16 Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water & Wastewater Systems

Definition: "Assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof"

Homeland Security

Today's Risk Landscape

As America remains at risk of a variety of naturally occurring and manmade threats including:

- Acts of Terrorism
- Cyber Threats
- Extreme Weather
- Pandemics
- Aging Infrastructure

NIPP 2013 offers a distributed approach for addressing the diverse and evolving risk environment

Homeland Security

Many Stakeholders, Many Strengths

NIPP 2013 embraces a collaborative partnership based on comparative advantage—where stakeholder groups bring their individual expertise and resources to bear—building a collective effort and enhancing the overall effectiveness of each partner's contribution.

Federal Government
- National Policy
- Coordination
- Information Sharing

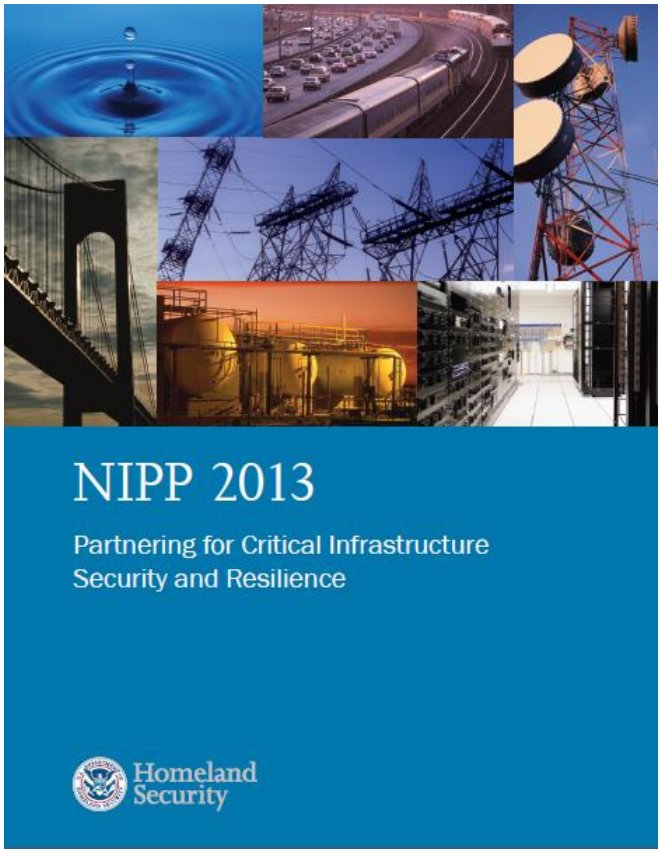
Owners-Operators
- Operations
- Investment
- Customer Relations

State Governments
- Utility Regulation
- Emergency Management
- Law Enforcement

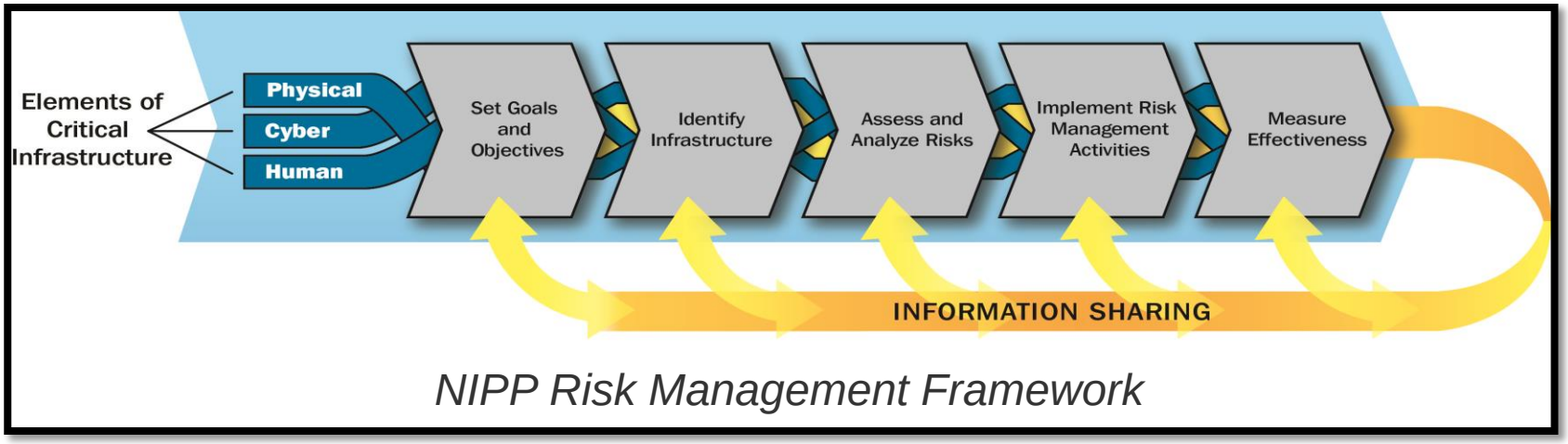
NGOs
- Community Building
- Research
- Standards

Core Tenets

1. Coordinated and comprehensive risk identification and management
2. Cross sector dependencies and interdependencies
3. Enhanced information sharing
4. Comparative advantage in risk mitigation
5. Regional and SLTT partnerships
6. Cross-jurisdiction collaboration
7. Security and resilience by design



Risk Management Framework



NIPP Risk Management Framework

- Partners benefit from access to knowledge and capabilities that would otherwise be unavailable to them
- Risk tolerances and priorities will vary
- Consider costs and benefits during decision making

Call to Action: Next Steps to Advance the National Effort

NIPP 2013 includes a Call to Action that describes how stakeholders work together to promote continuous improvement of security and resilience:

- Build on Partnership Efforts
- Innovate in Managing Risk
- Focus on Outcomes

Call to Action

Build upon Partnership Efforts

- Set National Focus through Joint Priority Setting
- Determine Collective Actions through Joint Planning Efforts
- Empower Local and Regional Partnerships to Build Capacity Nationally
- Leverage incentives to Advance Security and Resilience

Innovate in Managing Risk

- Enable Risk-Informed Decision-Making through Enhanced Situational Awareness
- Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
- Rapidly Identify, Assess, and Respond to… Cascading Effects During and Following Incidents
- Promote Infrastructure, Community, and Regional Recovery
- Strengthen Coordinated Technical Assistance, Training, and Education
- Improve Critical Infrastructure Security and Resilience by Advancing R&D Solutions

Focus on Outcomes

- Evaluate Achievement of Goals
- Learn and Adapt During and After Exercises and Incidents

Questions

Homeland Security