National Defense Industrial Association

Protecting What Matters

Strategies for Critical Infrastructure Resilience

Homeland Security Symposium

September 27, 2011

The Panel

- John Paczkowski
  - Vice President, Homeland Security and Resilience, ICF International
  - Former Director, Emergency Management and Security, Port Authority of New York and New Jersey

- Mike McAllister
  - Deputy Secretary, Veterans Affairs and Homeland Security, Commonwealth of Virginia
  - Co-Chair, DHS State, Local, Tribal, Territorial Government Coordinating Council

- Darrell Darnell
  - Senior Associate Vice President for Safety and Security, The George Washington University
  - Former Director, Critical Infrastructure Protection and Resilience Policy, The White House, National Security Staff

The Focus and Objectives

National Defense Industrial Association

- Regardless of ownership, operation, or location, infrastructure owners and operators have to be prepared for the worst.
- Underscore the vital importance of preparing for and protecting the nation's critical infrastructure from the ever present threats.
- Offer some insights on the trend toward "Resilience" and lessons learned from an organization, regional, and national perspective.
- Engage in an open exchange on infrastructure risk management and resilience among panel members and symposium participants.
- It is not a discussion from defense perspective but one that may somewhat enlighten us all and spark some ideas and take-aways.

The Audience

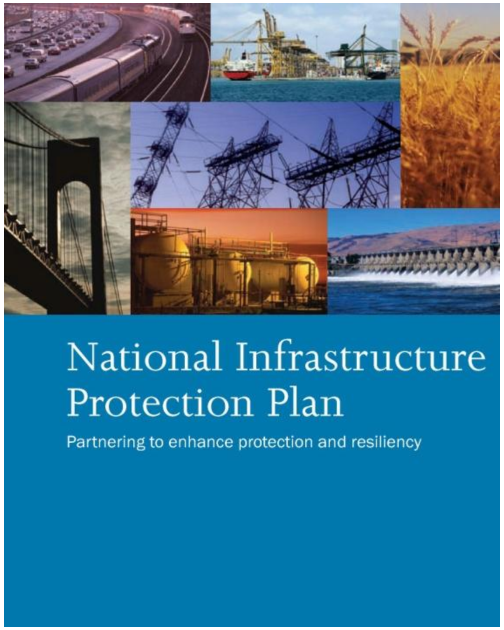
- NDIA - 1,780 corporate and 87,700 individual members from industry, the military, government, academia, and the international community.
- Make up the Defense Industrial Base (DIB) as defined by the President, DOD, and DHS, and DOD Guidance
- Research and development, design, production, delivery, and maintenance of weapon systems, subsystems, components, or parts.
- Diverse, autonomous, geographically dispersed, and highly interdependent with other critical infrastructure sectors.
- DIB owners are responsible for their own assets, in “an open, global environment that exacerbates the vulnerability of DIB Sector assets.”

A Few Words on the NIPP

- Critical Infrastructure - Systems and assets so vital that their incapacitation or destruction would have a debilitating impact on national security, the national economy, or public health or safety…
- National Infrastructure Protection Plan (NIPP)
  - A DHS National Strategic Context for critical infrastructure protection and resilience in response to a dynamic threat environment.

Natural Disasters	Terrorist Incidents
Cyber Attacks	Technical Hazards

- 18 Infrastructure Sectors
  - All different, yet interdependent
  - Asset-focused to systems and networks
  - Generally outside regulatory space
  - 85% privately owned and/or operated
  - 100% in State and local jurisdictions



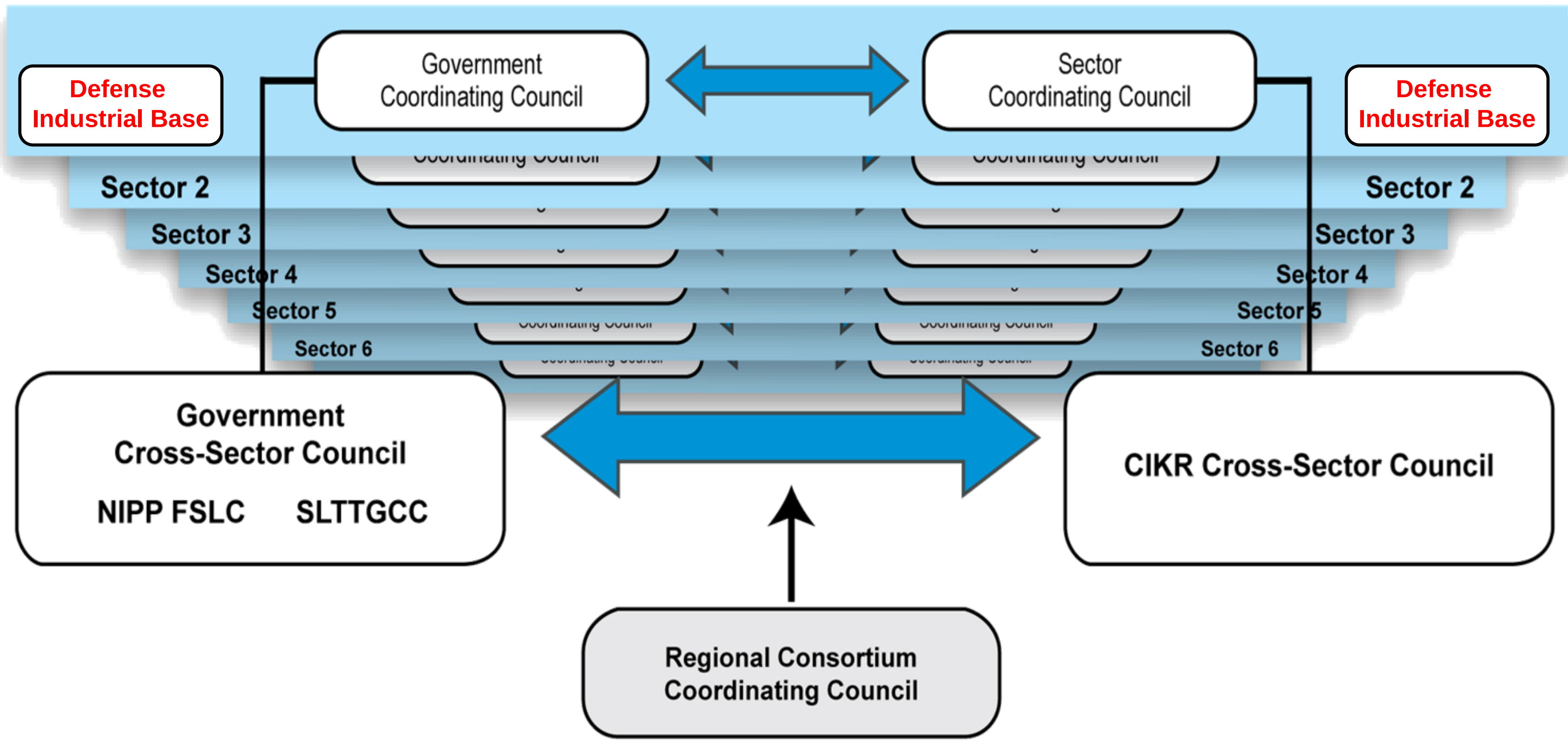
Sector-Specific Agencies

- DHS coordinates the overall national effort under the NIPP
- Sector-specific agencies lead the activities of each sector:
  - Collaborate with relevant stakeholders and develop sector-specific plans
  - Advance vulnerability assessments and encourage risk-management practices
  - Help identify, prioritize, and coordinate infrastructure protection efforts
  - Facilitate the sharing of information and best practices
- DOD Lead is the…
  Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs

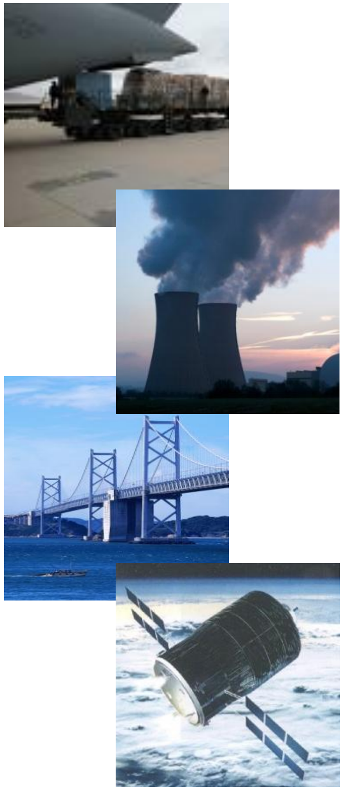
Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration *United States Coast Guard*	Transportation Systems
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

Sector Partnership Model

Protection and resilience are shared responsibilities of Federal, State, and local governments, regional coalitions, and industry as reflected in parallel government and private sector coordinating councils.



Resilience and Risk Management



- Infrastructure Protection and Infrastructure Resilience
  - Infrastructure Protection is the ability to prevent or reduce the effect of an adverse event.
  - Resilience is the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event.
  - Infrastructure Resilience is the ability to reduce the magnitude, impact, or duration of a disruption.

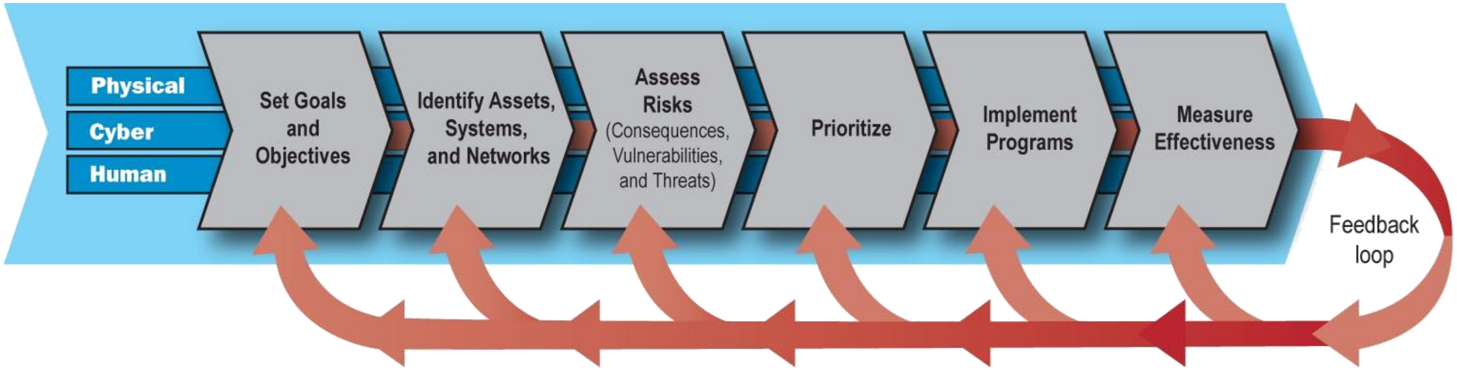
National Infrastructure Advisory Council (NIAC) 2009

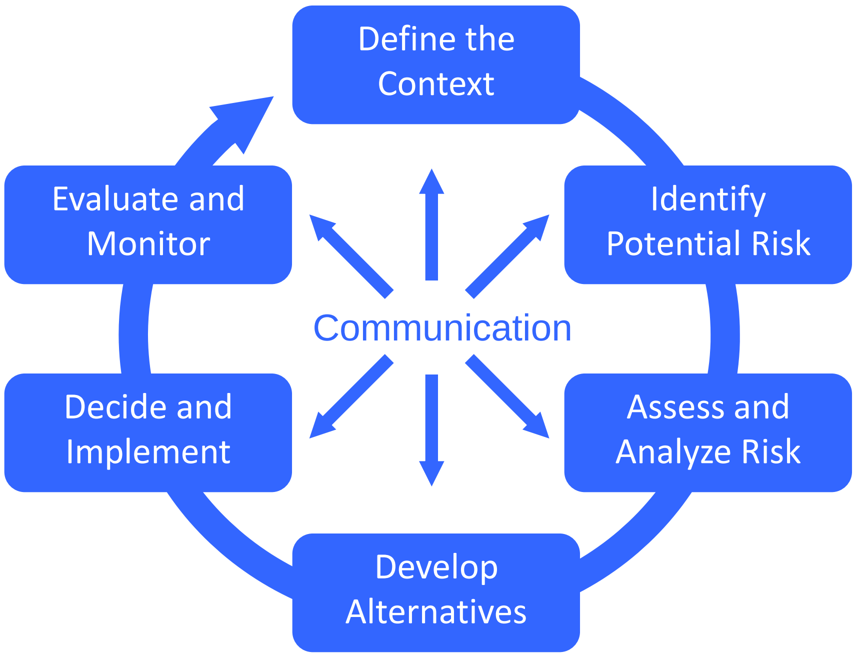
- Risk Management is the…
  - Process for identifying, analyzing, and communicating risk;
  - Accepting, avoiding, transferring, or controlling it to an acceptable level;
  - Considering the associated costs and benefits of any actions taken.

DHS Risk Lexicon, 2010

Risk Management Paradigms

NIPP Risk Management Framework





DHS Risk Management Process

Protecting What Matters

A Case study in Risk Management and Efforts Toward Infrastructure Resilience

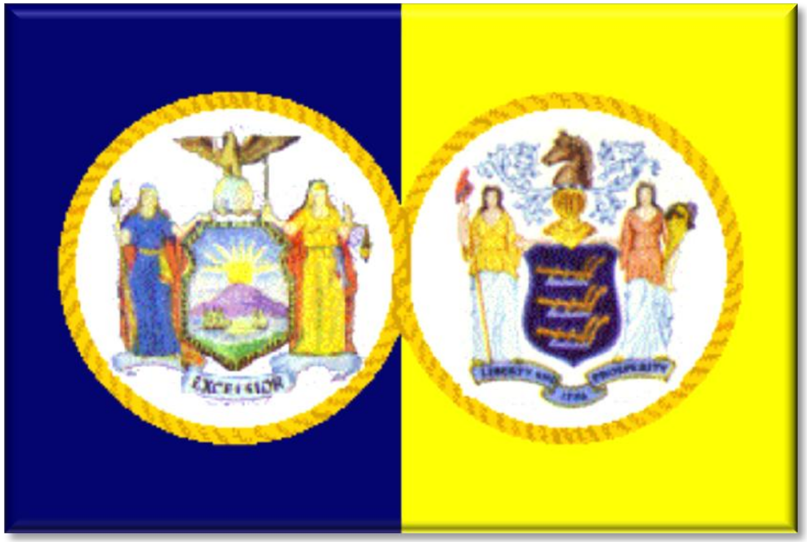
National Defense Industrial Association
Homeland Security Symposium
September 27, 2011

