



**CANADA – UNITED STATES CARGO SECURITY PROJECT
OPERATION SAFE COMMERCE - NORTHEAST**

**INTELLIGENT CONTAINER TECHNOLOGY
INFRASTRUCTURE AND INTEROPERABILITY “BEST PRACTICES”
SURVEY REPORT**

2005

NOTE

The National Infrastructure Institute Center for Infrastructure Expertise (NI²-CIE) is a not-for-profit applied research organization dedicated to improving the management and protection of the built infrastructure in the United States. The Center is funded through a grant from the U.S. Department of Commerce National Institute of Standards and Technology (NIST). This survey is funded through a grant from Small Business Administration.

Executive Summary

To be able to evaluate interoperability between transportation systems and public safety agencies, NI²-CIE first needed to understand how the transportation industry and public safety organizations perceived actual future use of intelligent container technology:

- Who would own it?
- How it would be maintained?
- How data would be reported?
- Did intelligent container data require analysis and verification?
- What about the possibility of false alarms?
- Do public safety organizations want to have direct access to intelligent container raw data?
- Who should pay for associated costs for maintenance and for operations?

To answer the above questions, NI²-CIE crafted a two part survey. The individuals surveyed included Canadian and American representatives from the container shipping industry, transport operators, seaport operators where containers are routinely handled, law enforcement specialists, and fire departments.

The survey's first part offered participants several options on how the technology should be implemented. The survey's second part asked participants to identify types of communication technologies used during incident response, how well these technologies aided inter-agency interoperability, what protocols are used, and what improvements should be made to integrate intelligent containers into existing communication systems?

Results of the first part of the survey identified that the technology should not be owned by public safety organizations. There should be a third-party commercial organization, which provides analysis services, owns, and operates intelligent container technology. This third party organization should be regulated and certified by an appropriate government agency. The third party would charge customers and recover associated costs from the intelligent container operation. The third party organization is also responsible for maintaining a secure web server, monitoring and analyzing in-container data, and notifying first responder agencies about emergency situations. It would be a government requirement to have all containers equipped with intelligent container technology, or as a minimum, there should be a regulation creating commercial incentives for those importers using intelligent containers. Also, government agencies could be granted access to intelligent container data. An international standard describing intelligent container technology is needed. It was also strongly recommended to limit importer's influence on security related activities.

Results of the survey's second part identified that there are a variety of communication technologies commonly used, but that there is no single universal law enforcement or emergency responder information system currently utilized for inter-agency emergency response interoperability. Only one of the participants specified that their agency follows the NIMS model. Survey participants explicitly stated that interagency interoperability is either very poor, or does not exist at all. The survey's outcome recommended the strong need to improve interagency communication, coordination and interoperability by improving interagency information sharing capabilities and performing interagency exercises.

TABLE OF CONTENTS

1. Introduction	7
1.1. Background	7
1.2. Objectives	8
1.3. Methodology	8
2. Survey Results and Analysis	9
2.1. Container ownership and operation “best practices”	9
2.2. Communication and interoperability	21
3. Recommendations	27
3.1. Container ownership and operation “best practices”	27
3.2. Communication and interoperability	28
4. Conclusion	30
Appendix A - Survey	
Appendix B - Survey results	
Appendix C - Glossary	

LIST OF FIGURES

Figure 1. “Best Scenario” results.....	10
Figure 2. Scenario A evaluation results.....	11
Figure 3. Scenario B evaluation results.....	12
Figure 4. Scenario C evaluation results.....	13
Figure 5. Scenario D evaluation results.....	13
Figure 6. Scenario E evaluation results.....	14
Figure 7. Question 1 results.....	15
Figure 8. Question 2 results.....	16
Figure 9. Question 3 results.....	17
Figure 10. Question 4 results.....	17
Figure 11. Question 5 results.....	18
Figure 12. Container transportation security information sharing network identified by Ports.....	21
Figure 13. Container transportation security information sharing network identified by First Responders.....	23
Figure 14. Container transportation security information sharing network identified by Government/Regulatory officials group.....	25
Figure 15. Container transportation security information sharing network identified by Industry....	26

LIST OF TABLES

Table 1. “Best Scenario” results	10
Table 2. Existing and suggested communication mechanisms by Ports	21
Table 3. Existing and suggested communication mechanisms by First Responders.....	23
Table 4. Existing and suggested communication mechanisms by Government/Regulatory officials group representatives	25
Table 5. Existing and suggested communication mechanisms by Industry	26

1. INTRODUCTION

1.1. Background

The Operation Safe Commerce—Canada/United States Cargo Security Project (CUSCSP), originally known as Operation Safe Commerce-Northeast, is an international/regional initiative, comprising a public-private partnership of federal, provincial, state, and local United States and Canadian members operating in northeastern North America. Its purpose is to provide a rapidly assembled prototype test-bed for elements of cargo container supply chain security. Since early 2002, its strategic goal is to create demonstration models for the international container shipping system that maintain open borders and facilitate commerce while improving security practices via the use of point-of-origin security, in-transit tracking, and real-time data monitoring designed to validate and facilitate the movement of containerized cargo. This project is administered by the National Infrastructure Institute (NI²) Center for Infrastructure Expertise in Portsmouth, New Hampshire.

Problem Statement

A significant deficiency in the security and safety of the international cargo supply chain is the lack of effective communications operability between the maritime and land-based intermodal shipping industry and the federal, state, provincial and local public safety agencies. In the event of a critical event involving an intermodal cargo container that has been detected to contain chemical, biological, radiological, nuclear, or explosive materials (CBRNE), there are no universally accepted procedures or protocols for notification, response, or mitigation, especially during incidents that may occur at or near the U.S.-Canada border. The shipping industry is moving quickly toward the future use of electronic devices on cargo containers that will track the location of a container, detect intrusion, and detect the presence of CBRNE. However, no system is in place to effectively transmit alarms from a container tracking device to the law enforcement and first responder agencies in the jurisdiction where the container is located at the time of the incident.

At this time, there is no defined infrastructure and procedures for operating new intelligent container technology. It is not defined who should, or be willing to own and operate the technology, who should collect the container data, who should analyze the container data, how the data should be analyzed (the extent of human intervention vs. extent of automated analysis), how alerts should be generated, who should receive the container alerts, who should be responsible for relaying the container alerts to first responders, and how the costs of the intelligent container technology should be covered in a way that creates economical incentive for those paying for the technology. The relation of the intelligent container technology to the existing regulatory requirements, such as CTPAT and CSI should be clearly stated.

1.2. Objectives

The goal of the Operation Safe Commerce—Canada/US Cargo Security Project is to demonstrate how the safety and security of the international cargo supply chains affecting the United States and Canada can be improved by 1) establishing communications interoperability between the shipping industry and public safety agencies; and 2) by establishing procedures and protocols for critical events involving intermodal cargo containers.

There are two main objectives of this milestone of the project:

- 1). to collaborate with representatives from law enforcement, first responder, and private sector organizations to identify the most effective infrastructure for intelligent container technology infrastructure and operation protocols;
- 2). to evaluate maritime, land-based intermodal transportation and law enforcement/first responder communications networks and to identify how to create an interface between these dissimilar networks to provide communications interoperability during a critical event involving an intermodal cargo container.

1.3. Methodology

We will interview a sample group that includes representatives from the maritime shipping industry, the domestic US land-based intermodal transportation industry, U.S. Coast Guard, US Immigration and Customs Enforcement, Canada Border Services Agency, Sûreté du Québec, Royal Canadian Mounted Police, Quebec Public Safety Ministry, ports of Halifax (Nova Scotia), Montreal (Quebec), Boston, MA and Portland, ME, a Northeast state police agency, the New England State Police Information Network (NESPIN) and Regional Informational Sharing System (RISS), a local or county law enforcement agency, and a fire department that includes a hazardous materials response team and an emergency medical service.

In the survey we will identify and document a list of possible options for the infrastructure and operational protocols configuration. We will ask the interviewees to identify the best option in each category and possibly give additional comments. We will observe the operations of their communications networks, and will identify at least one methodology or technology that could be utilized to transmit data concerning possible unauthorized entry or the possible presence of CBRNE in an intermodal cargo container to a law enforcement or fire service agency.

