



**INTEGRATING *iCONTAINERs* WITH EXISTING  
SHIPPING AND LAW ENFORCEMENT  
INFRASTRUCTURE**

---

**Dale Ferriere**

National Infrastructure Institute  
Center for Infrastructure Expertise

**Khrystyna Pysareva**

University of New Hampshire

**Andrzej Rucinski**

University of New Hampshire



UNIVERSITY of NEW HAMPSHIRE

May 2006



# PROBLEM STATEMENT

- 1) Who will own, operate and maintain “intelligent container” technology?
- 2) Who is responsible for monitoring “intelligent container” raw data and for notifying first responders about cargo container anomalies?
- 3) What communication technologies are currently used by first responders and maybe adopted for “intelligent container” data transmission?
- 4) How will existing cargo manifest data be integrated into “intelligent container” data?

**IDENTIFY** “intelligent container” technology ownership, maintenance & operations ‘best practices’.



## Problem Statement (continued)

### Re: *iContainer* Interoperability

If a containerized cargo supply chain's interoperability is to be used as a weapon, then to defend against it are law enforcement's and first responder's interoperability equally well defined?



## APPROACH

Query *key representatives* from the international maritime container shipping industry, the domestic US land-based inter-modal transportation industry, government regulators & first responders.

### *Qualitative Approach: 18 motivated & informed participants*

- First Responders – 5 representatives
- Government/Regulatory – 5 representatives
- Canada / U.S. Northeastern Ports – 5 representatives
- Supply-Chain Industry – 3 representatives



# QUERY STRUCTURE

## Section I: Part I: Container ownership and supply-chain operation “best practices”

- **Scenario A:** Container-owner (carriers / shippers) owns/operates “intelligent” container technology.
- **Scenario B:** Government owns/operates “intelligent” container technology.
- **Scenario C:** Importer owns/operates “intelligent” container technology.
- **Scenario D:** Third party owns/operates “intelligent” container technology.
- **Scenario E:** Combination of the above.



## QUERY STRUCTURE (continued)

### Section I: Part II:

“Build your own scenario”

- Introduction
- Communication and interoperability questionnaire
- Recommendations



# QUERY STRUCTURE

## “build your own” (sample)

Q1: Black box (intelligent container) is owned/purchased by:  
 a. Container owner;  
 b. Government/law enforcement;  
 c. Importer;  
 d. Shipping Line.

