EO-PPD Integrated Task Force

Evaluation and Planning Workgroup

National Infrastructure Protection Plan Update – Public Slides for National Infrastructure Advisory Council

July 17, 2013

Homeland Security

Agenda

- EO-PPD Background and Overview
- EO-PPD Deliverables Update
- NIPP Rewrite Development and Schedule

Enhancing Security & Resilience

State of Critical Infrastructure

- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies

Importance of Partnerships

- A strong partnership between government and industry is indispensable to reducing the risk to these vital systems
- We are building critical infrastructure resiliency by establishing and leveraging these partnerships

Making progress involves joint planning, information sharing, and capability development

Taking Action

President Obama announced two policies in February, 2013:

Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive – 21:
Critical Infrastructure Security and Resilience

- Together, they create an opportunity to effect a comprehensive national approach
- Implementation efforts will drive action toward ***system*** **and** ***network*** security and resiliency

EO 13636 and PPD-21

Integrating Cyber-Physical Security

Executive Order 13636

Directs the Executive Branch to**:**

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections
- Explore the use of existing regulation to promote cyber security

PPD-21

Directs the Executive Branch to:

- Develop situational awareness capability that addresses both physical and cyber aspects
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan
- Understand the cascading consequences of infrastructure failures

EO-PPD Deliverables

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

150 Days - **July 12, 2013**

- Identify cybersecurity critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

240 Days – **October 10, 2013**

- Develop a situational awareness capability
- Update the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

- Critical Infrastructure Security and Resilience R&D Plan

Passing the First Milestones

120 Days

- ✓ Incentives Reports from DHS, Commerce and Treasury
- ✓ Description of critical infrastructure functional relationships, which illustrates the Federal Government's current organizational structure to deliver risk management support to stakeholders and make it easier for them to collaborate with the Government;
- ✓ Instructions on producing unclassified cyber threat reports from all-source information to improve the ability of critical infrastructure partners to prevent and respond to significant threats;
- ✓ Procedures for expansion of the Enhanced Cybersecurity Services (ECS) program to all critical infrastructure sectors; and
- ✓ Recommendations on feasibility, security benefits and merits of incorporating security standards into acquisition planning and contract administration

PUBLIC-PRIVATE PARTNERSHIPS FOR CRITICAL INFRASTRUCTURE SECURITY

Mandate and Research Questions

Public-Private Partnership Analysis and Recommendations

PPD-21 requires that the Department of Homeland Security (DHS) "conduct **an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership** in both the physical and cyber space."

To this end, the EO/PPD Integrated Task Force (ITF) addressed the following research questions:

- How well does the current public-private partnership approach function and does it produce desired outcomes?
- What are opportunities for enhancing that partnership to achieve the desired purpose of the partnership?

Purpose of Critical Infrastructure PPPs

To provide context for the study (and other efforts), the ITF (in collaboration with CI community of stakeholders) created the following purpose statement for the critical infrastructure PPP:

Purpose Statement: Secure and make resilient the Nation's critical infrastructure by applying the spectrum of capabilities, expertise, and experience through proactive engagement across the critical infrastructure community.

Findings

Criteria

The evaluation identified **criteria** that define an effective public-private partnership:

1. Defined Purpose
2. Articulated Goals
3. Robust Membership
4. Engaged Leadership
5. Defined and Flexible Governance
6. Open Communication
7. Trusted Environment
8. Evaluated Outcomes

Mechanisms

The evaluation identified **"mechanisms"** by which public-private partnerships may promote CI security and resilience:

1. Policy Coordination
2. Joint Planning and Prioritization
3. Capability Development
4. Information Sharing
5. Shared Risk Management
6. Incident Management
7. Research and Development.
8. Joint Investment

PPP Report Recommendations

- Recommendations aim to strengthen the existing partnership model, as opposed to remaking it.
- Evaluation demonstrated the model has oftentimes produced the desired outcomes of joint efforts to manage critical infrastructure risk but that too often it fell short of proactively addressing evolving and emerging risks and being outcome-oriented

1. Affirm the purpose and value of the partnership
2. Set shared goals and review annually
3. Shift from process-focused operations to capability and performance
4. Define role and provide support to sector specific agencies
5. Leverage regional networks to expand reach
6. Launch National Critical Infrastructure Security and Resilience Innovation Challenge Program
7. Link the NIPP to incident management planning and policy
8. Define information sharing roles and responsibilities to reduce redundancy

UPDATING THE NATIONAL INFRASTRUCTURE PROTECTION PLAN

Public Comments on NIPP FRN

- 27 submissions were received, which break down as follows:
  - Trade Associations (Public & Private): 7 — Federal Agencies: 2
  - Private Sector (including 1 SCC): 5 — ISACs: 3
  - SLTT Governments/Associations: 6 — Individuals: 4
- Overall: Comments validated PPP findings to maintain existing partnership structures and build upon them. A more flexible strategy is needed to allow sectors to apply differing models (e.g., some with regulatory components, others voluntary).
- Risk Management: Need more flexible risk management strategy.
- Partnerships: Need renewed commitment to partner on cybersecurity goals
- Information Sharing: Emphasis on using SSAs, SCCs, and ISACs for information sharing. Recommend Critical Infrastructure Partnership Advisory Council framework remain intact and effectively utilized, as appropriate

Public Comments on NIPP FRN

- Regional Emphasis - Increase emphasis on a regional approach to critical infrastructure security and resilience; further integrate PS and SLTT into incident management
- All-sector focus: Emphasis within NIPP should be all sector focused due to changing threat environment (sub-sectors should be of equal importance).
- Resource Allocation - Resources and capabilities should be better coordinated to inform greater common situational awareness;
- Infrastructure Investment: Address the barriers to financing infrastructure improvements to be more resilient to the hazards posed by aging infrastructure and climate change

NIPP Update Purpose and Challenge

Purpose:

Guide the collective effort to strengthen the security and resilience of the Nation's critical infrastructure.