We will compile and analyze the survey feedback, and will present the results along with conclusions and recommendations. The data will be presented in a general manner, protecting confidentiality of each organization.

In addition to the survey, we will conduct a research of existing systems and systems under development for emergency incident notification of the first responders and other stakeholders. We will analyze our findings, identify advantages and drawbacks of every system, and will provide recommendations.

2. SURVEY RESULTS AND ANALYSIS

We have succeeded to receive a total of 18 completed surveys. For the analysis purposes the participants were split into 4 categories according to their affiliation:

First Responders ¹ – 5 representatives Government/Regulatory officials ² – 5 representatives Ports – 5 representatives Industry – 3 representatives
--

The fact that we have surveyed only 18 organizations does not minimize the statistical results, because those whom we did survey are involved with the international cargo shipping at the highest levels. For example, port officials whom we interviewed represented the major international ports for the flow of the containerized cargo in and out of the North-Eastern US and Canada.

2.1. Container ownership and operation “best practices”.

Survey section I: part I

In this part the participants were provided with the set of predetermined possible scenarios of the infrastructure configuration and were asked to evaluate each scenario using such parameters as functionality, security enhancement, cost effectiveness, etc. After that we asked participants to pick the best scenario among offered ones. We present the results of the “best scenario” question first, followed by the results for each individual scenario.

¹ From this point through the rest of the document, for the sake of clarity, we will capitalize a first letter whenever a group of survey participants is referenced, and we will use regular font size for the general term. For example, we will use First Responders vs. first responders, Industry vs. industry, etc.

² For simplicity from now on “Government/Regulatory” category will be referred to as “Government”

Table 1. “Best Scenario” results

Scenario	A	B	C	D	E
Total³	5	3	0	6	6
Total %	28	17	0	33	33
Ports	2	0	0	1	2
Ports %	40	0	0	20	40
Government	2	0	0	2	2
Government %	40	0	0	40	40
Industry	1	1	0	1	1
Industry %	33	33	0	33	33
First Responders	0	2	0	2	1
First Responders %	0	40	0	40	20

Scenario A: Container owner owns/operates the intelligent container technology;
Scenario B: Government owns/operates the intelligent container technology;
Scenario C: Importer owns/operates the intelligent container technology;
Scenario D: Third party owns/operates the intelligent container technology;
Scenario E: Combination of the above.

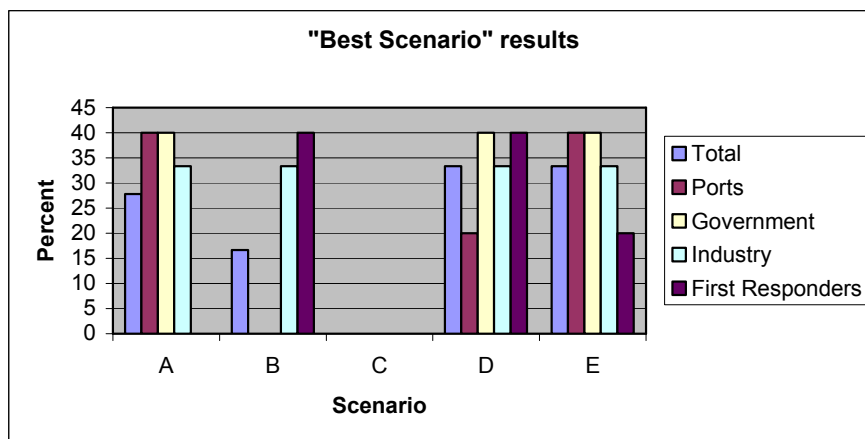


Figure 1. “Best Scenario” results

The above table indicates that the majority of surveyed ranked scenarios in the following order:

1. Scenario D and Scenario E – “Third party owns/operates the intelligent container technology” and “Combination”, i.e. distributed responsibilities between government and industry
2. Scenario A – Container owner owns/operates the intelligent container technology
3. Scenario B – Government owns/operates the intelligent container technology

None of the surveyed preferred Scenario C – Importer owns/operates the intelligent technology. Note that the survey participants were allowed to pick more than one “best scenario”.

³ Total – Total number of participants that picked a particular scenario; Total % - Percent value of a total number of participants that picked a particular scenario.

The following diagrams for Scenarios A – D were built based on data presented in Appendix B. Scores were assigned according to the following rule:

- 1 – Bad
- 2 – Neutral
- 3 – Good
- 4 – Excellent

In the borderline cases where equal percentage voted for different scores, the final score was decided based upon the second highest percentage. For example, if functionality received 40% of “Good” estimates and 40% of “Neutral” estimates, and if the second highest score is 20% assigned to “Excellent”, then the final score reflected on the diagrams below would be “Good”, e.g. “3”. This is a relaxed approach to statistical data analysis, but provides a good tool for visualization of data. Therefore, precise data results of scenario evaluation are given in Appendix B.

Scenario A: Container owner owns/operates the intelligent container technology

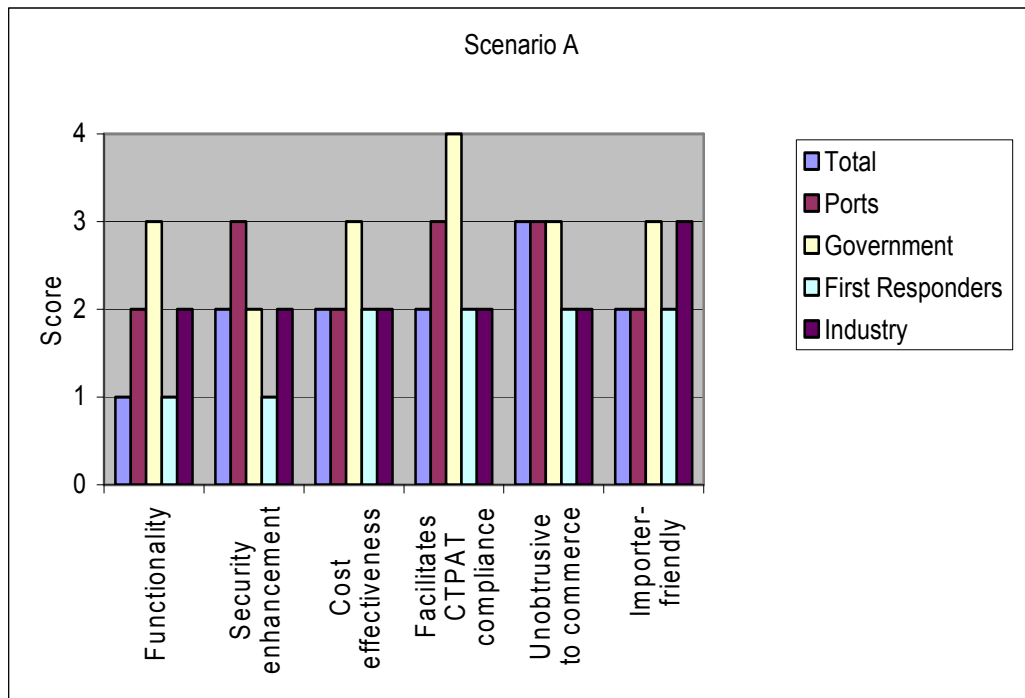


Figure 2. Scenario A evaluation results. Score distribution: 1 – Bad, 2 – Neutral, 3 – Good, 4 – Excellent

Most of the feedback on Scenario A stayed within a “Neutral” zone. The best evaluations to this scenario were given by Government. Scenario A took a second place on the best scenario chart among 4 possible places with the 28% vote. None of First Responders voted this scenario to be the best one.