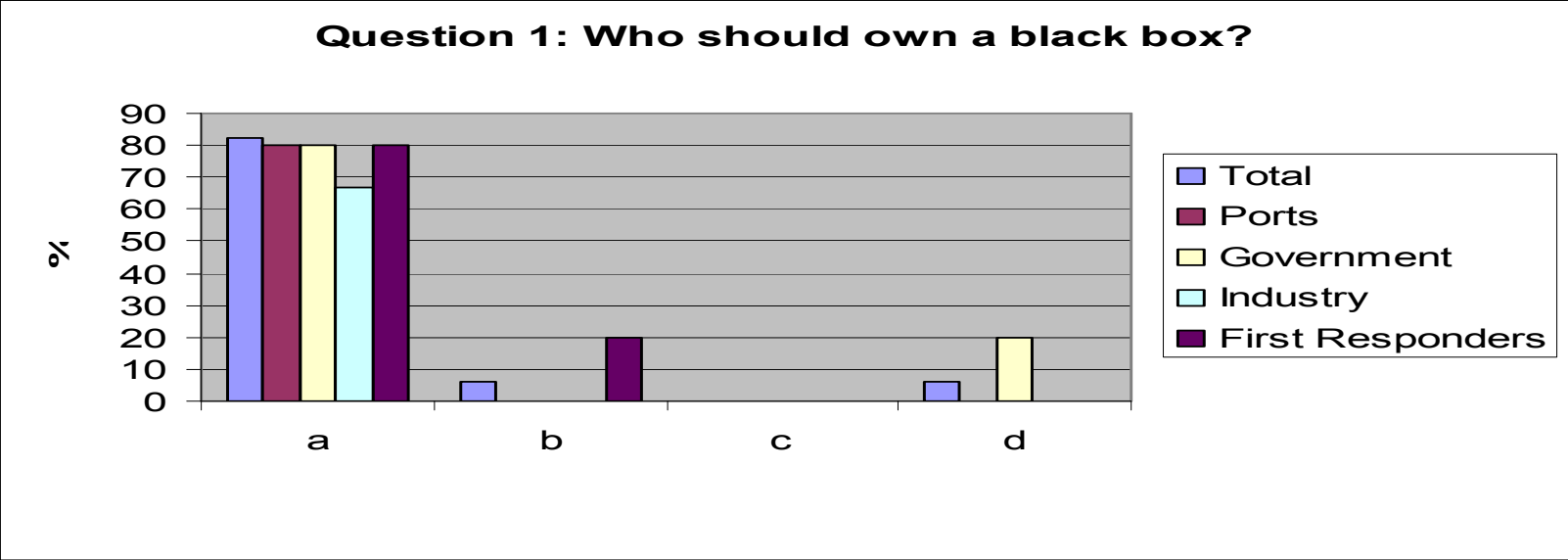
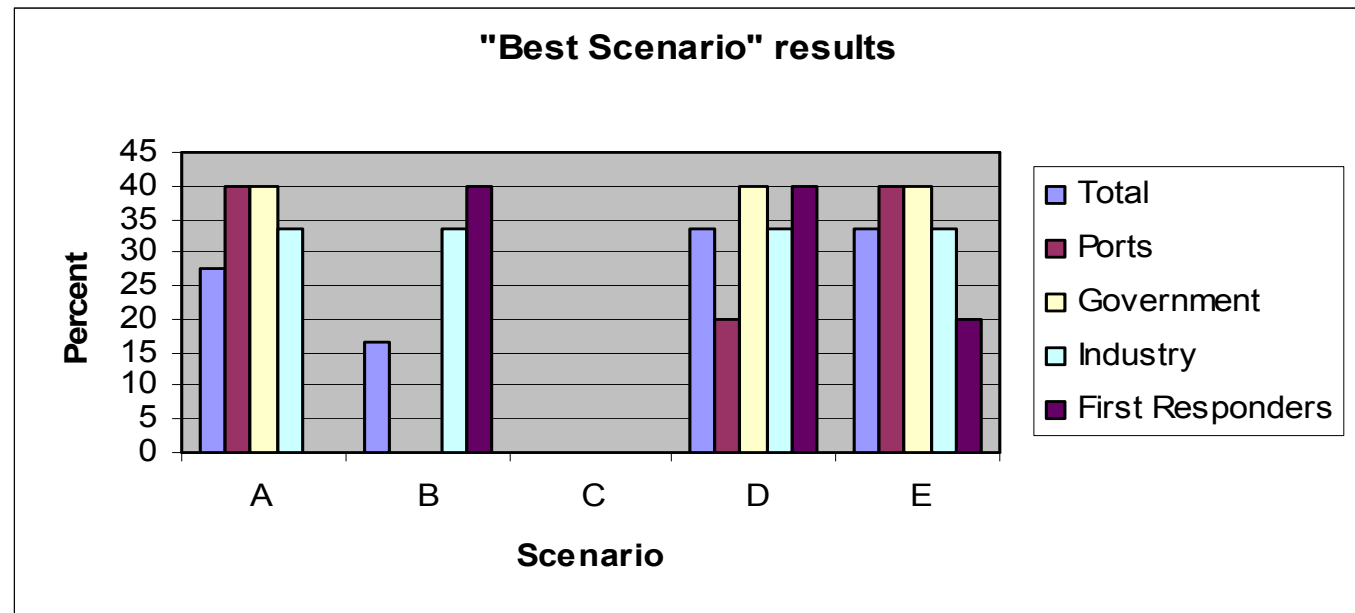


Figure 7. Question 1 results  
 Most surveyed chose a container owner as the party purchasing and owning a container black box. Multiple times the surveyed suggested introducing another option: a third party purchases and owns the black box.

