

National Infrastructure Advisory Council (NIAC)



Optimization of Resources for Mitigating Infrastructure Disruptions Working Group

October 19, 2010

Tom Noonan
Former General Manager,
IBM Internet Security Systems

Margaret Grayson
Vice President, Management & Compliance,
Tremco Roofing and Building Maintenance,
RPM Building Solutions Group

Overview

- Study Context: The DHS Mission
- Key Aspect: Enhancing the Synergy Between Infrastructure Resilience and Community Resilience
- Study Approach
- General Observations
- Findings
- Recommendations
- Study Leadership

Study Context: The DHS Mission

- The Administration has established a new strategic framework for the Department of Homeland Security.
- A core mission of resilience: “Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery.”
 - Mitigate risks to communities.
 - Enhance recovery capabilities.
 - Ensure continuity of essential services and functions.
- An objective of ensuring *infrastructure* resilience:
“Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.”
- An objective of ensuring *broad-based* resilience:
“Improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions.”

Key Aspect: Enhancing the Synergy Between Infrastructure Resilience and Community Resilience

- **Infrastructure resilience** is the ability to reduce the magnitude and/or duration of disruptive events. It is the ability to *anticipate, absorb, adapt to, and/or rapidly recover* from a potentially disruptive event.
- **Community resilience** is the capability to return citizens to work, reopen businesses, and restore the basic services and economic stability of a community or a linked group of affected communities.
- **Sectors may provide key resource capabilities;** e.g.
 - Lessons learned and model approaches.
 - Leadership in planning and response for service restoration.
 - Understanding of interdependencies, vulnerabilities, and options for resilient capabilities.

Framing the Study

- Leading Questions

- What are the potential enablers of infrastructure resilience that can support and strengthen community resilience?
- Are there significant weaknesses in infrastructure resilience that limit the ability of communities to achieve resilience?

- Supporting Questions

- **Functions**; e.g., What are current practices in aligning infrastructure resilience with community resilience?
- **Resources**, e.g., What are opportunities to enhance collaborative resource planning and management?
- **Government Policy and Programs**, e.g., What steps might the government take to encourage the contribution of infrastructure resilience to community resilience?

Study Approach

- **Four Phases**
 - **Eliciting Community Perspectives and Insights:** Developing an information baseline that crosscuts infrastructure sectors through discussions with the SLTTGCC, RCCC, other regionally-focused organizations and experts.
 - **Capturing Owner/Operator Perspectives:** Interviews and discussions with SMEs from key sectors to share results of first phase and build joint picture of infrastructure/community resilience.
 - **Comparing Community and Owner/Operator Perspectives:** Engagements to clarify and expand on identified issues and improve joint understanding of problems *and* potential solutions.
 - **Identifying and Clarifying Key Findings and Recommendations:** Assessment of gaps in resource availability and coordination and potential improvements in identifying, sharing, and developing efficiencies in resources use.

General Observations

- Preparedness and leadership, public and private alike, is vitally important to community resilience.
- Personal responsibility plays a key role in resilience, and efforts such as the FEMA Citizen Corps are critical to resilience at all levels – individual, community, regional, and national.
- Infrastructure sectors contribute not simply as service providers, but as employers, individuals, family members, volunteers, and neighbors.
- Many critical sectors and governments have long-established, well-proven programs and processes for resource sharing during disruptive events.

Findings

- The resilience component of the NIPP is not well understood by public and private partners alike – there is no widely shared view of what resilience activities are and how they contribute to community resilience.
- At the community level, interdependencies – among infrastructure and across communities – are often not well defined or understood.
- Education of stakeholders is critical and should be enhanced - a shared understanding of resilience is fundamental to progress.

Findings (continued)

- In general, many infrastructure systems are designed to be resilient in order to satisfy customer demands for service availability; none-the-less, cascading events may trigger unforeseen complications from interdependencies.
- Development of structured relationships and processes between critical infrastructure and the communities they serve is necessary, *but not sufficient*, for success.
- Testing and exercising of these relationships and processes is *necessary* for success.

Findings (continued)

- Existing information sharing mechanisms can be effective models for improving communications and understanding across sectors and communities.
- Mutual-aid agreements and other existing infrastructure sector and government mechanisms for resource management can be effective tools to aid community resilience.
- The legal and regulatory environment can vary significantly across different service areas, and may hamper the ability of service providers to bring to bear additional resources during times of service disruption.

Recommendations

1. Improve the understanding of resilient activities and how they are implemented.

- Develop a common framework to enable infrastructure and community partners to identify, plan, implement, and assess resilient activities.
- Encourage the development of regional infrastructure protection plans and catastrophe planning teams.

2. Enhance regional and community-level information exchange through the increased availability of data, information, tools, and techniques.

- Improve the representation and contributions of infrastructure owners/operators in Fusion Centers.
- Enhance owner/operator participation in national and regional exercises.

Recommendations (continued)

3. Expand the provision of scalable, low-cost tools and techniques.

- Champion the development and transfer of infrastructure-focused tools such as dependency analysis, and cybersecurity assessment.
- Expand the Regional Resiliency Assessment Program to enhance local, community, and regional resilience alike.

4. Enhance the transfer of expertise and lessons learned from national-level planning and analysis to regional and community-level systems.

- Sponsor regional-level exercises devoted to the distribution of goods and services.
- Expand non-traditional mechanisms such as webinars to deliver federally-developed training.

Recommendations (continued)

5. Develop a national “playbook” to identify the impact on infrastructure services from threat-level changes in the National Security Advisory System.

- Reduce unintended negative consequences on service delivery by improving the public-private understanding of actions and responses.
- Develop protocols that can accurately communicate these impacts to the public.

6. Remove cross-jurisdictional impediments to moving and using outside assets during emergencies.

- Identify key bottlenecks and implement standard approaches.
- Collaborate to develop model state legislation to ease restoration efforts.

Study Leadership

- NIAC Working Group and Sponsors
 - **Peg Grayson**, Vice President, Management & Compliance, Tremco Roofing and Building Maintenance, RPM Building Solutions Group
 - **Tom Noonan**, Former General Manager, IBM Internet Security Systems
- Study Group
 - **Peter Allor**, Senior Security Strategist, IBM Corporation
 - **Cherrie Black**, SLTTGCC Co-Chair and Chair, Regional Partnership Working Group
 - **Lt. Gen (ret.) Albert J. Edmonds**, Chairman, Edmonds Enterprise Services, Inc.
 - **Patrick Gray**, Principal Security Strategist, CISCO Systems
 - **David Kepler**, Executive Vice President, Chief Sustainability Officer, Chief Information Officer, Dow Chemical
 - **James B. Nicholson**, President and Chief Executive Officer, PVS Chemicals, Inc.
 - **Ulrie Seal**, SLTTGCC Chair

Questions

Questions?