Regional Resilience Planning and Development Through Public-Private Partnerships

Moderator: C. Ernest Edgar, P.E., Atkins
Speakers:

- Greg Carnevale, Critical Manufacturing & Defense Section Chief, Office of Infrastructure Protection, Department of Homeland Security
The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Regional Planning and Development through Public Private Partnerships

Section Chief, Greg Carnevale
Sector Outreach and Programs Division

May 21, 2015
The DHS’s Office of Infrastructure Protection (IP), leads and coordinates a nationwide network supporting critical infrastructure security and resilience.

**IP CORE CAPABILITIES**

- Information & Data Sharing
- Situational Awareness
- Assessments
- Partnerships & Capacity Building
DHS Authorities

Homeland Security Act of 2002

- Coordinated and comprehensive risk identification and management
- Establishes the framework for the private–public partnership
- Security and resilience by design


- Enhanced information sharing
- Regional, State, Tribal, & Territorial partnerships
- Cross-jurisdictional collaboration
- Cross-sector dependencies and interdependencies
- Comparative advantage in risk mitigation
Critical Infrastructure defined: “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 national security, economic security, national public health or safety, or any combination thereof.”

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
Many Stakeholders, Many Strengths

**Comparative Advantage**

- Engaging in collaborative processes
- Applying individual expertise
- Bringing resources to bear
- Building the collective effort
- Enhancing overall effectiveness
Strategic Drivers

Diverse Stakeholders

Complex Interdependencies

Evolving Threats

National Policies

Natural
Physical
Cyber

Homeland Security

June 17, 2003
America remains at risk from a variety of threats including:

- Acts of Terrorism
- Cyber Attacks
- Extreme Weather
- Pandemics
- Accidents or Technical Failures

NIPP 2013 offers a distributed approach for addressing the diverse and evolving risk environment.
Call to Action

A whole of community approach to advancing the national effort

Build on Existing Partnerships  Innovate in Managing Risk  Focus on Outcomes
## What Your Organization Can Do

<table>
<thead>
<tr>
<th>Build Upon Partnership Efforts</th>
<th>Innovate in Managing Risk</th>
<th>Focus on Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand the critical infrastructure landscape and how to regionally partner with stakeholders</td>
<td>Provide support for assessing criticality and managing risk</td>
<td>Understand dependencies and interdependencies</td>
</tr>
<tr>
<td>Bring private sector into linkages with Emergency Management and Law Enforcement communities</td>
<td>Utilize tools available from DHS (i.e. assessments, best practices guide, resilience guidelines)</td>
<td>Participate in implementation efforts</td>
</tr>
<tr>
<td>Embrace NIPP Calls to Action</td>
<td>Keep informed through actions sent out by the TISP Council</td>
<td>Establishment/awareness of regional consortia</td>
</tr>
<tr>
<td>Contact your Local Protective Security Advisor</td>
<td>Participate in DHS Voluntary Programs</td>
<td></td>
</tr>
</tbody>
</table>

**Contact Information:**

PSCDOperations@hq.dhs.gov