Scenario B: Government owns/operates the intelligent container technology

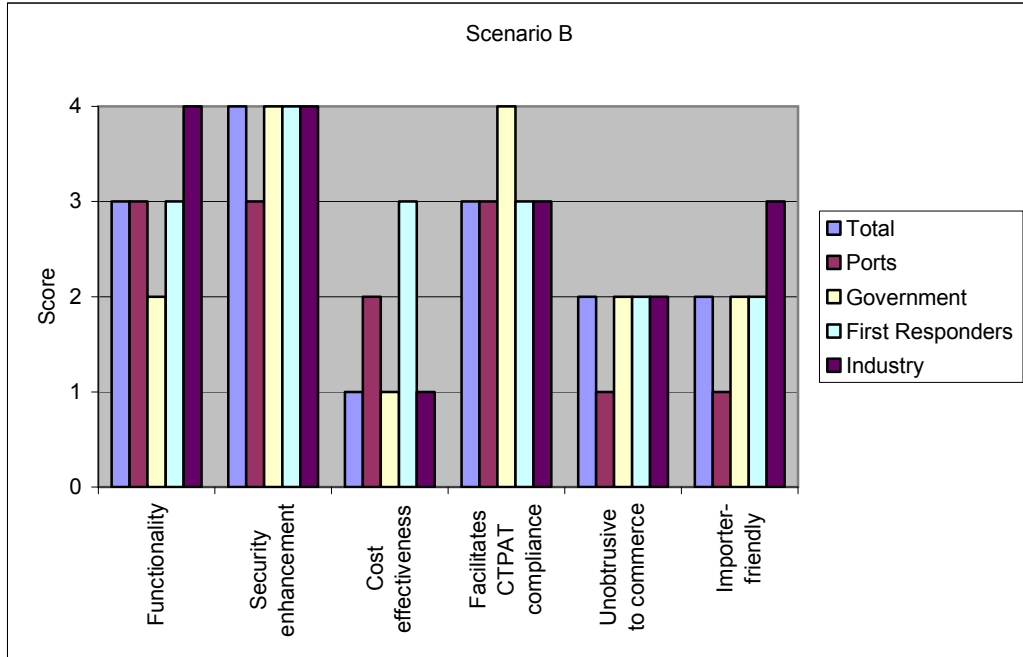


Figure 3. Scenario B evaluation results. Score distribution: 1 – Bad, 2 – Neutral, 3 – Good, 4 – Excellent

The majority of surveyed gave a good score to all parameters of this scenario, except cost effectiveness. Cost effectiveness was predicted to be poor for this setup by most of the parties. Port representatives seem to be concerned that with government operating the technology they will interfere with commerce and will introduce an additional burden to the importer. Even though an overall good evaluation was given to this scenario, it took a third place on the rating chart among 4 possible (17% voted for scenario B).

Scenario C: Importer owns/operates the intelligent container technology

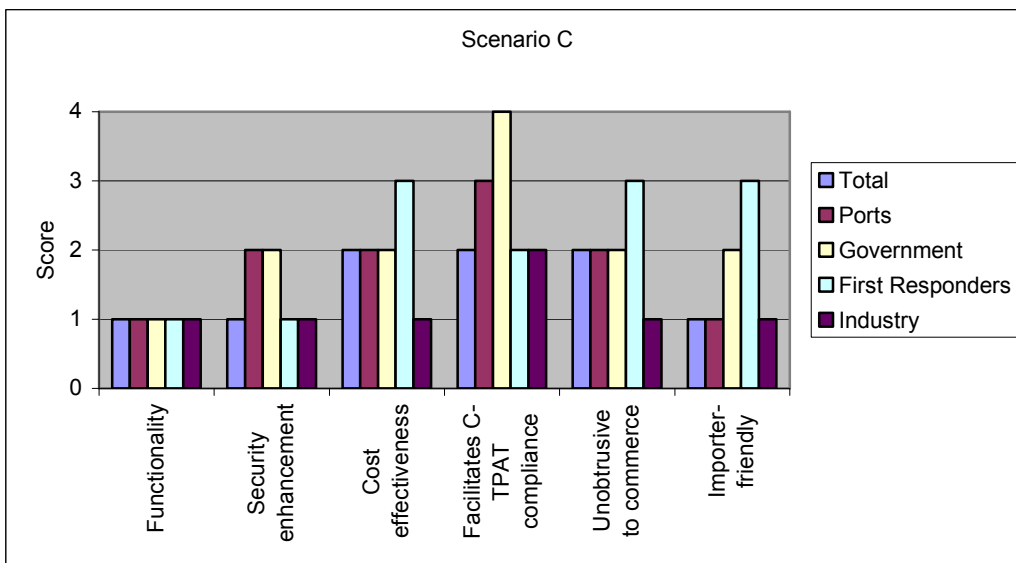


Figure 4. Scenario C evaluation results. Score distribution: 1 – Bad, 2 – Neutral, 3 – Good, 4 – Excellent

Nobody picked scenario C as “best one”, overall bad scores were assigned to each of its evaluation categories. Multiple times it was expressed that an importer should not have control over technology operation (for more details please refer to recommendations part of this report).

Scenario D: Third party owns/operates the intelligent container technology

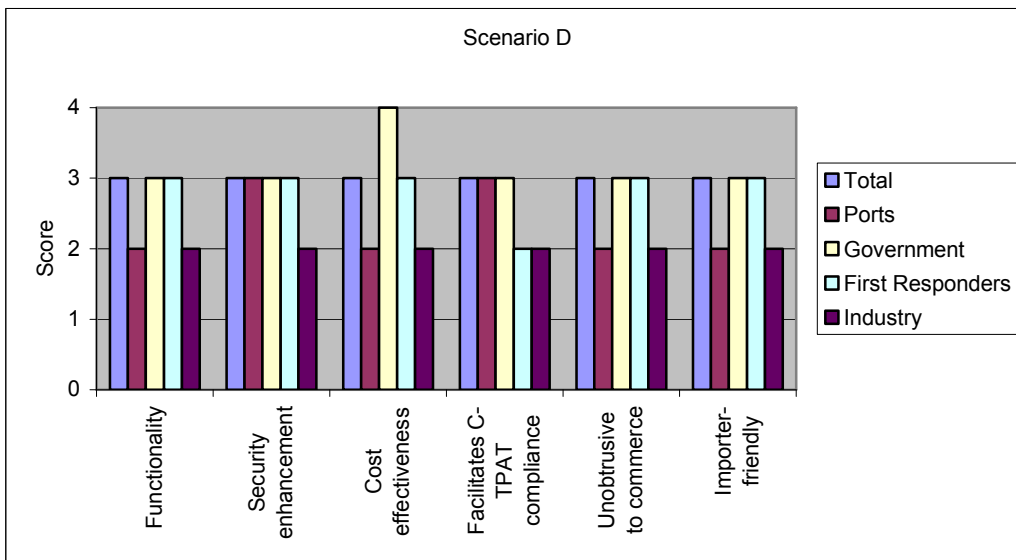


Figure 5. Scenario D evaluation results. Score distribution: 1 – Bad, 2 – Neutral, 3 – Good, 4 – Excellent

Along with the average “good” score given to each of the parameters of this scenario, third party owning and operating the intelligent container technology was chosen as a “best practice” setup. This opinion is consistent throughout the results of the whole survey.

Scenario E: Combination of the above

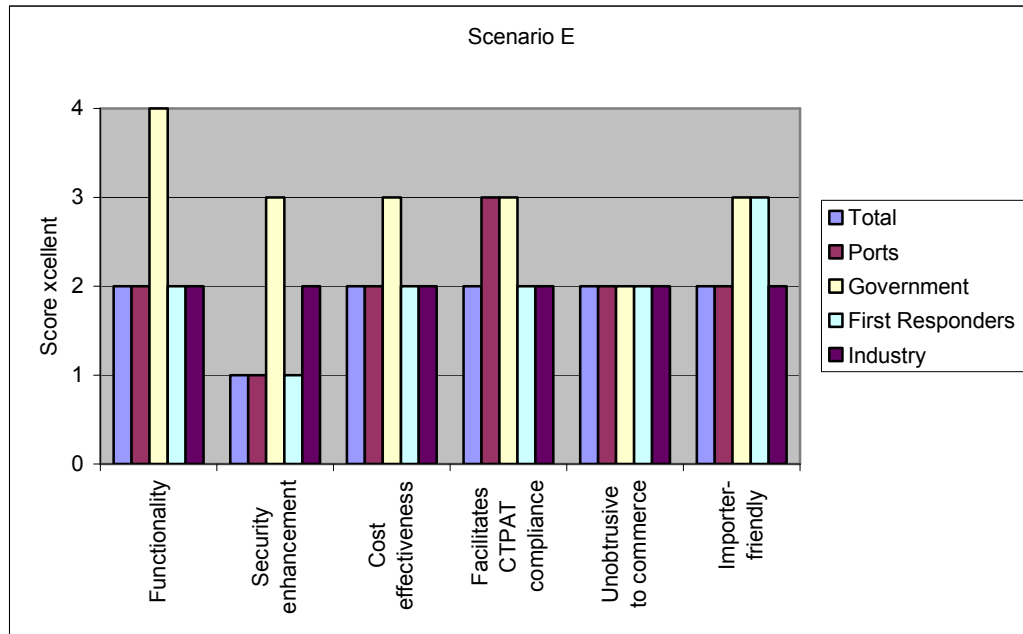


Figure 6. Scenario E evaluation results. Score distribution: 1 – Bad, 2 – Neutral, 3 – Good, 4 – Excellent

Government group gave good evaluation to each category of this scenario while the rest of the participants stayed within the neutral zone. On the overall rating, this scenario shares the first place with Scenario D. This is explained by the fact that almost all of the parties we interviewed expressed that it would be the best if a **THIRD PARTY AUTHORISED BY GOVERNMENT** owned and operated the intelligent container technology.

