

Transportation and Security

Robert E. Gallamore

*The Transportation Center
Northwestern University*

Transportation Research Forum

Annual Meeting

March 7, 2005



The New Challenge for Transportation – Security

- **Understanding Threats and Vulnerabilities**
 - Intelligence: Getting It and Sharing It
 - Facilities Protection –Gates, Guards, & Guns
 - Cyber Security
- **Aviation Security – the Most Visible Part of DHS**
- **Special Problem of Container Security**
- **Who Pays?**

THE
9/11
COMMISSION
REPORT

FINAL REPORT OF THE NATIONAL COMMISSION ON
TERRORIST ATTACKS UPON THE UNITED STATES



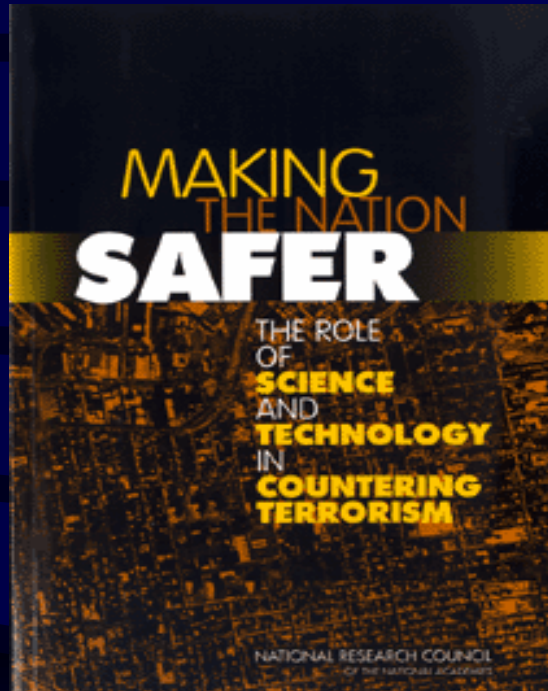
AUTHORIZED EDITION

9/11 Commission: Four Kinds of Failures

- *Imagination*
 - Problem of Cultural Asymmetry
 - Understanding Commercial Aircraft Could Be a WMD
- *Policy*
 - Underestimating the Threat
 - Richard Clarke's Warnings Incisive, but . . .
- *Capabilities*
 - Trapped in Institutions of the Cold War
 - Weaknesses of Domestic Agencies – FBI, INS, FAA
- *Management*
 - Missed Opportunities to Thwart 9/11
 - Info Not Shared, Analysis Not Pooled

“No one looked behind the curtain.”

National Academies Committee on Science and Technology to Counter Terrorism



Transportation Panel

Mortimer L. Downey, Chairman

Transportation Research Board

Study Focus

- Catastrophic Terrorism
- Combination of Likelihood and Severity

Catastrophic Threats

- Weapons of Mass Destruction
- Cyber Attacks
- Disruption as well as Destruction

GENERAL STRATEGIES AND RESEARCH NEEDS

- **Nuclear** Control weapons & materials at source
- **Biological** Research, prepare, distribute responses
- **Chemical/Explosives** Sensors & filters
- **Info Technology** Network security/ER communications
- **Energy** SCADA controls/adaptive grid/vulnerabilities
- **Cities/Infrastructure** Emergency responder support
- **Transportation** Layered system security
- **People** Trusted spokespersons
- **Complex Systems** Data fusion/data mining/red-teaming
- **Cross-Cutting Tech** Sensors/robots/SCADAs/systems analysis
- **Deployment** Homeland Security Institute, Partnerships among feds/states/locals/universities