# Container ownership and operation

## “best practices – best scenario results”



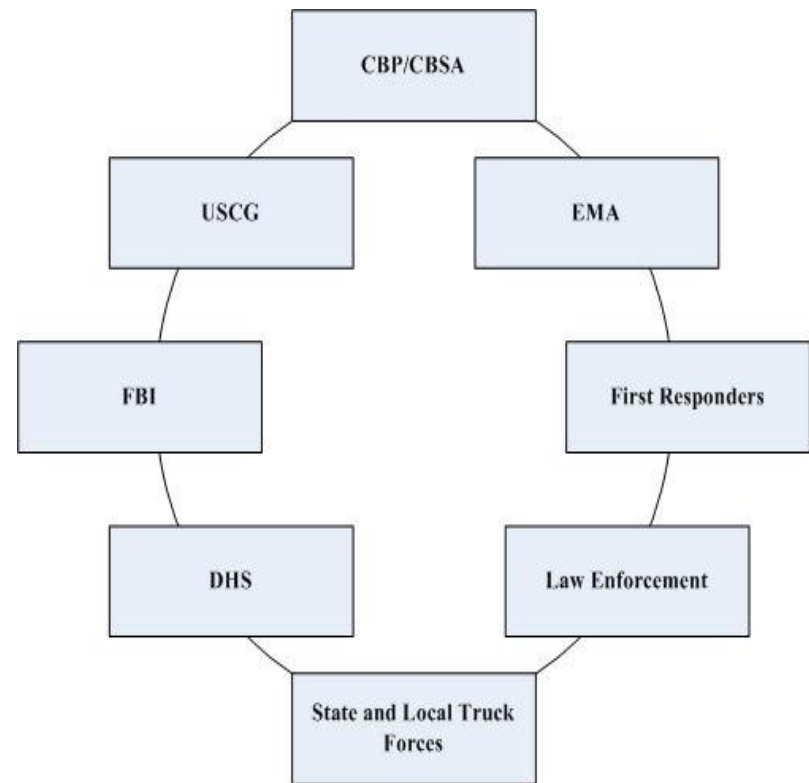
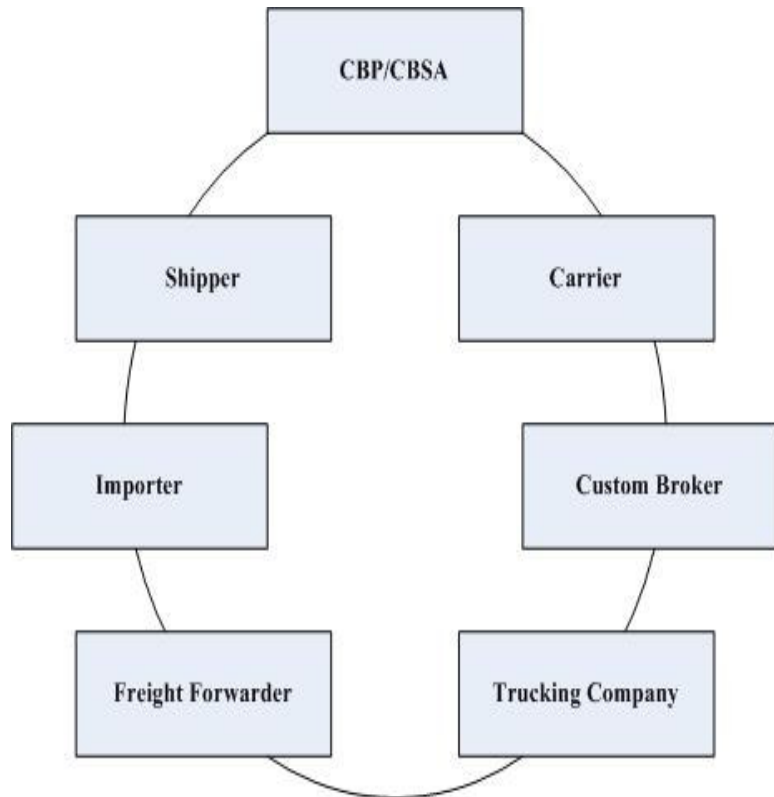
1. **Scenario D & Scenario E** = Third party owns/operates smart container technology & Combination: distributed responsibilities between government and industry.
2. **Scenario A** = Container owner (carrier) owns/operates smart container technology
3. **Scenario B** = Government owns/operates smart container technology