Survey section I: part II “Build your own scenario”

In this part the participants were asked to recommend the best scenario by building their own (as opposed to predetermined scenarios in part I). We asked them to circle the favored option(s) for each statement.

Question 1: Black box (or a intelligent container box) is owned/purchased by:

- a. Container owner;
- b. Government/law enforcement;
- c. Importer;
- d. Shipping Line.

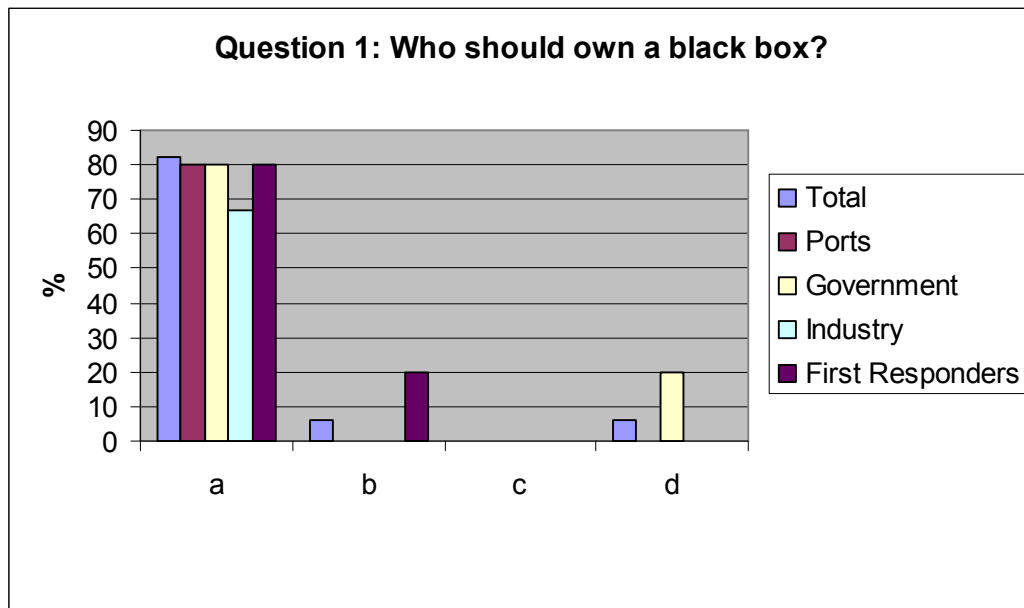


Figure 7. Question 1 results

Most of the surveyed have chosen a container owner as a 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.

Question 2: The black box distributor will provide:

- a. The box distribution, service, and maintenance;
- b. The box installation;
- c. The box configuration;
- d. Logged data recovery;
- e. Satellite service receiving equipment and data processing engine;
- f. Maintain, and operate a secure website where authorized users may access info on their respective containers;
- g. A specially trained team to monitor the container's status;
- h. A choice to Customers to purchase this service (g) or have their own staff trained and responsible for container monitoring;
- i. Distribution of the Data Receiving Package²: satellite receiving equipment, data processing engine (configured to receive the data only from the purchased black box ID's), secure website application.

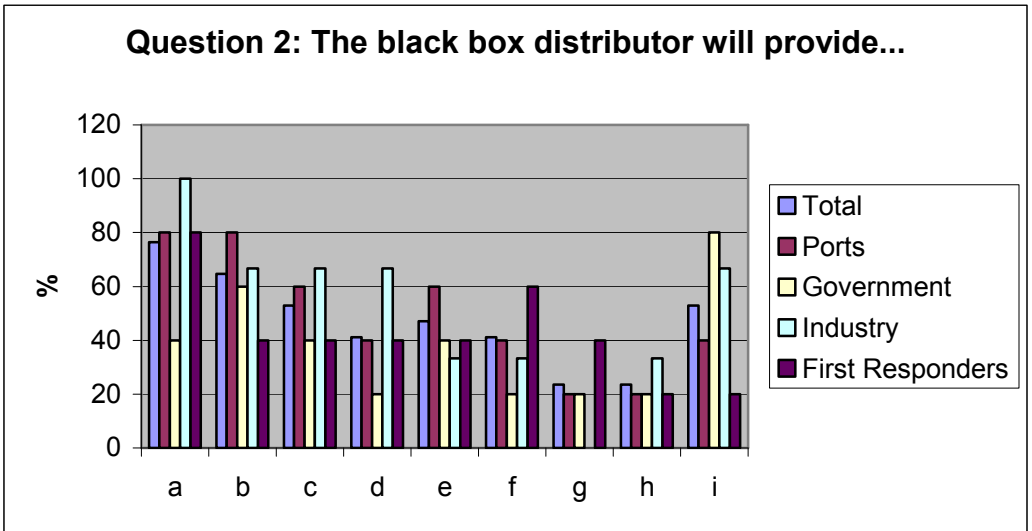


Figure 8. Question 2 results

Most of the surveyed thought that whoever provides a black box distribution should also provide black box installation, configuration, service, and maintenance. It was not recommended for the black box distributors to provide logged data recovery.

47% of the surveyed agreed that the satellite service receiving equipment and data processing engine should be provided along with the black box by the distributor. Neither of the options pertaining to operation of the black box once it is purchased and installed in the container (options f, g, h, and i) was approved by the surveyed.

Question 3: Container owner:

- a. Purchases a Data Receiving Package w/access to the Importer’s secure website for the duration of the container lease;
- b. Provides a specially trained team to monitor the container’s status by;
- c. Provides black box log data recovery;
- d. Maintains its own box service and maintenance department.

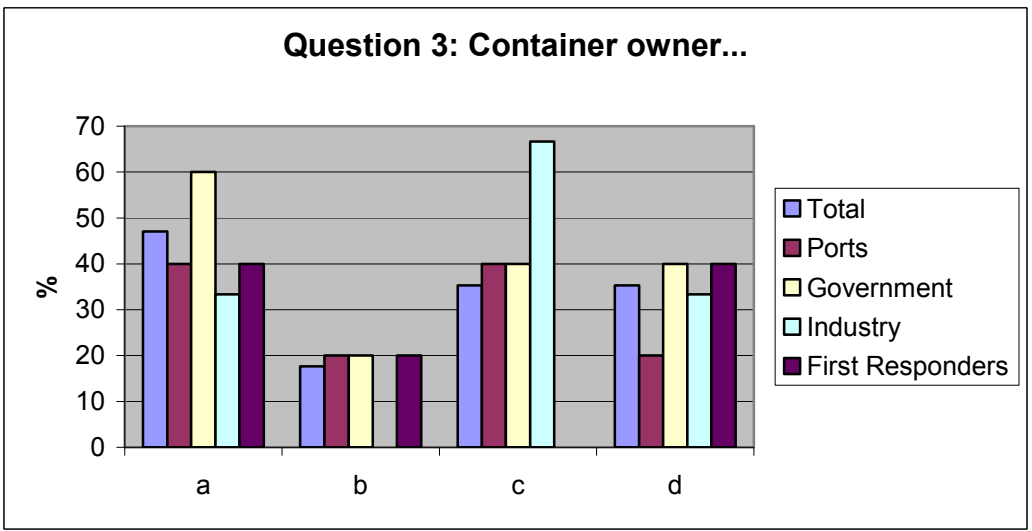


Figure 9. Question 3 results

Each of the responsibilities mentioned in a question on average received less than 50% vote. This result is consistent with the recommendations that a third party authorized by government should carry all of the above responsibilities.