TRANSPORTATION SYSTEM

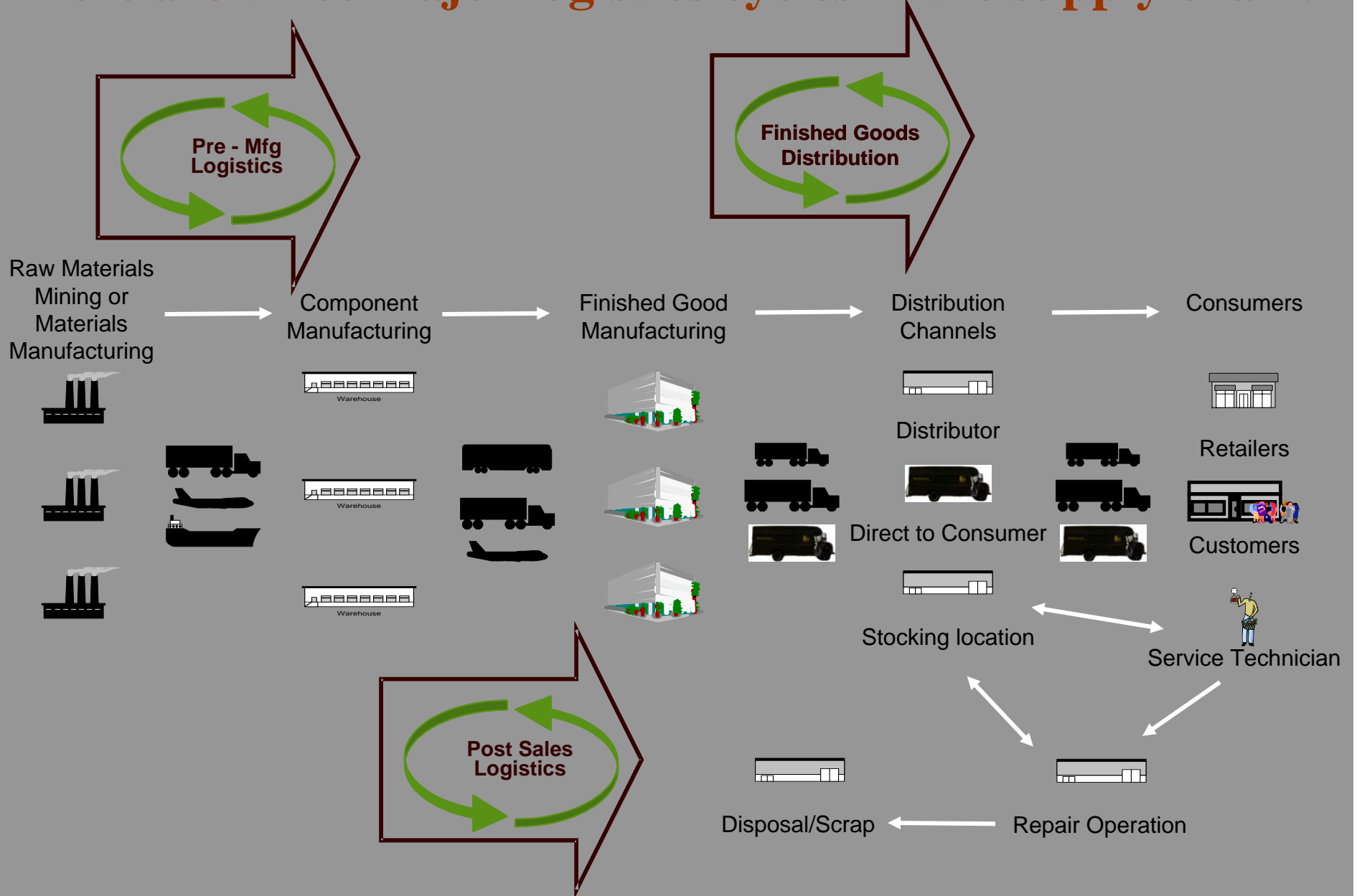
- Open and accessible—by design
- Extensive and ubiquitous
- Diverse and institutionally divided
- Global linkages to society and the economy
- Transport as target and weapon

• “Logistics Revolution” = Take Out Inventory & Redundant Facilities

Freight Industry Characteristics

- Scale and Complexity of the Transport Networks
 - Diversity of Modes and Providers
 - Range of Operations
 - Multiple Points of Interconnection
 - Both Fixed Facilities and Vehicles
- Information Systems Complexity
 - Increased Dependency on Vulnerable Systems
 - Difficulty of Authenticating Users
- Public-Private Interactions
 - Multiple Security Agencies Requiring Coordination

There are three major logistics cycles in the supply chain.