Challenge:

Developing the Plan in collaborative manner, recognizing the evolving risk landscape and complex decision-making environment of diffuse authorities and responsibilities

Guiding Principles

Through partnerships, infrastructure is made more secure and resilient

Build on the successful work to date and leverage existing knowledge and structures wherever possible

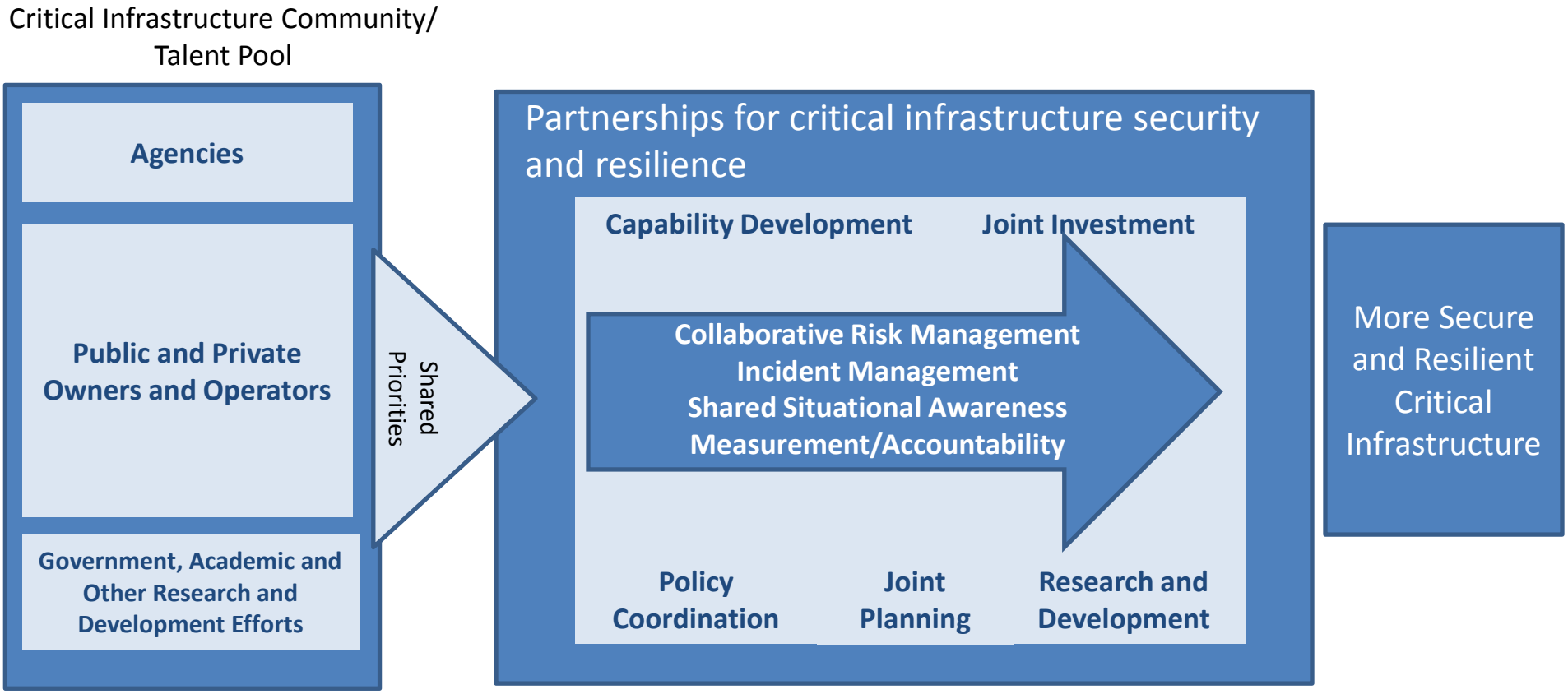
Describe the conditions that necessitate an updated approach to critical infrastructure security and resilience

Lay out the broad principles and policies that underpin this approach in the public and private sectors

Describe the national program that will implement these principles and policies to achieve shared outcomes

Narrative for the Successor to the NIPP

Guide collective efforts to secure and make resilient the Nation's critical infrastructure



Applying the spectrum of capabilities, expertise, and experience through proactive engagement across the critical infrastructure community

Homeland Security

For Discussion: Draft Table of Contents

- **Introduction**
  - Scope, Vision
  - Challenge/Problem Statement
  - Building on the Partnership Model
  - Critical Infrastructure Security and Resilience Environment
- **Guiding Principles, Roles and Relationships**
  - Maintain a strong public-private partnership model
- **Fundamentals of Risk Management/ Best Practices**
- **Driving Collective Action**
  - Execute partnership mechanisms and functions to achieve shared risk management to elevate the level of security and resilience for steady state and incident management
  - Share information to identify and assess risk and criticality
  - Enhance situational awareness to recognize and adapt to emerging risks as well as incidents
- **Maintaining and Sustaining Collective Efforts**
  - Education and Awareness
  - Innovation and R&D
  - Resource allocation
  - Evaluate, measure and report

QUESTIONS

Homeland Security