Question 4: Importer:

- a. Purchases a black box;
- b. Leases a container equipped with a black box;
- c. Leases access to the secure website to monitor the container's status;
- d. Provides access to allow government law enforcement and regulatory officials to view the container status;
- e. Decides to share full or partial information with law enforcement/regulatory agencies.



Figure 10. Question 4 results

None of the surveyed agreed that a container black box should be purchased by the importer, but rather a container pre-equipped with a black box should be leased by the importer.

Less than a half of the surveyed (and nobody from the Ports group) agreed that an importer should lease an access to a secure website for a purpose of monitoring the container status. Similar result were obtained for options d) and e), with a general comment that an importer should not be a party deciding whether to share a container status information with the law enforcement and regulatory officials, neither should it be importer's decision which information to share.

Question 5: Government/regulatory/law enforcement/first responders:

- a. Possess Data Receiving Package;
- b. Have unlimited access to secure websites of the container companies;
- c. Have access to the complete pre-agreed container importer data;
- d. Have access to partial container data as determined by the importer;
- e. Establish an agreement similar to CTPAT, which would result in a lower risk number to importers who agreed to share the black box info;

- f. Monitor the container status by a specially trained team in exchange for permission to have unlimited access to container data.

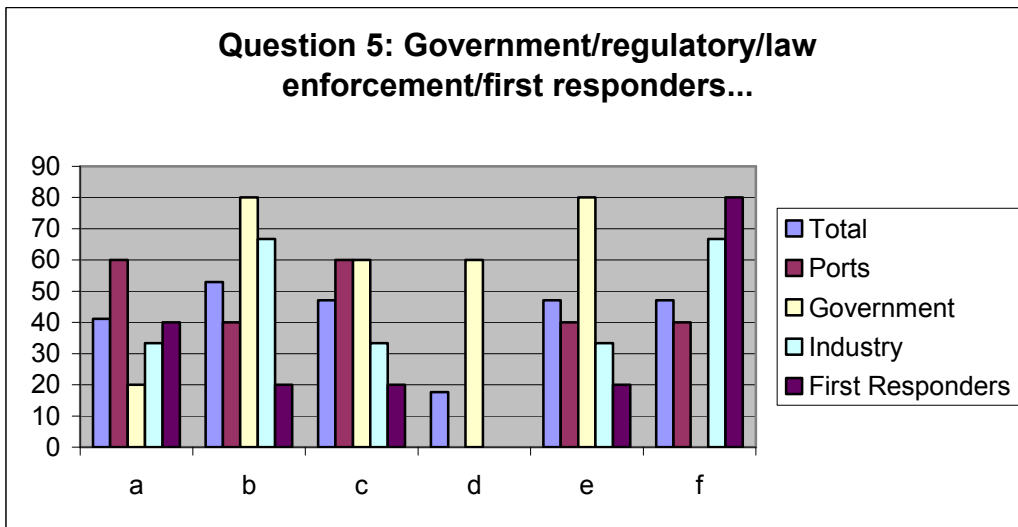


Figure 11. Question 5 results

60% of Ports agree that the “government/law enforcement/regulatory officials/first responders” should possess Data Receiving Package⁴ and have access to a complete pre-agreed container data. While only 20% of government and 40% of first responders would like to be in possession of Data Receiving Package.

80% of participants from the Government group expressed a desire to have an unlimited access to secure websites with the container data. This opinion is supported by 67% of Industry representatives, and 53% of the all surveyed.

Government group was the only party that agreed “government/law enforcement/regulatory officials/first responders” should have access to a partial container data as determined by the importer. The rest of the surveyed expressed a strong disagreement with this statement (0% of Ports, Industry, and First Responders).

80% of participants from the Government group favored the option of establishing an agreement similar to CTPAT, which would result in a lower risk number assigned to importers who agreed to share the black box info.

While nobody from a Government group considers that “government/law enforcement/regulatory officials/first responders” should monitor the container status by a specially trained team in exchange for permission to have unlimited access to container data, 40% of Ports agreed with such a possibility, and so did the majority of Industry and First Responders.

⁴ See the list of terms and abbreviations for the definition of Data Receiving Package

Survey section I comments and recommendations

The following are selected comments and recommendations provided by the interviewed parties after completion of section I (including both parts I and II).

Industry

“It is necessary to find a way between cost and the interests of security. In the next years the costs per container shipments will increase dramatically. Reason: Oil price, capacity on vessels and increased container traffic.”

“There should be a mandate that the importer has to use “intelligent containers” to import goods to USA. The third party, approved by government, would provide such services. The third party will be responsible for alerts, and will possess all equipment. Government does not have financial resources to manage the process, but is a recipient of container data, similar to the current practice of sending electronic cargo manifest to USCBP. USCBP has a list of approved vendors (third parties).”

The following concerns were brought to attention for future research:

“What happens when a container at the bottom of the stack reports an alarm? Will ship personnel be certified to inspect and clear the alarm, or does the ship have to be diverted to a special ‘safe harbor’ to unload the specific container for inspection?

Will DHS/DOC randomly or regularly ‘audit’ the alarm logs? Will they audit them at all? What is an acceptable alarm error rate?”

Ports

The best practices scenario suggested by one of the port representatives:

“A private company produces a universally employable international regulated “intelligent-black box” which is tamper proof. This box provides a blank re-usable format that is then activated when secured to a container. The activation occurs from the exporter’s warehouse and the activation is monitored through the transit until received by the importer (not the terminal but the actual importer). Through the intermodal network, periodic checks at regular neutral waypoints in the system, highway overpass and truck stops, rail portals, terminal gates and portals, gantry crane hoists, the intelligent boxes are challenged by governmental sensors which confirm exporter, transportation means and modes, through the transfer to importer. At any point that verification identifies a tampering or alarms due to contents, the container is flagged by government agencies and withdrawn from the pipeline and inspected. If cleared a new intelligent box is re-programmed and the container continues on its way until it arrives at the destination. The intelligent box is a cost recoverable and wipe cleanable component and is reused on the other end to reship the next shipment. They are interchangeable but not unless the importer code is entered to release it as provided by the exporter. Government maintains the validation and security of the network through transportation checks, industry maintains the costs for incorporating the black boxes into the pipeline on both ends and in the middle to evenly distribute the cost load. The security can only exist in the regulation of the equipment and the monitoring of the seal and alarms. To off-load the regulation and auditing of the technology defeats the security component and leaves it susceptible to third party tampering.”

First Responders

"I would strongly suggest that we look for a vendor that will meet strict guidelines and fall under the oversight of the US Government. This vendor should have no interest in financial gain as it relates to any aspect of Container Security.

Containers should come completely out-fitted with all equipment needed to allow successful transportation of commerce into the US. This is an area where Government and the vendor may have to share expense for the initial start up.

Agencies outside of the vendor and government should have limited access to the status of the container. For example:

Owner/Operator should be able to access the web for location and condition of the container and contents. There will need to be an associated fee for this privilege.

If a problem develops with the container it will be up to the vendor to provide this information to the Company that owns or possibly lessees the container.

On the flip side of the coin, if we allow private ownership and maintenance of the container and black box, we will set ourselves up for corruption and failure. Government needs to work with commerce on this in order to be successful. If we can provide security and tracking of the containers, along with easing Border access, it maybe in the best interest of everyone involved."

"System should be modeled after a "CHEMTREC" type of system. However, with critical information designed to flow out to "first responder" agencies, and of course with first responders able to call in.

"Intelligent Box" should be required by government, as an industry standard.

A third party agency should regulate the technology. Not the importer, not the exporter, or other directly impacted stakeholders.

Example: "Black boxes" are required on all passenger aircraft by FAA."

"The "intelligent container technology" or "intelligent boxes" themselves should be manufactured, furnished, installed and /or maintained only by duly authorized provider. That is to say, with strict maintenance and regular testing along with proper record keeping of those activities, which would be subject to governmental oversight."

Government/Regulatory Officials

"I think that the owner is to be made accountable for the purchase and maintenance of the system. He could then charge an extra fee to the importer.