Briefing Outline

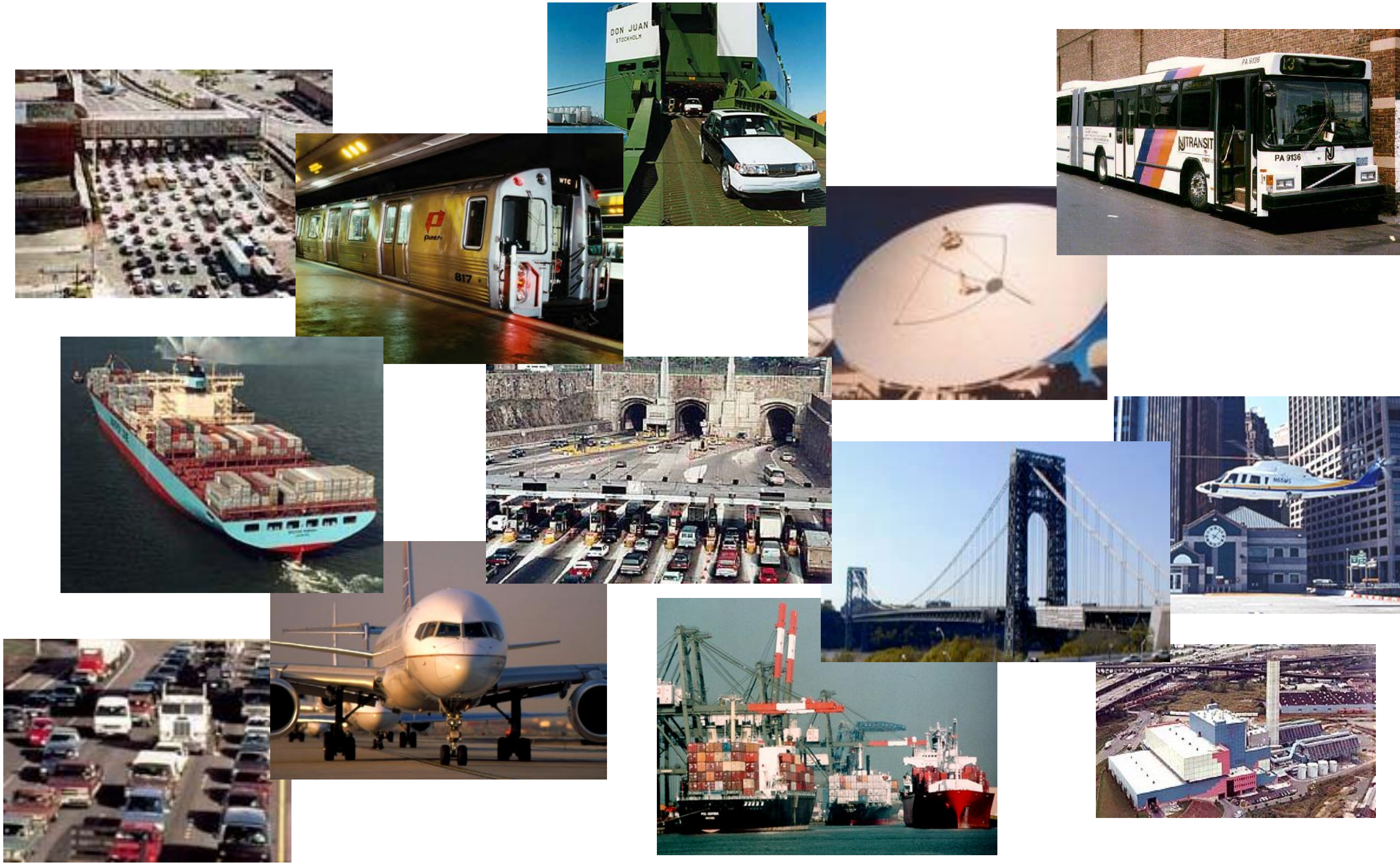
- Case Study Background and the Security Challenge
- Factors Driving the Application of Risk Management
- The Problem and Approach to Evaluating Risk
- Terrorism Risk Assessment and Management Methodology
- Elements of Risk Assessment in the Calculation of Risk
- Presentation of Risk Data for Decision-making
- Cost-benefit Analysis of Mitigation Alternatives
- Some Closing Thoughts

Case Study - Port Authority of NY & NJ

- Bi-state Agency, Formed by Compact in 1921
- Transportation and Development Mission
- Port Region Jurisdiction 1,500 Sq Miles
- Self-supporting from Business Income
- Capital Investment $3.0 billion
- Gross Revenues $3.5 billion
- Net Assets $10 billion
- 7,000 Employees



Facilities for Travel and Commerce



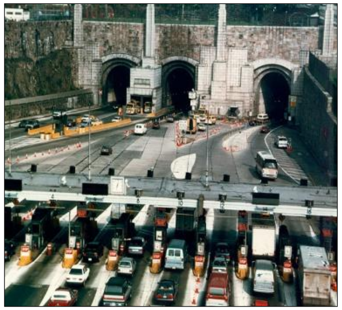
Spanning the Port Region

Scope of Operations

- Tunnels and Bridges (George, Lincoln, Holland, Staten Island)
  - 242 mil trans-Hudson Vehicle Trips
  - 74 mil Bus Passengers, 3.3 mil Bus Movements
- Port Authority Trans-Hudson (PATH - Rail Transit System)
  - 74 mil Rail Transit Riders
- Commercial Airports (Kennedy, Newark, LaGuardia, Stewart)
  - 105 mil Air Passengers
  - 2.3 mil Tons of Air Cargo
- Port Facilities (Newark / Elizabeth, Brooklyn, Staten Island)
  - Serves a 10 State Hinterland; 70 - 80 million People
  - 5.0 mil Containers (TEUs)

Infrastructure Security Challenges

- Complex and Critical Facilities
  - Gateways to Nation, Region, Urban Core
- Public and Varied Environment
  - Moving Almost 500 Million People Per Year
- Identified as High Threat Targets
  - Top of the National Target List
- Need to Balance Security and Mobility
  - Transportation is Essential to Commerce
  - Commerce is the Lifeblood of Democracy



Twice the Target of Terrorist Attacks

Factors Driving Risk Management

- Prior Attack on the World Trade Center in 1993
- Comprehensive Security Audits Post 9/11
- Immediate Operational / Physical Improvements
- Identified Initial $1 Bil in New Security Investment
- Management's Questions Were Predictable:
  - "Do we understand what we are protecting and why?"
  - "Is all that's recommended really needed?"
  - "How do we make choices among competing priorities?"
  - "How will we defend our decisions and tradeoffs?
  - "How will we know if we are returning good value?"

The Problem

- Large Number of Critical Targets
- Impossible to Fully Protect Them All
- Limited Financial and Personnel Resources
- Must Prioritize Needs on Some Rational Basis
- Interdependencies; Potential for Cascading Effects
- Provide for Efficient Use of Scarce Investment Funding
- And Do It Across Targets, Systems, and Business Sectors
- With a Process that is Consistent, Repeatable and Defensible

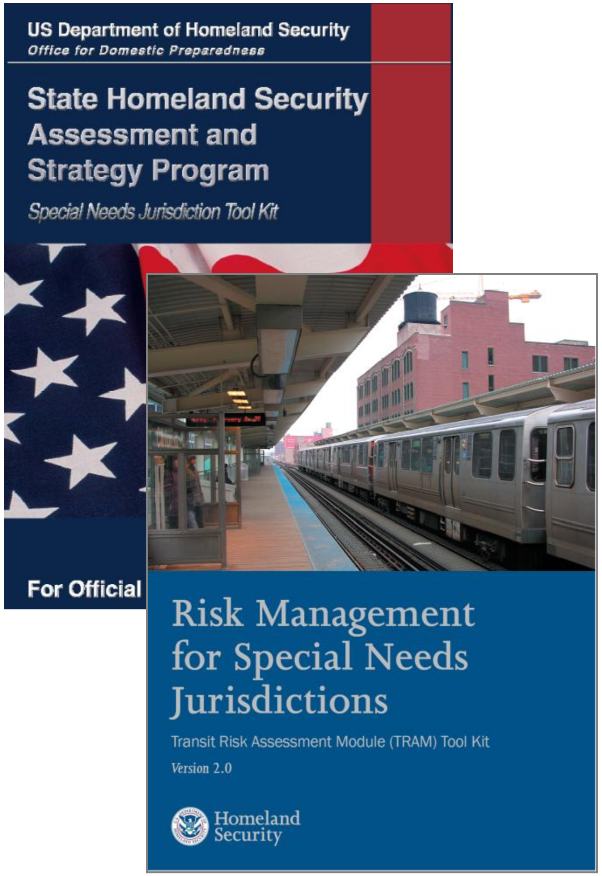
Risk Management Program

- Engaged DOJ Office For Domestic Preparedness
  - To Develop a Security Risk Assessment Methodology
  - Prepare A Risk-based Needs Assessment
  - Continue Refinement of a "Best-practice" Model
- Initial $500 Mil 5-year Security Improvement Program
  - Agency-wide Risk Assessment on a Two-year Cycle
  - Rolling Five-year Security Plans for Each Business Unit
  - Integration into Corporate Planning and Budgeting Cycle
- Continued Investment in Ongoing Security Capital Program

Evolution of TRAM

Terrorism Risk Assessment and Management

- Initial PANYNJ Application
- Base Methodology
- Documented Case Study
- ODP Technical Assistance
- Port and Mass Transit Program
- Standard Attack Scenarios
- Standard Mitigation Measures
- Automated Risk Assessor Tool Kit
- Refined Cost-Benefit Module
- DHS Program Manager - FEMA / NPD



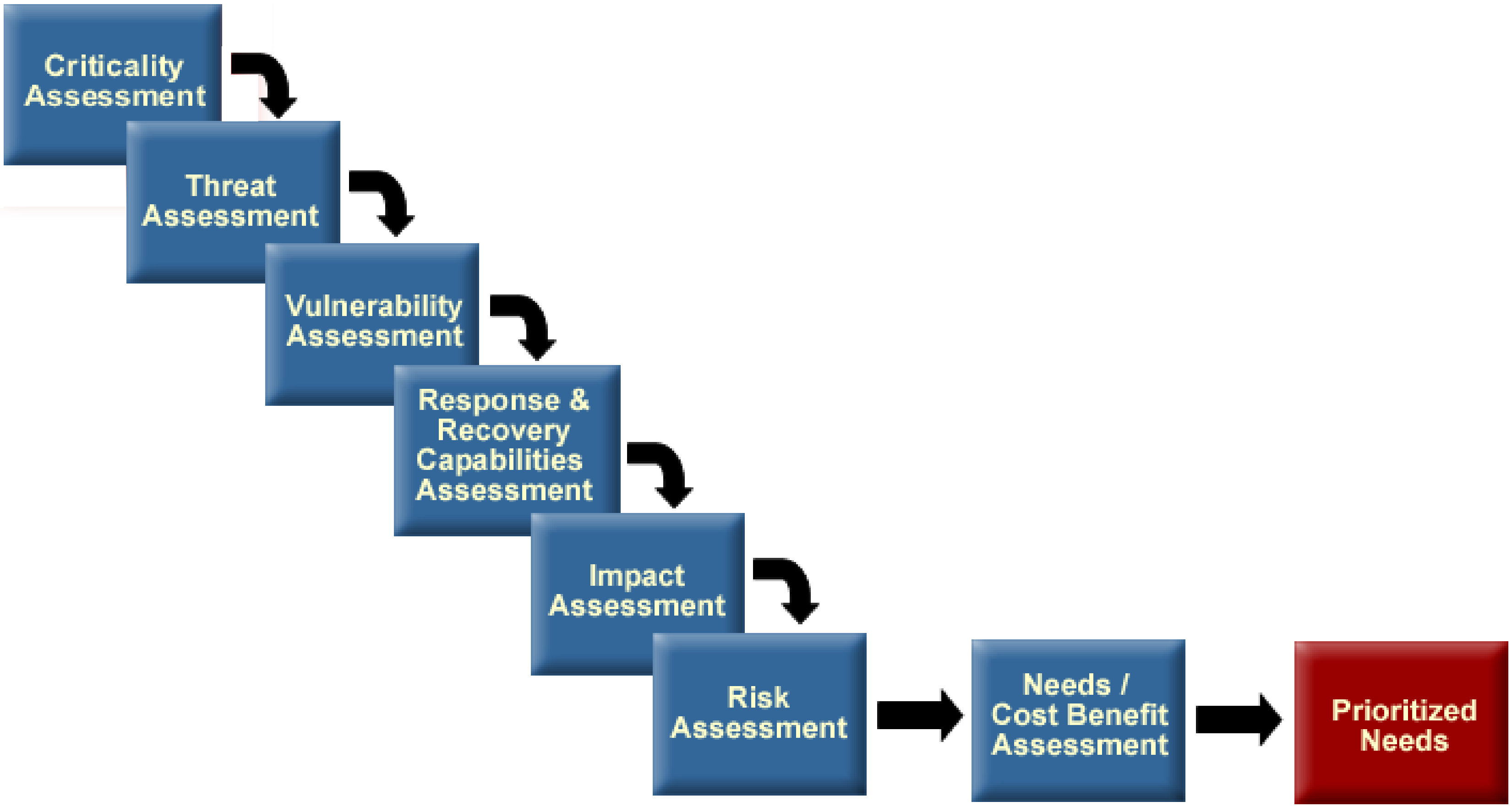
Continuous Improvement

- 1993-2001 Incremental Industrial Security Surveys
- 2002-2003 Initial Agency-wide Security Risk Assessment
- 2004-2005 Risk Update; Cost-Benefit Prototype
- 2006-2007 Complete New Baseline of Security Risk
- 2007-2008 Application of Cost-Benefit Methodology
- 2009-2010 "Multi-Hazards" Risk Assessment Prototype
  - Five Natural / Technical Hazard Scenarios
  - Documentation of the Risk Management Program
  - Standardization of Security and Preparedness Plans
  - Decision Support Tool, Integration with Corporate Processes

Operationalizing Risk Management

- Establish Risk Management Governance Structure
- Identify Risks; Expose Gaps in Security and Response
  - Joint Police / Security / Operations / Engineering Teams
- Formulate Potential Risk Reduction Solutions
  - Develop Set of Project Options for Further Analysis
- Established Risk Mitigation Priorities Based on a Risk Ranking and Relative Risk Reduction Expected
  - Target Projects for Further Cost-Benefit Analysis
- Develop Multi-year Security Plans & Capital Budgets
  - Strict Accountability Via Operating Chain of Command
  - Track Implementation and Reassess Risk

Risk Assessment Process Flow



Risk Assessment Elements

Threat
Likelihood of an Event Occurring

Vulnerability to Attack
Likelihood that Event would Impact Asset

Identify Assets To Be Protected

Likelihood
Likelihood of Event Occurring and Impacting the Asset

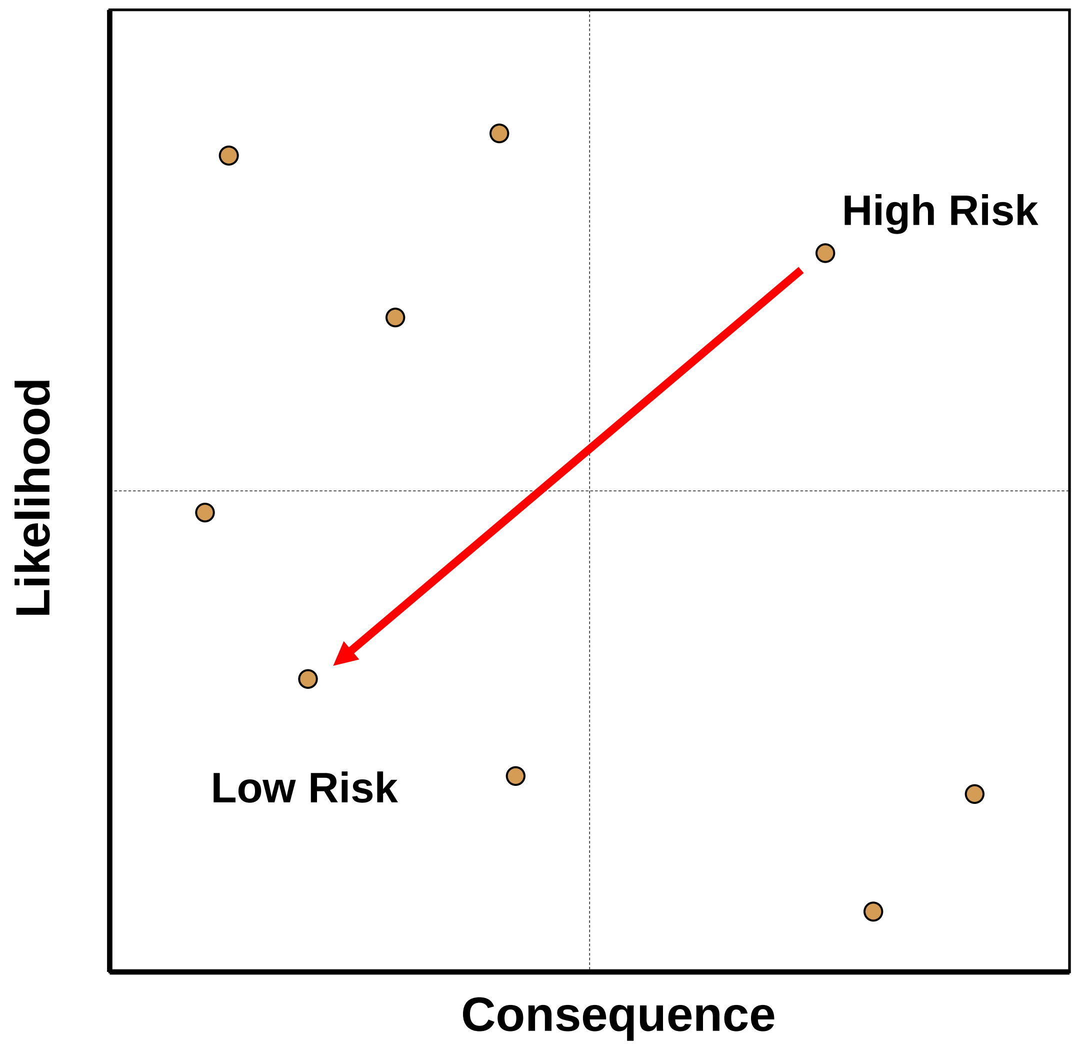
Consequence
Portion of Criticality Eliminated as a Result of the Event

Relative Risk

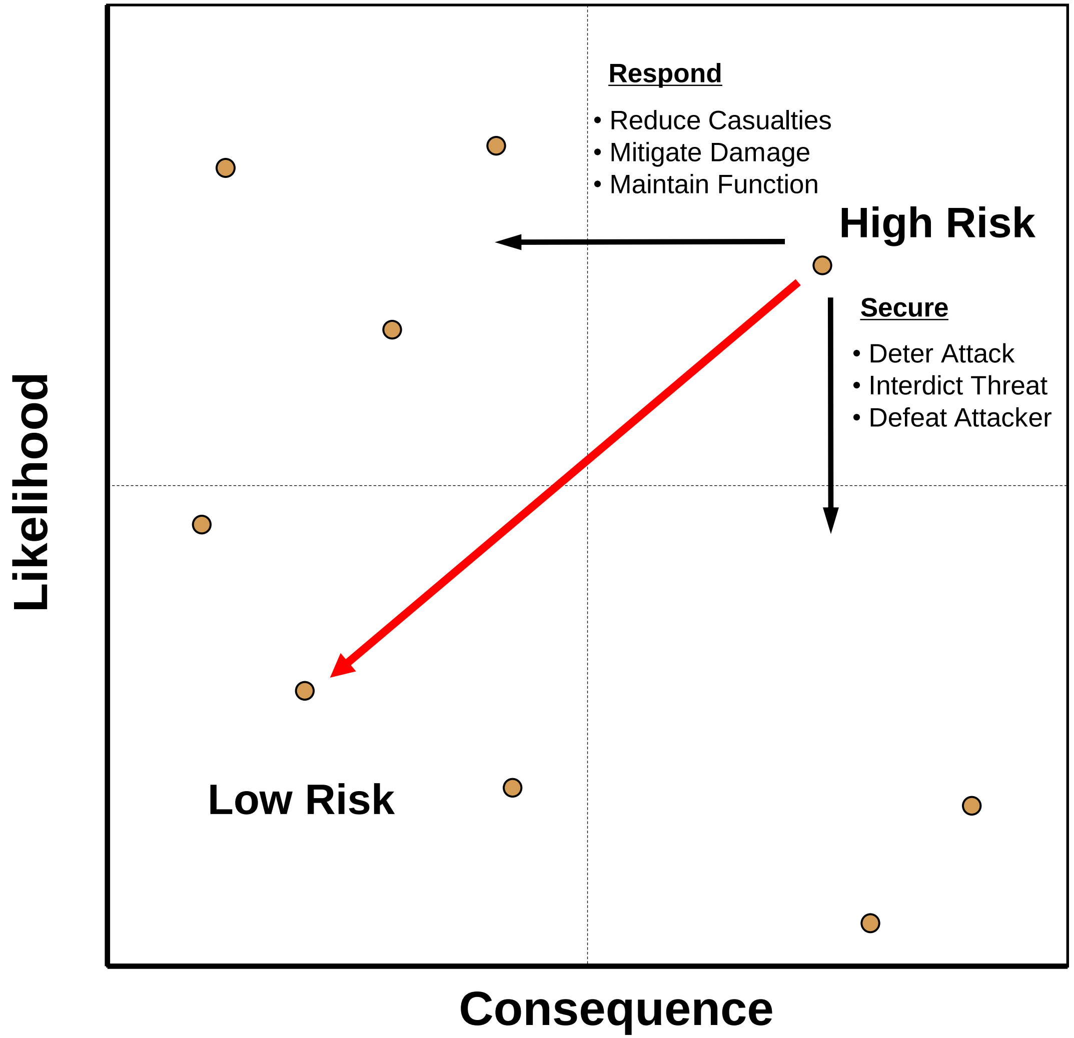
Criticality
Importance of Asset

Overall Impact
Fraction of Asset Criticality Lost

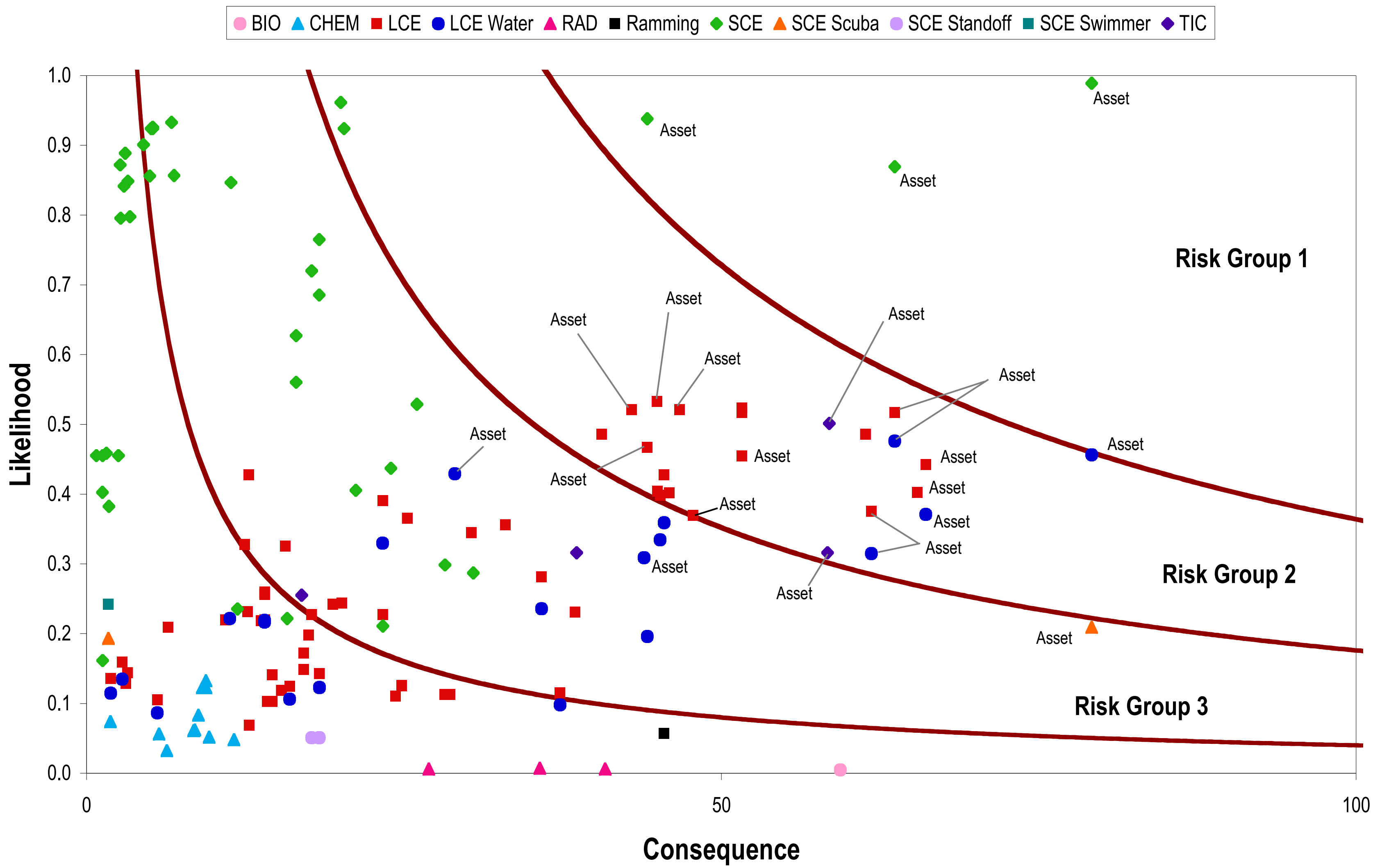
Risk Mapping



Risk Mitigation

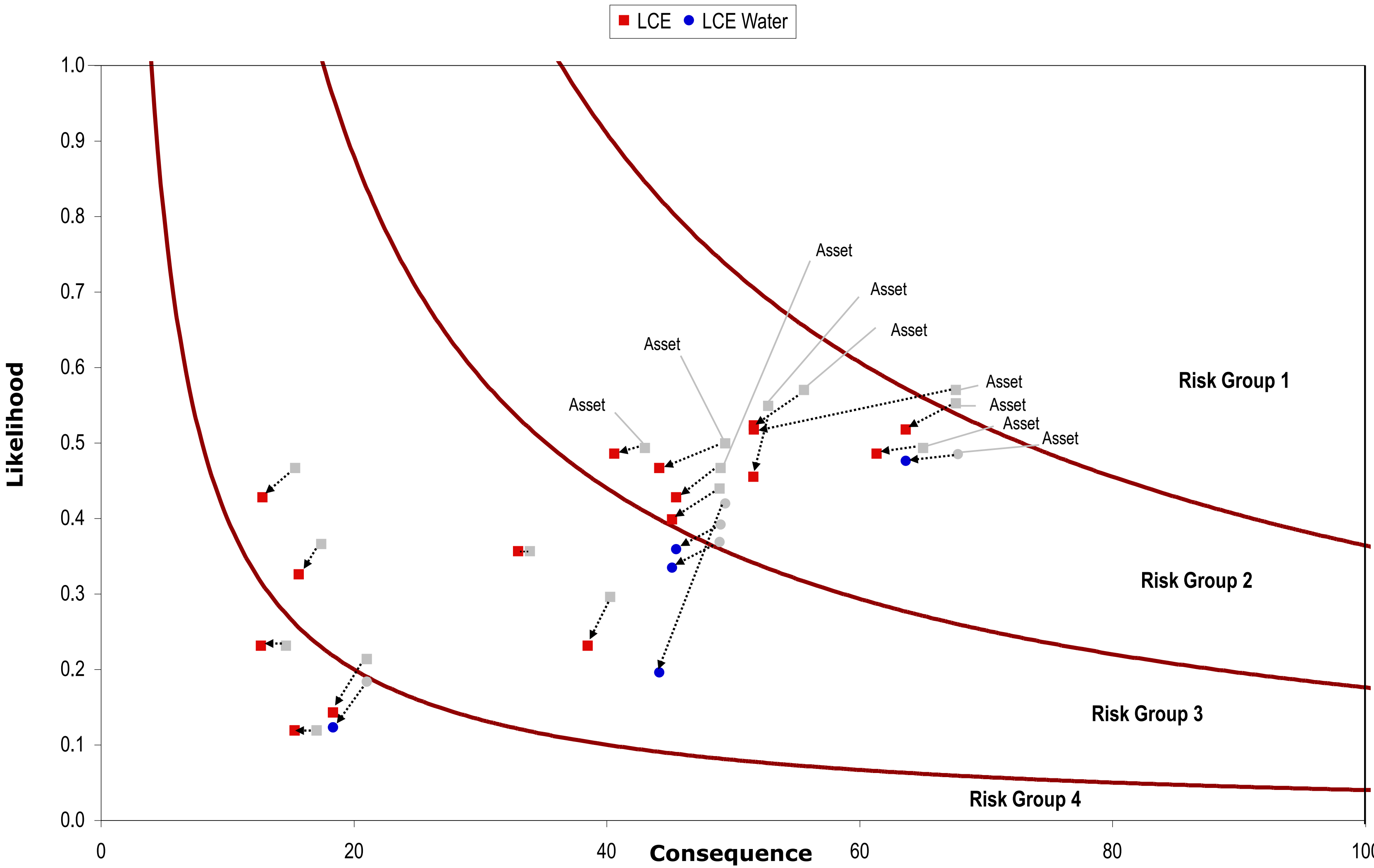


Relative Risk Diagram or Risk Map



Measuring the Buy-Down in Risk

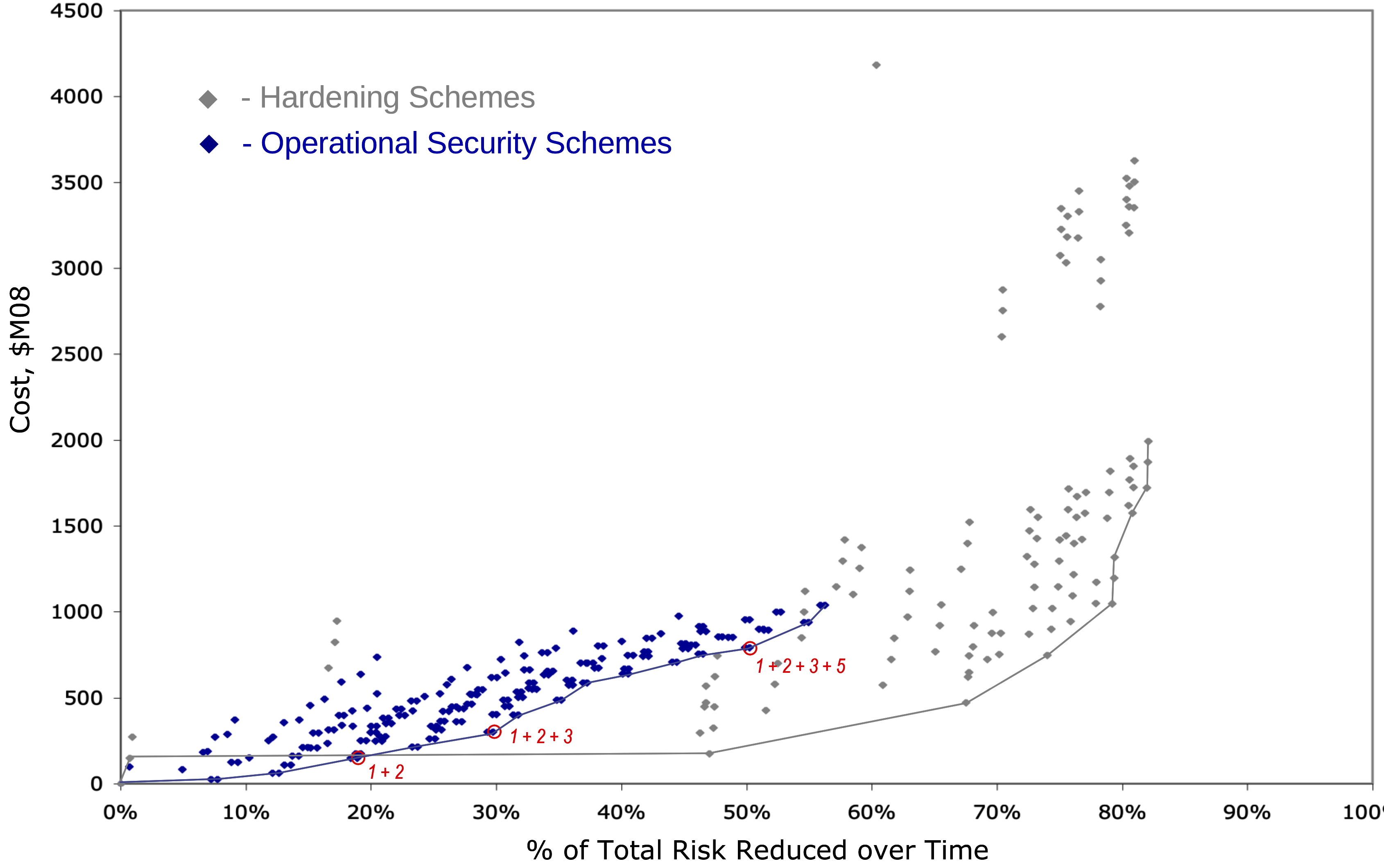
Relative Risk Diagram – For a Bridge, Tunnel or Maritime Facility



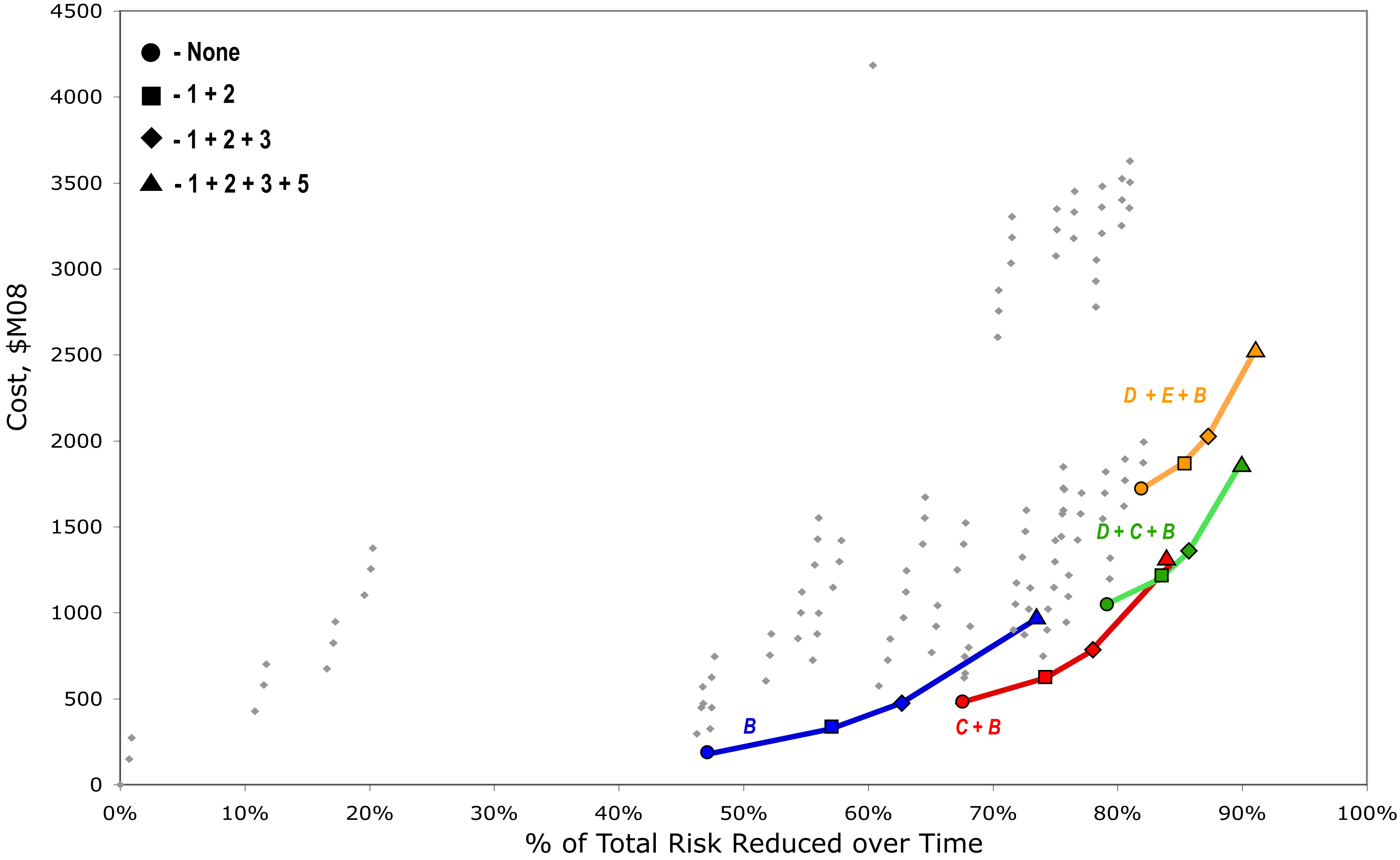
Cost-Benefit Analysis

- Evaluate the Effectiveness of Individual Mitigation Options and Sets of Options In Reducing Risk
- Conduct a Cost-benefit Analysis to Compare Risk Reduction Benefit as a Function of Estimated Costs
- Select a Set of Projects that Result in Maximum Risk Reduction and Greatest Return on Investment (ROI)
- Amend Capital Investment Plan to Accommodate Programming of New Solution Sets
- Reset Strategic Business Unit Spending Plans to Reflect New Expenditures

Array of Alternatives

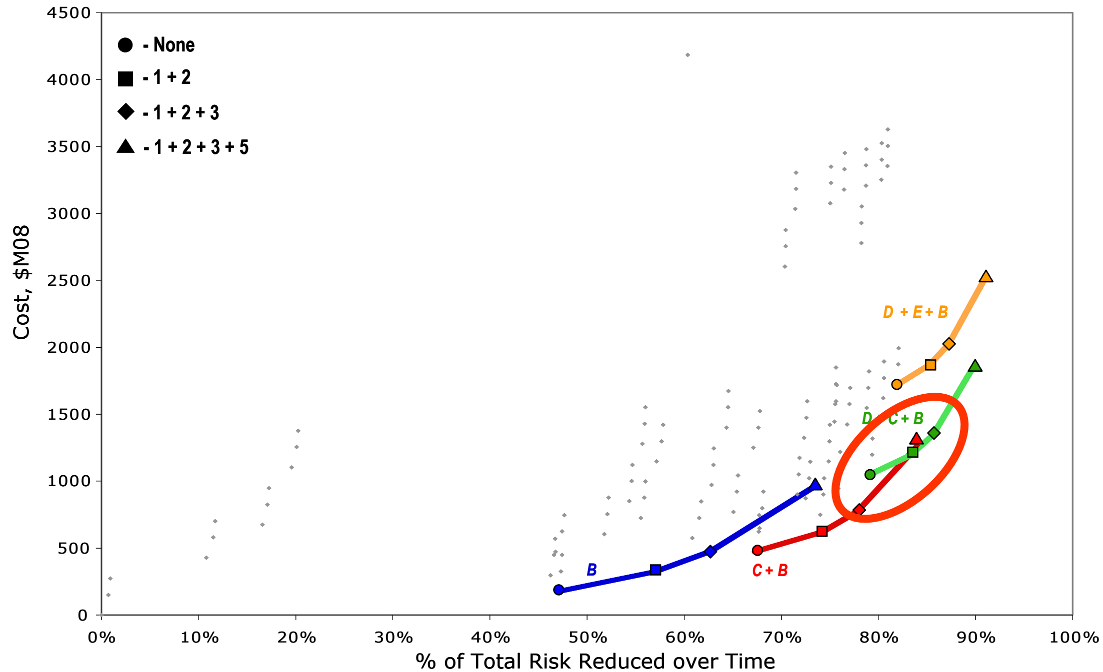


Combined Sets of Alternatives



Risk Tolerance in Decision-making

Frontier Case	Risk Reduction, %	Cost, $M08	Initial Cost, $M08	Recurring Cost, $M08	Marginal Cost per %R Over Previous Option	Probability of Catastrophic Loss
B	47%	$175M	$175M	$0	$3.7M	51%
B / 1 + 2	57%	$324M	$175M	$10M	$15.0M	40%
C + B	67%	$472M	$472M	$0	$14.4M	23%
C + B / 1 + 2	74%	$621M	$472M	$10M	$21.5M	18%
C + B / 1 + 2 + 3	78%	$773M	$472M	$21M	$41.8M	15%
D + C + B / 1 + 2	83%	$1196M	$1047M	$10M	$76.8M	8%
D + C + B / 1 + 2 + 3	86%	$1348M	$1047M	$21M	$66.1M	3%
D + C + B / 1 + 2 + 3 + 5	90%	$1841M	$1047M	$43M	$122.0M	2%
D + E + B / 1 + 2 + 3 + 5	91%	$2516M	$1722M	$43M	$521.0M	1/2%



Overlay Onto DHS Risk Process

Closing Thoughts

- TRAM is a Sound, Well-Documented, Repeatable Process
- Establishes a Consistent Baseline for Security Risk
- Can be Extended Across all Asset Types
- Expansion to Multi-Hazards Risk Appears Promising
- Must Be Complemented with Other Decision Support Tools
- It is Not Perfect But it Doesn't' t Need to Be
- States / Regions at Nexus of Managing Risk
- Solid Model for State / Regional Risk Management
- Could Provide a Viable Option for DIB Sector Risk Management

References

- Homeland Security Presidential Directive (HSPD) 7: Critical Infrastructure Identification, Prioritization, and Protection www.dhs.gov/xabout/laws/gc_1214597989952.shtm
- DHS National Infrastructure Protection Plan 2009 www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
- DHS Office of Risk Management and Analysis: Risk Management Fundamentals www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf
- DoD Directive 3020.40: DoD Policy and Responsibilities for Critical Infrastructure www.dtic.mil/whs/directives/corres/pdf/302040p.pdf
- DoD Instruction 3020.45: Defense Critical Infrastructure Program (DCIP) Management www.dtic.mil/whs/directives/corres/pdf/302045p.pdf
- NIAC Study - Critical Infrastructure Resilience 2009 www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf
- HIS Study - Concept Development: An Operational Framework For Resilience 2009 www.homelandsecurity.org/hsireports/Resilience_Task_09-01.pdf
- HIS Study - Risk and Resilience: Exploring the Relationship 2010 www.homelandsecurity.org/hsireports/Risk-Resilience_Report_Final_public_release_version_Task_10-17_29-Nov-2010.pdf
- The George Washington University – Homeland Security Policy Institute www.gwumc.edu/hspi/policy/taskforce_resilience.cfm

Contact Information

John Paczkowski
Vice President, ICF International
Office: 703-934-3717
Mobile: 703-789-3480
E-Mail: jpaczkowski@icfi.com

Lisa Bendixen
Vice President, ICF International
Office: 703-934-3114
Mobile: 508-740-0834
E-Mail: lbendixen@icfi.com

For Information on the NIPP E-mail: nipp@dhs.gov