COUNTER-TERRORISM ACTIONS

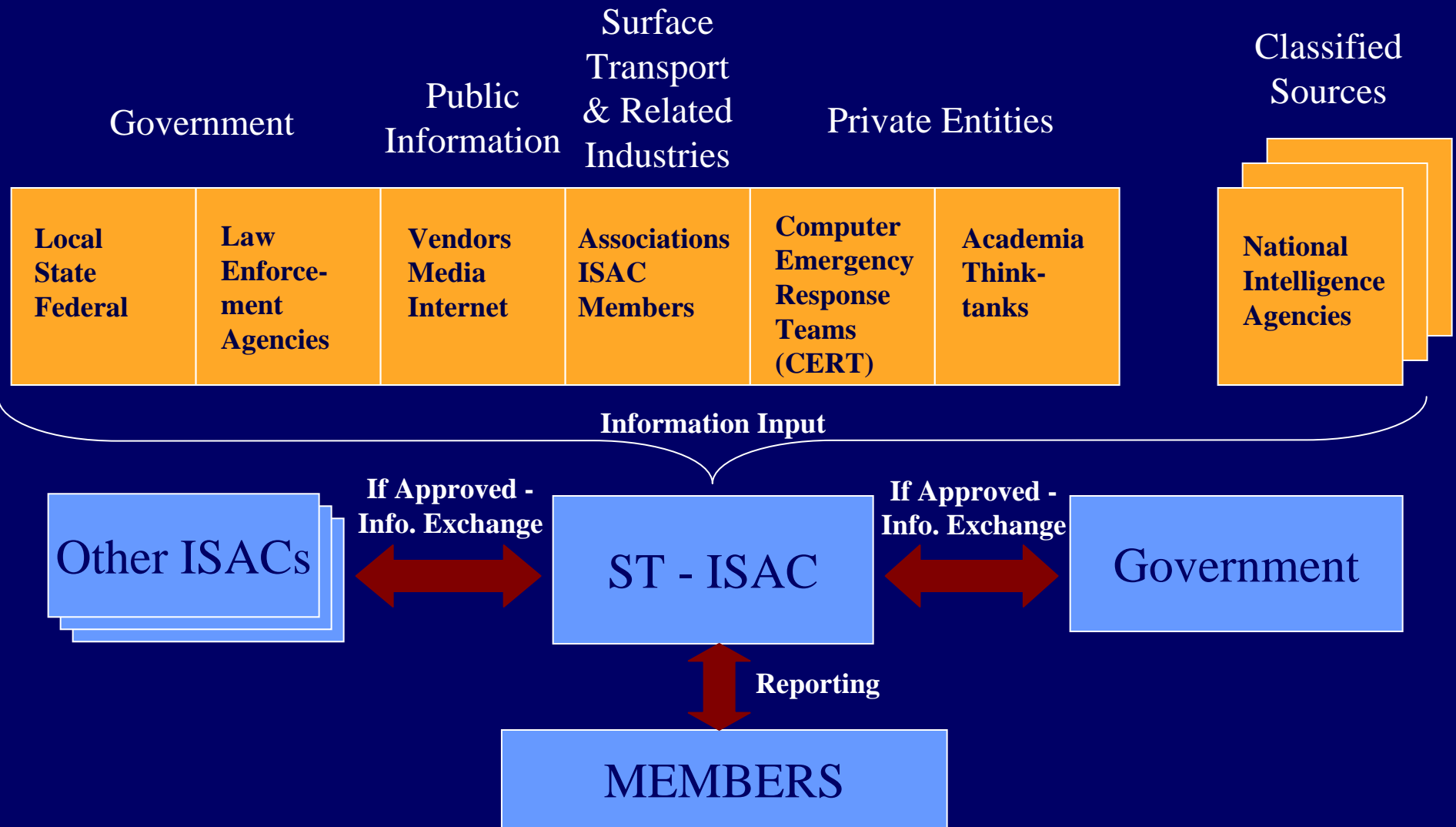
- **Predict:** Intelligence and surveillance of targets and means
- **Prioritize:** *Use risk management techniques to rank and fund counter-measures*
- **Prevent:** Disrupt networks, contain threats
- **Protect:** Harden targets, immunize populations
- **Interdict:** Frustrate attacks, manage crisis
- **Response & Recover:** Evacuate, **re-route traffic**, mitigate damage, expedite cleanup
- **Attribute:** Identify attacker to facilitate response

OPTIMUM SECURITY SYSTEMS

- Technologically sophisticated, yet operationally feasible
- Layered—multi path, multi challenge to terrorist
- “Curtains of Mystery”
- Go beyond “gates, guards, and guns”
- Take account of economic consequences of both the terrorist action and counter-measure

Must make difficult trade-offs based on risk analysis, cost, and benefit of specific strategies for countering terrorist plots.