I don't think that government agencies should administer the system as the costs are always prohibitive when government run.

I think they should be monitored by law enforcement officials or by a private company with government security clearance, for security reasons.

If they were to be monitored by the owner or the importer there would be more room for security breaches.

I do believe the owner and the importer should be able to monitor the container as FEDEX or UPS do for customer service."

"Shipper should be paying for the service. Gathering of data should be centralized, not divided among all shippers. Need to make sure to tie the electronic cargo manifest and bill of lading. The cost will be ultimately passed onto a consumer. Importer should not have a large share of participation other than cargo manifest for the purpose of preserving security and accuracy. Certain "for profit" entity should manage the program."

2.2. Section II: Communication and interoperability

Survey Section II

Container transportation security information sharing network diagrams below do not necessarily reflect the complete interoperability infrastructure. The diagrams reflect only those parties identified by the survey participants.

Ports

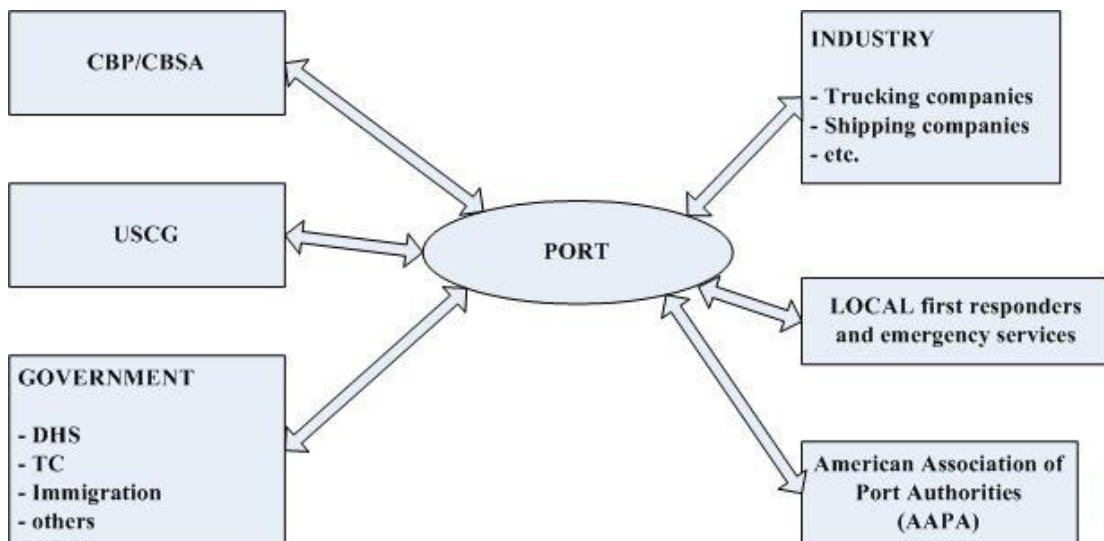


Figure 12. Container transportation security information sharing network identified by Ports

Table 2. Existing and suggested communication mechanisms by Ports

Communication Mechanisms	
Currently in use	Suggested for sharing container security data
1. verbal 2. phone 3. fax 4. e-mail 5. internet 6. intranet (VPN) 7. database sharing (in some cases ⁵) 8. paperwork	1. tie the intelligent container data into existing system for spatial terminal management 2. VPN station with various access levels 3. build an integrated system of command and control in an automated format that can alert the government agencies of potential problems with a container

⁵ Database sharing not mentioned as one of the communication mechanisms does not necessarily indicate that it does not take place.

9. walkie-talkie (portable bi-directional radio transceiver) used within the facility	4. e-mail
10. dedicated phone lines to Emergency Services	5. fax
	6. access to a container security data website

Most of the participants from the Ports group expressed a desire to receive intelligent container alarms as opposed to raw container data (sensor readings). It was noted that the system for electronic manifest transfer is already in use by ports, but it desirable to integrate this information with the intelligent container alarms.

List of interagency interoperability improvement recommendations by port representatives:

1. "Share access to databases and messaging services";
2. "The system is not improved nor is security achieved unless the "honor system" of manifests is somehow made tamper proof from a origin to destination tamper proof technology that can be universally applied in the global market";
3. "I would recommend a joint operations center that manages facility and container information to give all concerned government agencies, operational awareness";
4. "Continue/expand coordination dialog and coordination among agencies and industry partners".

To identify emergency management regulations that could be applied to intelligent container emergency situation the question "What emergency plans/protocols do you currently use?" was included in the survey. The following facts about port emergency management were learnt:

1. some ports use their own "in-house" first response teams, like fire team, hazmat team, and port police department;
2. port-wide "Central Communication and Coordination Center";
3. use a local area emergency response plans that comply with the National Response Plan and NIMS (National Incident Management System) model;
4. MTSA (Maritime Transportation Security Act).

General opinion of Ports group representatives regarding first responders receiving intelligent container data is that first responders should not be receiving raw sensor data. Instead alarms along with the alarm pertinent sensor readings should be delivered to first responders, e.g. first responders "should know what exactly they are dealing with".

First Responders

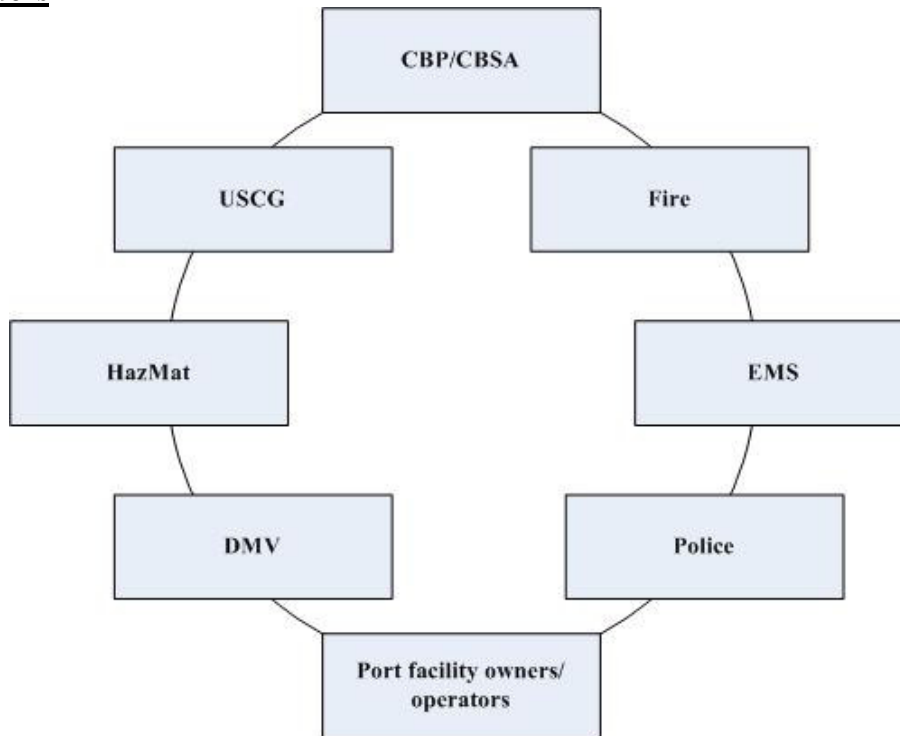


Figure 13. Container transportation security information sharing network identified by First Responders

Table 3. Existing and suggested communication mechanisms by First Responders

Communication Mechanisms	
Currently in use	Suggested for sharing container security data
1. verbal 2. phone 3. internet 4. e-mail 5. intranet (VPN) 6. database sharing (in some cases) 7. paperwork 8. NESPIN/RISS	1. phone 2. e-mail 3. secure Internet connection 4. access to a secure website 5. through Fusion Center 6. fire and police department dispatchers

The table above lists the communication mechanisms for general interagency operation. Only one representative of First Responders indicated that they receive “ship’s manifest from USCG”. The rest of the First Responders specified that they do not receive any of container data and there are no communication mechanisms for that in place.

General opinion expressed by First Responders is that they would like to receive an “immediate”, or “real time” notification of an alarm together with more detailed data related to alarm (partial specific container data). It was also suggested that a real time notification should be backed up by a follow up electronic note from the agency monitoring intelligent containers.