# Communication Infrastructure Identified by Participants

## Industry

## Government/Regulatory Officials

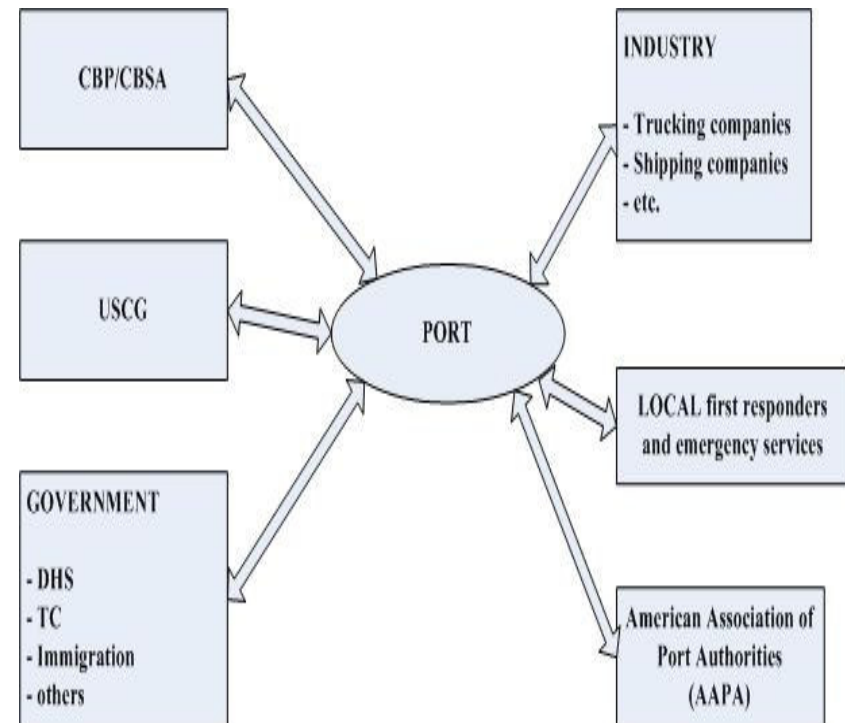
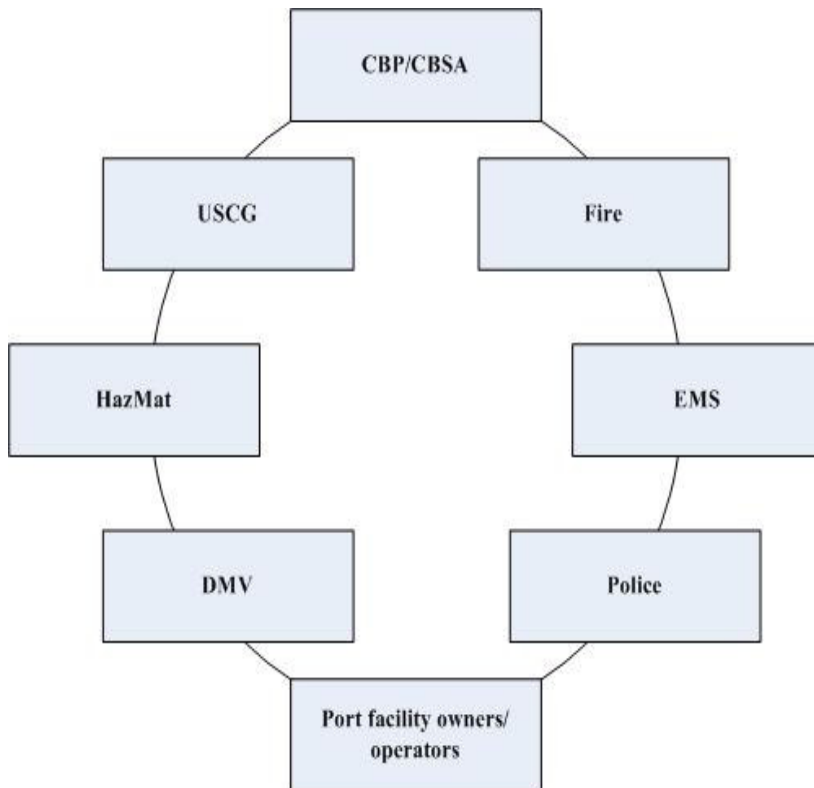


# Communication Infrastructure Identified by Participants (continued)



## First Responders

## Ports





## ***i*CONTAINER OWNERSHIP “BEST PRACTICES” RECOMMENDATIONS**

### *QUERY RESULTS:*

- A commercial organization, “third party”, provides, owns, operates & maintains intelligent container technology.
- The “third party” should be approved and certified by government.
- The “third party” is responsible for intelligent container satellite communications.
- The “third party” invoices customers to recover all associated fees.



## CONTAINER OWNERSHIP “BEST PRACTICES” RECOMMENDATIONS

### QUERY RESULTS *(continued)*

- Third party maintains secure web server, monitors and analyzes in-container data, and notifies first responders about container anomalies.
- International regulations either mandate that containers are equipped with “intelligent” technology, or as a minimum, create commercial incentives (liability disincentives) for importers (supply chains) using smart containers.
- Regulators (government) is granted access to smart container data and secure web-sites.



## COMMUNICATION AND INTEROPERABILITY: Results & Recommendations

- All queried would like to have access to the intelligent container's secure website. *However, none surveyed considered it to be their responsibility for monitoring in-container data for anomalies and alarms.*
- Whenever an in-container ALERT is transmitted, it should be:
  - (a) Timely
  - (b) Accurate (eliminate false positives)
  - (c) Available for analysis with e-cargo manifests, e-bills of lading.
- There isn't a recognized notification and information network for communication interoperability between law enforcement and hazardous material first responders. A standard set of requirements agreed to by DHS and DOJ is urgently needed.



## CONCLUSIONS

- Successful “intelligent containers” will have considered *human engineering* aspects.
- To be able to accurately contrast container anomalies from *false positives* is critical.
- *Effective interoperability* between supply-chain providers (carriers), end-users (importers), regulators (CBP, USCG) and first responders is critical.