The Information Sharing Challenge



THE AVIATION SYSTEM

- High visibility even if not highest risk – passenger screening has received disproportionate funding and attention
- Steps to improve layering are underway
 - Access Controls
 - Better Screening and Sensors
 - Coordination/Systems Approach
- Better information integration can improve performance
 - Trusted shippers/travelers
 - CAPPS for screening selection
 - Human factors tools useful for supporting screeners
- [Some] Hardening still required

THE INTERMODAL CONTAINER SYSTEM

- Excellent delivery system for international and domestic cargo—including terrorists and WMDs
- Current security is essentially perimeter-based, 2%-3% inspection
- Future needs to be collaborative among carriers, shippers, and security forces

PUBLIC TRANSIT SYSTEMS

- Open system—difficult access control for public spaces
- Key needs—situational awareness, sensor development, operational planning
- System recovery and cleanup capacity
- Long run: Better station designs and system redundancy

OTHER TRANSPORTATION MODES

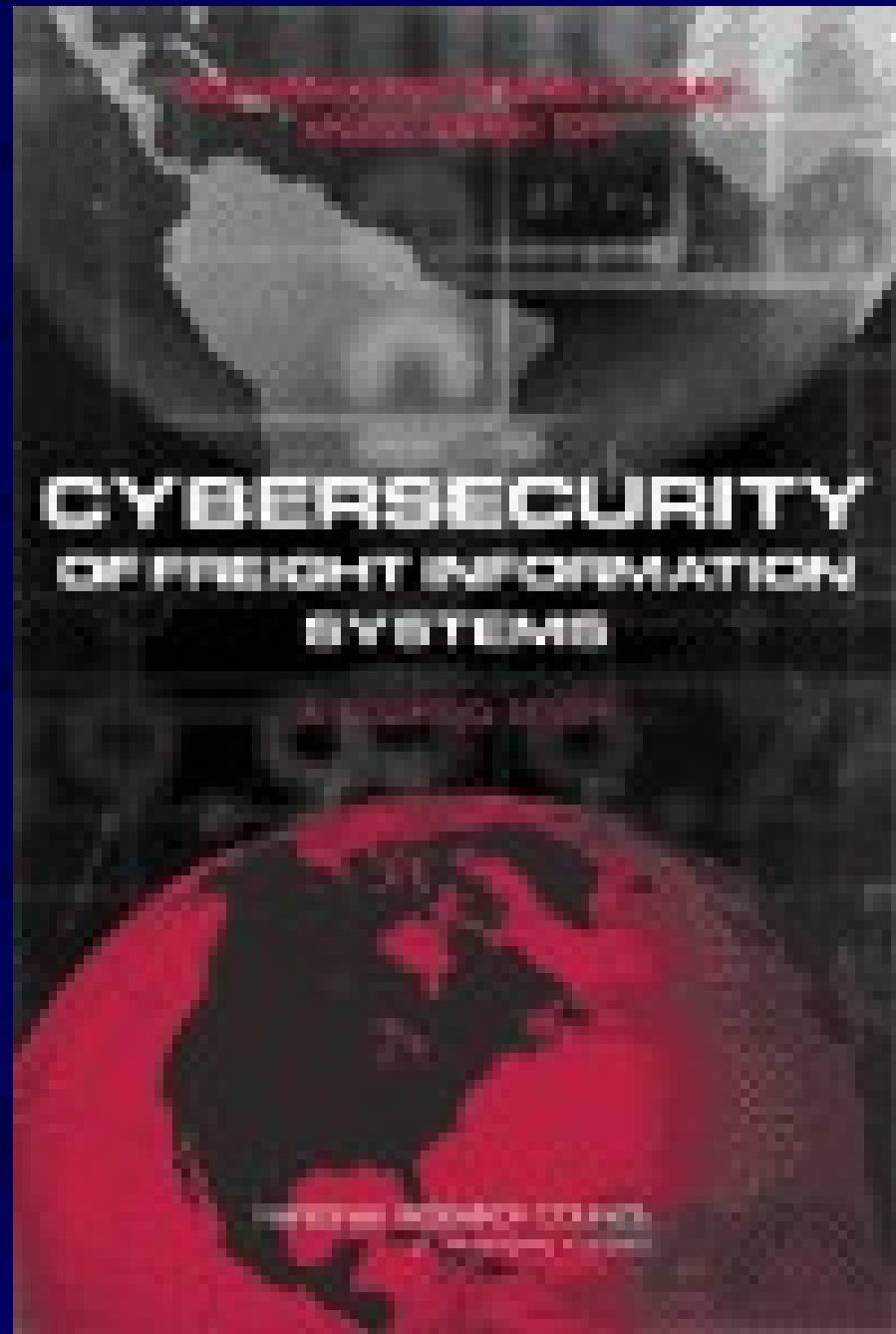
- Hazardous Materials Shipments –
 - Truck and Rail
 - Barges
 - Pipelines
 - LNG Imports
- Cyberthreats to SCADA systems