List of interagency interoperability improvement recommendations by first responders:

1. provide as much as possible of real-time information;
2. make sure all agencies have access to a container tracking database;
3. keep track of the information regarding container inspections and deficiencies, make sure to provide this information to everybody;
4. enhance training and coordination among agencies.

To identify emergency management regulations that could be applied to intelligent container emergency situation, the question “What emergency plans/protocols do you currently use?” was included in the survey. The following plans/protocols were identified:

1. Local SOP (Standard Operating Procedure)
2. Regional GRP (Geographic Response Plans)
3. USCG Area Contingency Plan
4. Local fire and mutual aid agreements
5. New Hampshire Emergency Response Plan – NHERP, that is expected to get amendments to reflect container security in a near future
6. Commercial Truck Team Plans
7. HazMat team response Plans
8. Manning the EOC (Emergency Operations Center)
9. Emergency Management plans

First Responder comments and recommendations (collective view):

It should be a goal of this project to ensure that all current container data that can be shared with the appropriate agencies is done so in a timely fashion. The first responders in turn need to have related information that will provide them the opportunity to approach with caution and safety.

There is no mechanism currently in place to allow inspection of the container contents without court ordered documents. Further research needs to be done on this so that if there is a suspicion by the officer it will not have to reach a court recognized level of authority. However, they would be able to do a cursory inventory of the contents before sending the shipment on its way.

Government/Regulatory Officials

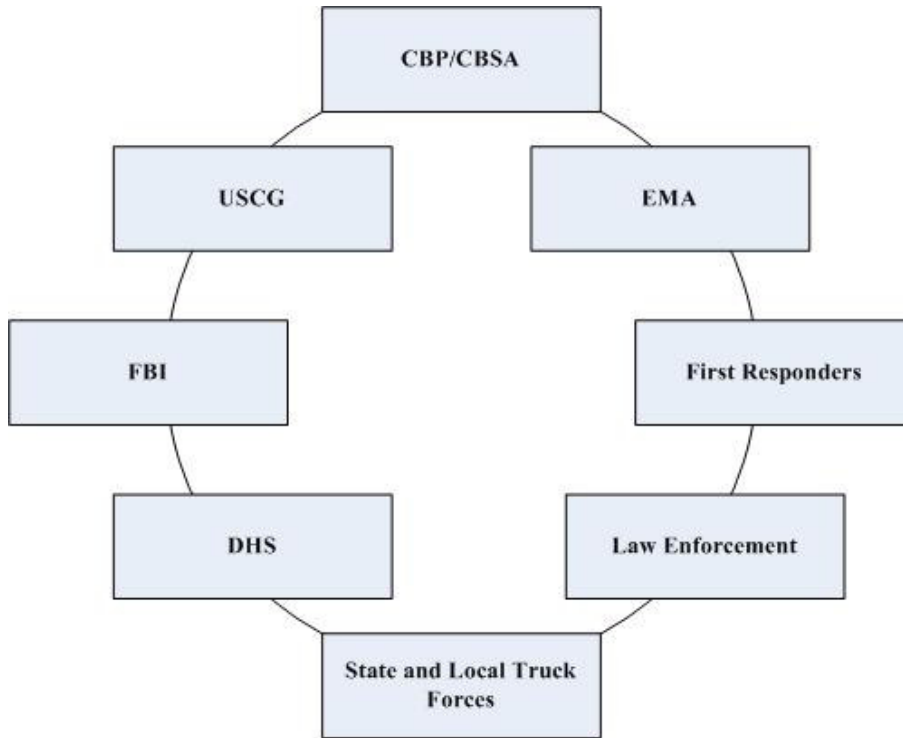


Figure 14. Container transportation security information sharing network identified by Government/Regulatory officials group

Table 4. Existing and suggested communication mechanisms by Government/Regulatory officials group representatives

Communication Mechanisms	
Currently in use	Suggested for sharing container security data
1. verbal (including interagency trainings) 2. phone 3. paperwork 4. e-mail 5. fax 6. special phone lines (for ex., NAWAS – National Warning System, GETS – Government Emergency Telecommunication Service) 7. teletype 8. intranet 9. TECS computer system	1. unlimited access to the secure website 2. instant verbal notification of breaches as soon as possible 3. phone

Government/Regulatory officials group expressed a desire to have unlimited access to all of the container security data including sensor readings, tracking information, cargo manifest, and alerts.

The only recommendation for interagency interoperability improvement is to ensure “a full representation of all Law Enforcement and Safety agencies that have a vested interest in container security present at the Maritime Intelligence Center (MIC).”

USCG utilizes MISLE database (Marine Information Safety and Law Enforcement system) for importing container data after an incident involving container. This info is not readily shared outside USCG.

Intelligent container data **should** be communicated to ACE (Automated Commercial Environment).

Industry

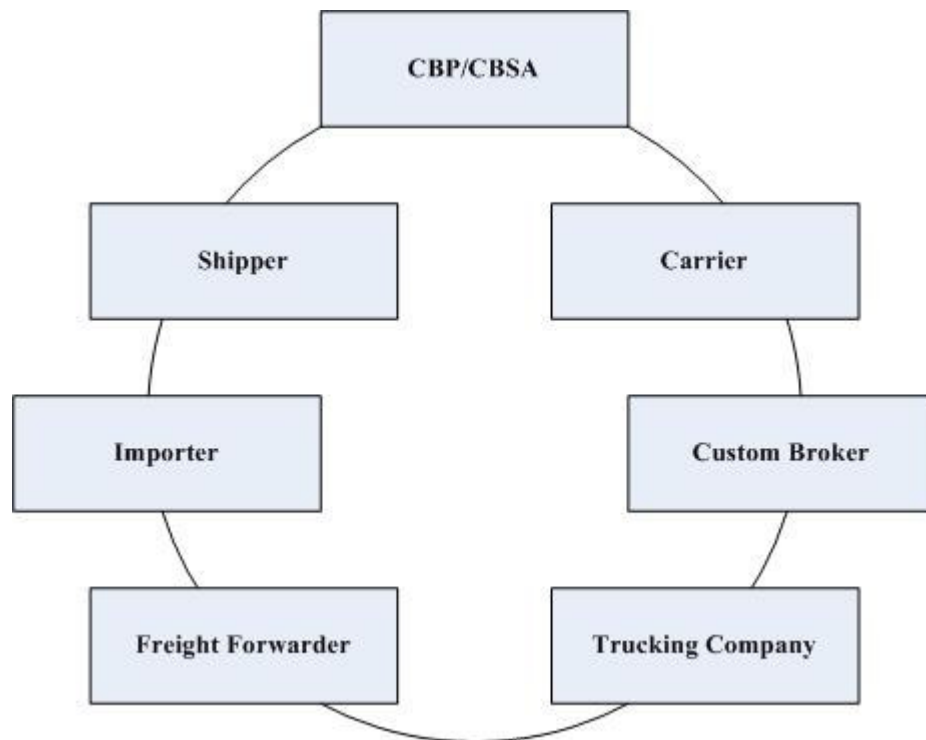


Figure 15. Container transportation security information sharing network identified by Industry
 Table 5. Existing and suggested communication mechanisms by Industry

Communication Mechanisms	
Currently in use	Suggested for sharing container security data
1. phone 2. verbal 3. internet 4. database sharing 5. excel sheets	1. phone (direct notification from a trusted party) 2. web 3. FTP (File Transfer Protocol)

Industry would like to receive notifications of emergency alarms, location of a container that causes an alarm, and information about a nature of the alarm (for ex. danger rating of the alarm).

3. RECOMMENDATIONS

3.1. Container ownership and operation “best practices”

The best practices scenario for the intelligent container technology ownership and operation according to the results of this survey is the following:

- there exists a commercial organization(s), a “third party”, that provides, owns, and operates the intelligent container technology;
- this third party should be approved, or certified, by government;
- third party pays to the satellite service provider for communication with the intelligent containers;
- third party charges a customer to recover all the fees associated with the intelligent container operation;
- third party is responsible for maintaining a secure web server, monitoring and analyzing the container data, and notifying first responder agencies in the emergency situations;
- it is required by government to have all containers equipped with the intelligent container technology, or at least there is a regulation creating commercial incentives for those using intelligent containers;
- government is granted access to intelligent container data.

