

Department of Homeland Security Office of Infrastructure Protection

Dean Checknita

Chief, Risk Development and Modeling Branch
Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

November 16, 2010



Homeland
Security

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 16 NOV 2010		2. REPORT TYPE		3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE Challenges in Infrastructure Risk Management Analysis in a Distributed Risk Management Environment				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Homeland Security, Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), Risk Development and Modeling Branch, Washington, DC, 20528				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Optimizing Investments in Critical Infrastructure Protection, 15-18 Nov 2010; ANSER Conference Center, Arlington, VA.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 11	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Challenges in Infrastructure Risk Management Analysis in a Distributed Risk Management Environment

Military Operations Research Society

Nexus of National Security and Homeland Security

Working Group 4, Session 1



Homeland
Security

Agenda

- Distributed Risk Management Environment
- Security vs. Resilience
- Risk Avoidance vs. Risk Tolerance
- Way Ahead



**Homeland
Security**

Distributed Risk Management Environment

The homeland security “enterprise” refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners — as well as individuals, families, and communities — to maintain critical homeland security capabilities. It connotes a broad-based community with a common interest in the safety and well-being of America and American society.

Quadrennial Homeland Security Review Report, February 2010



**Homeland
Security**

Distributed Risk Management Environment (Cont.)

- There is an expectation of local, high-fidelity coverage throughout the Nation
- Much of the infrastructure and data are privately owned
- The NIPP taxonomy for administration does not correlate well with physical “systems of systems”
- The lack of consistency among systems increases the challenge in performing cross-sector analysis
- The network topology of the systems does not correlate with political boundaries



Security vs. Resilience

- National Preparedness Goal Balances Security vs. Resilience
 - Resilience is a buzz word on the Hill
 - Security
 - Something that secures: protection
 - Measures taken to guard against espionage or sabotage, crime, attack, or escape
- Merriam-Webster



**Homeland
Security**

Security vs. Resilience (Cont.)

- Resilience

- Ability of systems, infrastructures, government, business, and citizenry to resist, absorb, recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance
- Capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures

– DHS Risk Lexicon



**Homeland
Security**

Security vs. Resilience (Cont.)

Infrastructure Risk Management Continues to Mature

- Started with asset protection from terrorists: gates, guards, guns
 - Police/Security function
- Next evolution was understanding dependency on inputs to the asset
 - Police/Security Plus function
- Current evolution was understanding a nodes role within a system/network
 - Operations Analyst/Systems Engineer/Logistician function
- Programs stuck in Police/Security mode will not evolve



Risk Tolerance

- **Risk Avoidance:** strategies or measures taken that effectively remove exposure to a risk
- **Risk Control:** deliberate action taken to reduce the potential for harm or maintain it at an **acceptable** level
- **Risk Tolerance:** degree to which an entity, asset, system, network, or geographic area is willing to accept risk



Way Ahead

- Continue to collaborate and coordinate
- Look within organizations for systems analysis expertise
- Continue to work with private sector partners



**Homeland
Security**



Homeland
Security