RESEARCH NEEDS

- **Technology**—faster, better, cheaper, smaller, usable in the real world
- **Systems Approach**—understand how the system works—design security in
- **Human Factors**—recognize that even perfect systems are run by imperfect people
- **Unconventional Thinking**—what is in the terrorist's mind? How do we stay ahead?

***TRB
SPECIAL
REPORT 274***

**Robert E. Gallamore, Chair
The Transportation Center at
Northwestern University**



IT Trends and Emerging Technologies

- Electronic Supply Chain Manifesting
- Real-Time Monitoring
- Decentralized System Architecture
- Embedded Processors
- Electronic Data Interchange
- Increased Reliance on the Internet
- Global Interconnection of Systems
 - Firewalls – Access Controls
 - Problems of User Authentication

Risk is new IT applications make transport / logistics more vulnerable to terrorist acts – even from far away.

Embedded Processors and Enabling Technologies

- Direct Transfer between Real and Cyber Worlds – Untouched by Human Hands
- RFID Tags, Active and Passive
- E-Sensors
- Smart Seals

Controversial Area: Standards, Info Security, Cost Burden

Committee Recommendations for DHS / TSA Transportation Cyber-Security Analysis

- Task 1. Determine Vulnerabilities in Freight IT Systems
 - Existing & Evolving Systems
 - Prioritization by Risk (Probability * Consequences)
 - Plus Cost & Operational Impact of Implementation
- Task 2. Review Current Practices for IT Security
- Task 3. Determine Potential for IT Security Enhancements in Transport and Logistics Sector
- Task 4. Analyze Policies to Reduce Cyber-Vulnerabilities
- Task 5. Assess Economic Impact of Cost Penalties Imposed on Freight Transport

The New Challenge for Transportation – Security

- Understanding the Threats and Our Vulnerabilities
 - Intelligence: Getting It and Sharing It
 - Facilities Protection –Gates, Guards, & Guns
 - Cyber Security
- Aviation Security – the Most Visible Part of DHS
- The Special Problem of Container Security
- Who Pays?

The New Challenge for Transportation – Security

- Understanding the Threats and Our Vulnerabilities
 - Intelligence: Getting It and Sharing It
 - Facilities Protection –Gates, Guards, & Guns
 - Cyber Security
 - Aviation Security – the Most Visible Part of DHS
 - The Special Problem of Container Security
- Who Pays?

Some Economic Issues

- What Is the Effect of Security Investments on Economic Outputs?
- Can Thin Margins in Transport Support Additional Security Mandates if Privately Borne?
- When Does Security Cost Become a Concern?
- What Form of Public Participation in Security Costs Would Be Most Effective (e.g. Tax Credits)?