This setup was derived from the scenarios A and E that share the first place on the rating chart, from the results of the section I: part II, and from recommendations provided by the surveyed.

Scenario A took a second place on the overall rating chart due to the following. First of all, it was recommended that there should be an international standard mandating the use of intelligent containers, therefore it is logical to have container owner to also own an intelligent box, which may be considered to be a part of container body. Another factor is that a great percentage of the overall world container shipping is done by the big shipping companies that own their own containers. It is logical to foresee that when intelligent containers become used often enough, those big shipping companies would expand their service to include container monitoring thus providing a “one stop shop”. In such cases the setup described in scenario A takes place which explains its popularity among the survey participants. Note, that in such a case, according to the survey results, shipping company would have to obtain a government authorization to monitor the intelligent container data. This result is consistent with the result of the first question of “build your own scenario” part, where the surveyed specified that the black box should be owned/purchased either by a container owner, or a third party.

There should be established a standard describing intelligent container technology functionality and operation requirements. This should be an international standard recognized around the world. The standard should be introduced at the early stages of the intelligent container technology deployment to prevent a chaotic situation with multiple-vendors multiple-standards situation that was historically observed in other parts of the industry. As for example in cellular communication industry up until

about four years ago Europe and United States were using different communication standards (US AMPS, US Digital, US IS-95 CDMA, and GSM in Europe). In this case the standards were defined, but were different in different parts of the world.

Standardizing the intelligent container technology also helps implement a recommendation that an intelligent container black box should be reusable, this will aid a cost reduction for the end user.

It is recommended to limit importers impact on the security related activities as much as possible. This is different from C-TPAT, where importer is held responsible for the supply chain C-TPAT compliance. None of the surveyed picked Scenario C – “Importer owns/operates the intelligent container technology” as a best one. Reasoning for that is that an importer is removed too far away from a supply chain, importers vary from big companies and regular customers to small one time importers, importers hold too much commercial interest in the shipping process, therefore may be trying to avoid additional costs associated with security improvement. The biggest concern is that it is the one-time small unknown importer who has the highest terrorism-related risk score.

Along with all described above, the following issues should be addressed:

- ensure that the cargo manifest is tied into intelligent container data;
- whatever party or organization is distributing an intelligent container box, it should provide such services as box installation, configuration, service, and maintenance. But this party should not be involved in any customer/cargo-specific activities after the box is purchased and installed in a container;
- special attention should be paid to balance between cost and security while designing the infrastructure. Especially taking into consideration increasing cost of shipping due to the oil price, increase of traffic, and a limited capacity of vessels.

3.2. Communication and interoperability

All of the surveyed would like to have access to an intelligent container data secure website, but none of the surveyed considers that his/her organization should be monitoring the intelligent container data for alarms. Government group participants stressed that they would like to have “unlimited” access to a secure web site.

Whenever an alarm is transmitted, it should be delivered: 1) in a timely manner, i.e. with a minimal delay, and 2) with all available support, or explanatory data related to the nature of the alarm.

A general concern expressed by the First Responders was that there is a lack of a unified system for communication with first responders and among first responders. A recommendation is for the government to define a standard system or a set of requirements for such a system that would be used by all first responders across the country. If such system or set of requirements is developed in future, one of the features should be the capability to transmit and deliver intelligent container alerts to first responders, therefore an additional set of requirements for the type and for of container alert data should be developed and agreed upon.

The above opinion is supported by the rest of the surveyed, the participants explicitly stated that interagency interoperability is either very poor, or does not exist at all in some cases. It was

recommended to improve interagency communication and coordination, ensure interagency information sharing, and conduct interagency trainings.

While designing an information sharing network for the intelligent container data, we recommend making sure to utilize already existing *agencies* and *information sharing systems*, i.e. build a new system on top of existing pieces. The following agencies already exist and should be involved in the intelligent container data communication network:

- fusion centers which are used mostly for intelligence gathering and analysis;
- communication and coordination centers exist in some ports;
- fire and police department dispatchers as recommended by First Responders;
- Maritime Intelligence Centers (MIC).

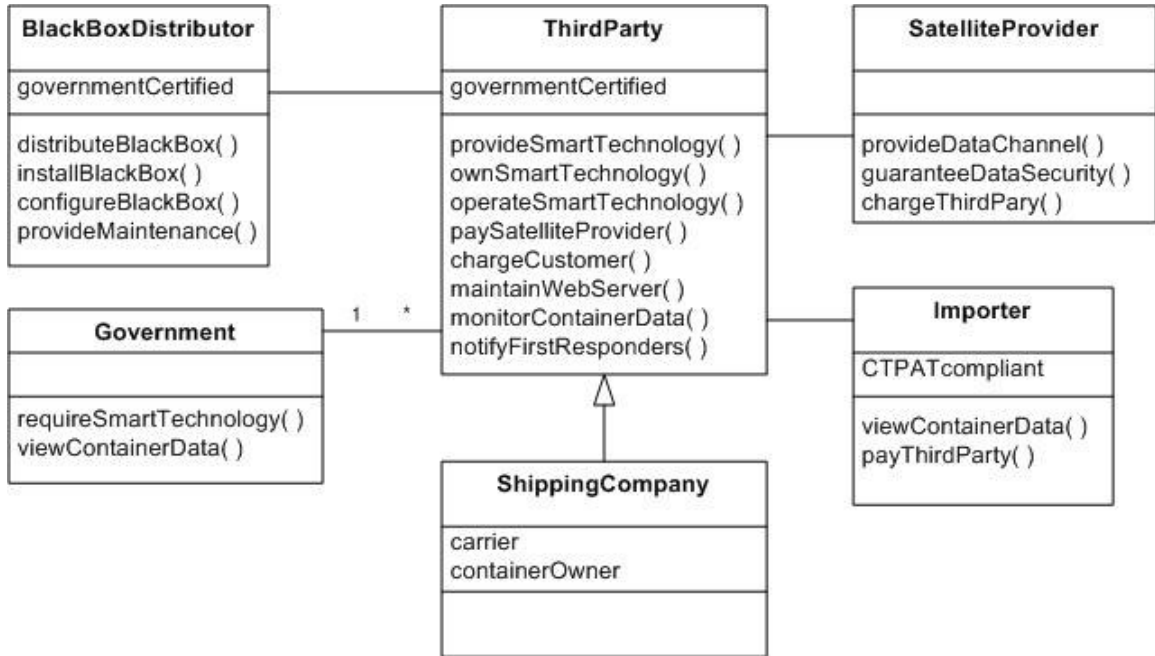
The following information sharing systems already exist and should be involved in the intelligent container data communication network:

- Regional Information Sharing System (RISS) network together with its subnets;
- Automated Commercial Environment (ACE) used by customs;
- USCG Marine Information Safety and Law Enforcement (MISLE) system is used for importing container data after an incident involving a container;
- systems for spatial terminal management are used in some ports and would help to quickly locate the container generating an alarm.

One of the questions of the survey was “What emergency plans/protocols do you currently use?” None of the specified plans and protocols was container specific; in fact different agencies had completely different sets of plans and protocols. Such a setup works well until there is a need for interagency interoperability. Only one of the participants specified that their agency follows the NIMS model. Therefore, we recommend along with the technology and infrastructure development to develop universal emergency response plans and protocols that would provide a comprehensive guide on handling the emergency situations involving intelligent containers.

4. CONCLUSIONS

Best practices scenario for intelligent container technology ownership and operation is described in details in section 3.1 of this report. The UML (Unified Modeling Language) class diagram describing this best practices scenario is presented below⁶.



Government is not willing to share costs associated with the intelligent container technology, does not want to be responsible, or create a new agency from monitoring intelligent containers.

Independently from who provides the intelligent container monitoring services, container owner and an importer should be able to view intelligent container data.

There is no unified system for communication with and among first responders, which could be used for delivery of intelligent container alarms.

There exists intelligence gathering and information sharing systems such as MISLE, ACE, fusion centers, etc. Those agencies and systems are not interlinked, and information is not shared outside of the home organization. Interagency interoperability in general was defined as poor and needing improvement.

There are no existing emergency plans, or protocols that could be adapted for situations involving intelligent containers. Such plans and protocols should be developed.

⁶ Class diagram notation:

