AASHTO Special Committee on Transportation Security

Fundamentals of Effective All-Hazards and Security Management for State DOTs

SCOTS Annual Meeting
August 2007
Project Objective from SOW

- Develop “compelling materials”
  (Short, plain English, on topic)
- That “communicate to agency leaders”
  (Set in DOT context, avoid “weeds”)
- “Fundamentals of... all hazards security program”
  (Must cover a lot of ground)
No State Left Behind

or

NSLB

or

“Toward a Unified Theory of Effective All-Hazards and Security Management for State DOT’s”
Guiding Statements

“You have to think viciously” - John Voeller
“Imagination is more important than knowledge.”
- Al Einstein
“The missing ingredient in hazard and security planning is imagination.”

Imagine that your whole organization agrees on the following:

- What you have to believe as your goals:
- What you have to understand as your responsibilities:
- What you have to be able to do:
Overarching Goals
(DOT missions fit with security goals?)

1. Safeguard lives of transportation system users and DOT personnel
2. Protect property and transportation system assets
3. Minimize disruption and delays to transportation system
Key Capabilities
(Some are new, some are old?)

- Security awareness
- Readiness, response & recovery
- Critical infrastructure & key asset protection
2007 Security Priorities for State DOTs

Responses Grouped by Category*

- Securing Transportation Infrastructure (Particularly Bridges) - 35
- All Hazards Emergency Prevention, Preparation, Mitigation, response, and Recovery - 14
- Employee Training & Awareness - 13
- Evacuation Planning - 8
- Communications & Information Exchange - 4
- Continuity of Operations - 4
- Other - 19

*Authors developed categories to summarize DOTs’ individual responses

(Note: 36 DOTs responded to this question)
Transportation System Threats

Impact of occurrence

Probability of occurrence

Possible Occurrences

Terrorism

Traffic Collisions/Highway Fatalities

Vandalism
Your Area of Prime Responsibility

Possible Occurrences

Impact of occurrence

Probability of occurrence
Fundamental Responsibilities

1. Prevent incidents within control of DOT
2. Protect transportation system users, DOT personnel, and critical infrastructure and key assets, and mitigate loss by responding to incidents and events
3. Support regional, state, and local incident response with resources
4. Recover promptly from incidents with available resources, systems, and programs
5. Evaluate each incident response and continually improve and update plans and procedures.
Organizational Framework
Example “Fundamentals”

1. Avoid narrow or niche security structures
2. Create all hazards/security manager position
3. All hazards/security manager reports to senior management
4. All hazards manager has strong interpersonal skills and generalist expertise
5. Establish an inter-disciplinary committee to address all hazards and security
6. Participate in other state and Federal agency emergency management activities
Linking Goals, Responsibilities, and Capabilities

NIMS-based Countermeasures
Organizational Framework
Planning
Planning
Example “Fundamentals”

1. Ensure all plans are consistent with the principles embedded in NIMS, ICS, and NRP
2. Create an overall base *DOT Emergency Management Plan*; integrate other plans into it; Create Hazard Annexes or Incident Management Plans to support the overall DOT Emergency Management Plan
3. Establish a Continuity of Operations Plan - Essential (COP-E) and a Continuity of Operations Plan (COOP)
4. Update plans on a regular basis
## Typology of Countermeasures

<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Prevention</td>
<td>Actions taken to try to ensure that harmful security and hazard events do not occur</td>
</tr>
<tr>
<td>2. Preparation</td>
<td>Actions taken to anticipate and minimize the harmful impacts of events and to insure that DOT reactions to events are efficient and effective</td>
</tr>
<tr>
<td>3. Mitigation</td>
<td>Actions taken to reduce or eliminate long term risk harm from hazard and security events and to reduce the human consequences or asset loss of an event</td>
</tr>
<tr>
<td>4. Response</td>
<td>Those activities taken to react to incident and events consistent with plans and procedures using all appropriate resources.</td>
</tr>
<tr>
<td>5. Recovery</td>
<td>Actions taken to promptly return to normal</td>
</tr>
</tbody>
</table>
Key Terms

- Prevention
- Mitigation
- Preparedness
- Response
- Recovery
34 Actions in 3 Categories:

1. Physical Security
   - Conduct regular physical security inspections of all security critical facilities and assets

2. Public Security and Emergency Awareness
   - Use real time traffic congestion website capabilities to post information about time, location, and nature of incidents and updates and as incident is cleared

3. Information Sharing
   - Participate in information sharing processes for threat and intelligence information
Preparation – Example “Fundamentals”

58 Actions in 6 Categories:
Control access to sensitive information
• Training and training tracking
• Homeland Security Advisory System (HSAS)
• Emergency traffic operations and evacuation
• Communications interoperability and notification
• Memorandums of agreement and mutual aid agreements
• Equipment, facilities and personnel inventory management
Conclusion and Next Steps

- Draft distributed for comment
- Share comments with S.A. Parker
- Final document ready by end of September

Thank you!