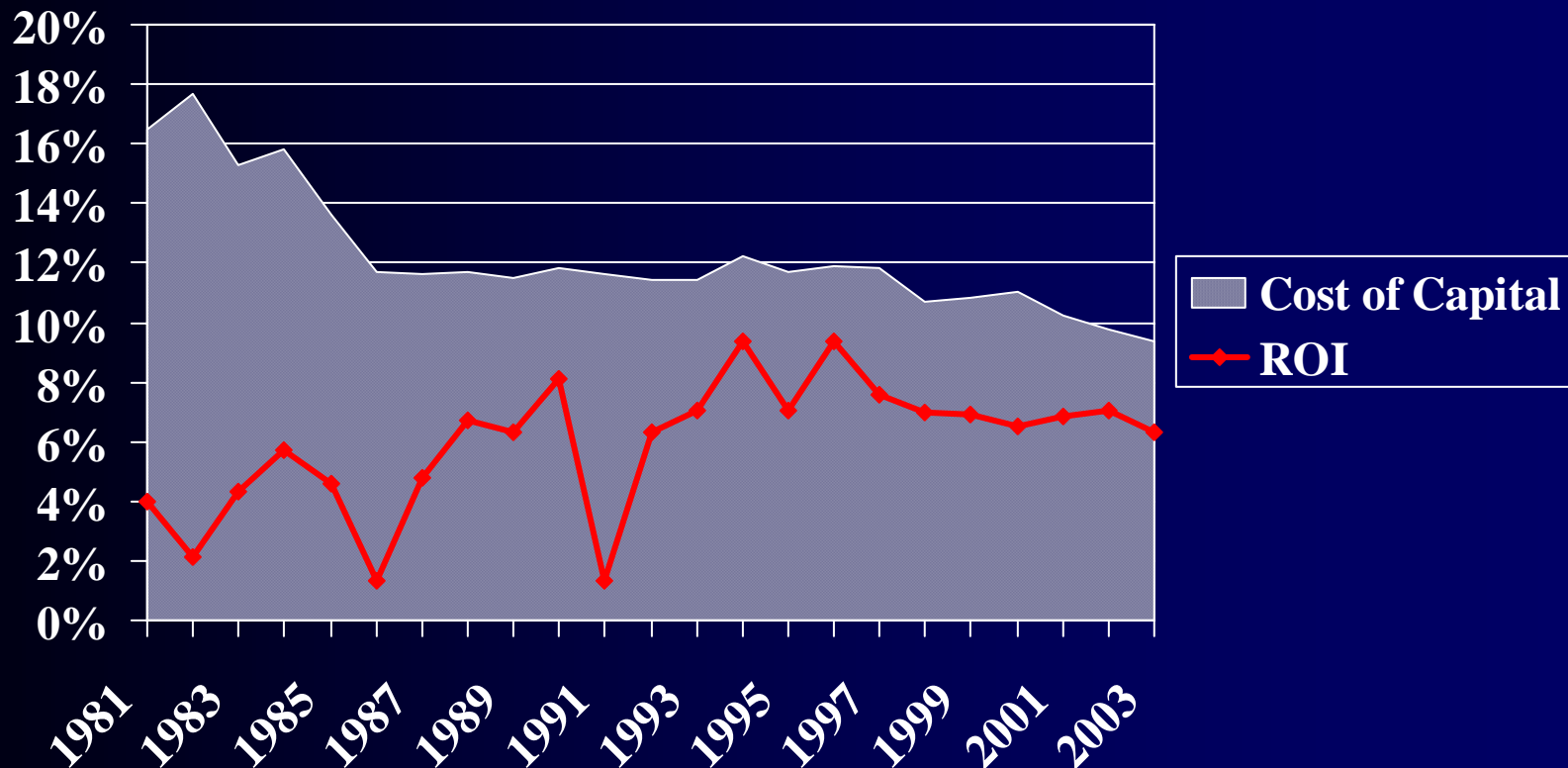
Can We Afford to Reinvest in Transportation?

- **Can We Not?!**
 - Total Logistics Portion of GDP = **10%**
 - About \$1,000,000,000,000 (\$One Trillion) Annually
 - Transportation = 19% of Consumers' Expenditures
- **Traffic Cyclical but Trend Steadily Up**
- **Carriers Largely Used Up Excess Capacity**
 - Railroads & Intermodal Facilities – Access to Ports
 - Interstates, Urban Arterials – 52% of Urban Interstates Congested (1995)
 - Inland Waterways – e.g. Ohio River
 - Pipelines to Some Regions – e.g. Nashville and Chicago

Financing Future Capacity

- Private Firms Need Adequate Returns for Reinvestment
- Public Policy Needs to be Fair and Flexible
 - Avoid Market Distortions
 - Allow States and Regions to Influence Choices
- Public Incentives for R&D, Security, Environment, Energy Technology

Class I Railroads: Cost of Capital Exceeds Return on Investment

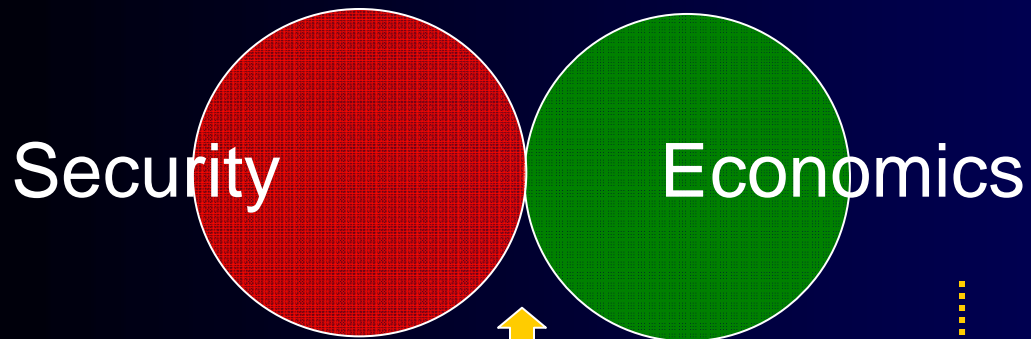


Source Data Courtesy of the Association of American Railroads

Summary: Solutions Going Forward for Transportation with Security

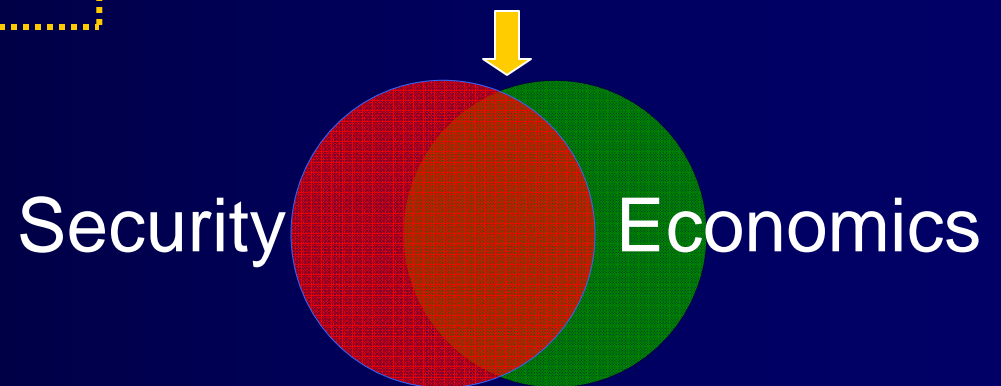
- Improve Private Carrier ROI to Enable Reinvestment and Service Improvement – (Surge/Slack Capacity Trade-offs)
- Promote Intermodal Service Alternatives
 - Make the Best Use of Available Modal Capacity
 - Reauthorize and Fund Flexible Public Intermodal Infrastructure Program – Focus on Connections and Hubs
 - Develop Genuine Public Private Partnerships
- Invest in Technology – Intelligent Systems
- Public Financing for Anti-Terrorism Measures
 - Hardening of Key Physical Facilities (e.g. Control Centers)
 - Cyber Security Measures, Including ST-ISAC Support
 - Container Security Initiatives (Operation Safe Container, Monitoring, etc.)

Is There Synergy Between Transport Economics and Security Outlays?



No Economic Benefit to Security Enhancements

Significant Economic Benefit to Security Enhancements



Thank You

Robert E. Gallamore

r-gallamore@northwestern.edu

(847) 491-7286