Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
SWUTC/08/473700-00095-1		

4. Title and Subtitle	5. Report Date
Addressing Cargo Security with Strategies Involving Private Sector	December 2008
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Jason R. West, C. Michael Walton and Alison J. Conway	Report 473700-00095-1

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Center for Transportation Research University of Texas at Austin 3208 Red River, Suite 200 Austin, TX 78705-2650	11. Contract or Grant No. DTRS99-G-0006

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Southwest Region University Transportation Center Texas Transportation Institute Texas A&M University System College Station, TX 77843-3135	14. Sponsoring Agency Code

15. Supplementary Notes

Supported by a grant from the U.S. Department of Transportation, University Transportation Centers program.

16. Abstract

The public and private sectors contributing to goods movement agree that cargo security has not been addressed nearly as much as physical and vessel security. Addressing cargo security will require additional operational data that is not currently used in public sector security analysis and decision making. The two strategies presented to acquire operational data are freight advisory councils and cargo data collection portals that have been developed by Horizon Services Group. The report identifies four steps that freight advisory councils could implement to improve coordination for cargo security and provides an overview of the cargo data collection portal as envisioned by Horizon Services Group.

17. Key Words	18. Distribution Statement
Security, Cargo, Freight Transportation, Planning, Public-Private Partnerships	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

19. Security Classif. (of report)	20. Security Classif. (of this page)	21. No. of pages	22. Price
Unclassified	Unclassified	38	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

ADDRESSING CARGO SECURITY WITH STRATEGIES INVOLVING PRIVATE SECTOR

by

Jason R. West
C. Michael Walton
Alison J. Conway

Research Report SWUTC/08/473700-00095-1

Southwest Regional University Transportation Center
Center for Transportation Research
University of Texas at Austin
Austin, TX 78712

DECEMBER 2008

DISCLAIMER

The content of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation and the University Transportation Center's Program in the interest of information exchange. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

ACKNOWLEDGMENTS

Support for this report was provided by a grant from the U.S. Department of Transportation, University Transportation Centers Program to the Southwest Region University Transportation Center.

Greg Skinner with Horizon Services Group was the industry partner who provided documentation and presentations describing an electronic data collection portal for security and cargo flow being evaluated with the Jacksonville Port Authority (JAXPORT).

ABSTRACT

The public and private sectors contributing to goods movement agree that cargo security has not been addressed nearly as much as physical and vessel security. Addressing cargo security will require additional operational data that is not currently used in public sector security analysis and decision making. The two strategies presented to acquire operational data are freight advisory councils and cargo data collection portals that have been developed by Horizon Services Group. The report identifies four steps that freight advisory councils could implement to improve coordination for cargo security and provides an overview of the cargo data collection portal as envisioned by Horizon Services Group.

EXECUTIVE SUMMARY

Cargo security is an important concern in global trade and freight transportation. U.S. Department of Homeland Security initiatives have addressed physical facility security and vessel security, but answering the important questions, "What is in the box (container)?" and "Where has the box been?" will require more information sharing and partnerships between the private sector and the public sector.

Public-private partnerships are becoming more commonplace in the transportation industry, but unique challenges must be addressed when information sharing is being considered. Many private sector entities are concerned about losing their competitive advantage. Additionally, many private companies are concerned that their participation will not provide improved security but only the appearance of security, or that they will not receive intelligence from the public sector. These concerns are not unfounded, as the public sector is often hesitant to give intelligence to the private sector. These issues must be overcome to improve cargo security.

This report presents two strategies that allow for information sharing in ways that addresses the concerns of the private sector. The strategies utilize existing frameworks including freight advisory councils and cargo data collection portals to share information and potentially improve cargo security in the process. The public sector will not have to reinvent the wheel to make these adjustments to respond to cargo security concerns. Past efforts to develop freight transportation plans, to use Intelligent Transportation Systems to collect data and to provide transportation visibility within a network, and to develop transportation strategies will prove helpful to agencies responsible for transportation and security at all levels of government in addressing vulnerabilities in cargo security.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Traditionally, most analysis related to national security and transportation has focused on airports, seaports, and border ports of entry. When narrowing the scope to freight transportation, seaports are viewed as the greatest vulnerability. The main reason for this concern is containerized trade, and answering the question, "What is in the box?" Federal legislation and contemporary analysis has placed an emphasis on the uncertainties of knowing the contents of a container transported by a container vessel operated and owned by a foreign company, and whether the container ever deviated from the planned route or was opened unexpectedly during transit.

A major push for freight and trade security has come from the private sector. In 2006, Charles Raymond, CEO of Horizon Lines, called for increased efforts to secure cargo along with physical and vessel security. He agrees that asking, "What is in the box and where has the box been?" are the more pressing questions than whether container terminals are managed by foreign companies.[1] More information is needed to answer these questions than what current Department of Homeland Security initiatives provide. This report presents strategies using freight advisory councils and cargo data collection portals to address shortfalls in cargo security.

1.1 BACKGROUND

As recent terrorism events in the United States, United Kingdom, and Spain have demonstrated, transportation networks remain a potential target. Freight transportation systems are particularly viewed as vulnerable because of hazardous material shipments. As a result, practice, technology, and communications improvements are seen as a tool to

[1] Charles G. Raymond, "World Trade Security is Imperative and Attainable", *TR News*, September-October 2006, 1

address security concerns. Government agencies, industry, and the public realize that a terrorism event occurring at a major port or at key locations on the nation's highway network will have negative economic and social consequences. For example, Texas not only provides a key entryway for truck traffic from Mexico, but the state also contains one of the nation's leading international seaports. As a result, the state's cargo transportation system must be secured to prevent entry of dangerous materials and to protect its vital links in the global trade network.

In order to achieve this secure network, comprehensive trade security that addresses physical, vessel, and cargo security is needed. Communications and information flow between government and industry is seen as one area where improvements can still be made. Industry officials assert that more information is available from the private sector that is not being used effectively by government agencies. Although shippers and carriers are interested in a more secure global supply chain, they also have hesitations about sharing information with the public sector. Identifying strategies that address the concerns of the private sector while improving cargo security would be a significant step forward in international trade security.

1.2 OBJECTIVES AND WORK PLAN

The goal of this project is to identify strategies for using operational data from industry in public sector security analysis and decision making. Industry officials who have demonstrated a desire to work closely with the government in these initial phases were contacted to ascertain partnership potential. Frameworks and strategies are needed to describe how the operational data utilizing information technologies can be useful for

agencies responsible for securing freight transportation networks and assets. The two strategies presented for this study utilize:

1) Freight advisory councils, and
2) Cargo data collection portals.

The following steps were taken to complete the study.

1. Conducted a literature review on freight transportation planning, intelligent transportation systems, and public-private partnerships related to information exchange between the transportation industry and government agencies.
2. Contacted industry officials who have demonstrated a willingness to provide initiative in improving operational data exchange with CBP.
3. Identified strategies that rely on information sharing with the private sector to address cargo security concerns.
4. Completed a final report detailing study findings.

1.3 ORGANIZATION

The introduction provided a background to outline the relevancy of this study and related issues and presented the study objectives and work plan. Chapter 2 is a literature review on four areas: freight transportation planning, intelligent transportations systems, and public-private partnerships for information exchange, and freight transportation and security strategies. Chapter 3 presents the two strategies to improve trade security with an emphasis on cargo security. The overall approach with steps to accomplish each strategy is discussed. Chapter 4 concludes the report with a discussion on what is needed to make either method a success based on the public-private partnership literature.

CHAPTER 2: LITERATURE REVIEW

Efforts to improve transportation security with an emphasis on freight or international trade security are not a new development. The Clinton administration outlined critical infrastructure that needed security improvements in 1998.[2] Certainly, attention on this issue has risen since 9/11 and recent incidents of terrorism in Europe. Responding to the concerns over international trade security is made possible though by ordinary efforts to meet other challenges associated with freight transportation and international trade. Freight transportation planning is becoming more common in state departments of transportation and metropolitan planning organizations. Technology applications in transportation or Intelligent Transportation Systems (ITS) have been used by industry and standardized by transportation planners. Transportation planners have developed strategies to address a number of transportation issues including freight transportation and homeland security. Public-private partnerships are used in a number of industries, and the experience in transportation and for transportation security has been documented.

2.1 FREIGHT TRANSPORTATION PLANNING

Freight transportation has unique impacts on transportation that require special consideration in the transportation planning process. On most freeways, trucks comprise anywhere from 5 percent to 10 percent of the total traffic, but are responsible for a considerably higher percentage of infrastructure damage. The legal weight limit for a conventional tractor-trailer is 80,000 pounds. Terminal operations produce and attract a high volume of trucks that can lead to unusually high noise and air pollution. Increased

[2]U.S. Department of Justice, "The Clinton's Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63", May 22, 1998, <http://www.fas.org/irp/offdocs/paper598.htm>, (May 31, 2008).

development near freight rail lines is also causing more noise pollution concerns. Container terminals are viewed as a vulnerable site for terrorism. These infrastructure, environmental, and security concerns have led more transportation agencies to conduct goods movement planning.

Metropolitan planning organizations (MPOs) are addressing freight transportation issues in transportation planning and programming. For example, the North Central Texas Council of Governments (NCTCOG) has a goods movement program area within the transportation department. The program area studies freight transportation problems in the Dallas/Fort Worth Region and communicates potential solutions to elected officials through the Regional Transportation Council.[3] The transportation department also has a Transportation Security and ITS Project Implementation program area to coordinate emergency responses and improve transportation security with technology applications. MPOs have a role in securing transportation systems as a planning entity that varies on the phase of a security incident. The phases defined by Meyer are prevention, response/mitigation, monitoring information, recovery, investigation, and institutional learning.[4] A shortfall for MPOs is that goods movement program areas do not necessarily have security as a focus area. The emphasis is typically on transportation issues like mobility and environment. MPOs conduct security planning, but the effort is separate from the goods movement program area.

Statewide freight plans are also becoming more common. The *Minnesota Statewide Freight Transportation Plan* produced by the Minnesota Department of Transportation documents current and future freight flows and identifies freight planning

---

[3] See Transportation Department website for the North Central Texas Council of Governments, (Available at: http://www.nctcog.org/trans/index.asp).

[4] Michael Meyer, "The Role of the Metropolitan Planning Organization in Preparing for Security Incidents and Transportation System Response", (Available: http://www.planning.dot.gov/Documents/Securitypaper.htm). Accessed: May 29, 2008.

policies for the state.[5] This document was the first of its kind for Minnesota. Plans like the MnDOT freight plan describe the freight system and quantify goods movement by mode, region, and commodity. The plan even introduces the idea of working with the private sector.[6] The main reason given for private-public partnerships is infrastructure investment. Security does not have a prominent role in the MnDOT freight plan. A survey of state freight plans was not conducted for this study, but given that MnDOT is on the cutting edge of freight planning, the assumption is made that few if any states have incorporated freight security in freight planning efforts.

The California Department of Transportation (Caltrans) has also developed statewide freight policy objectives. Like Minnesota, security policy objectives were not included. Policy objectives included safety, reliability, mobility, accessibility, equity, economic well being, and environmental quality. Each of these policy objectives had associated performance measures.[7] Although freight security is not explicitly incorporated in the freight plans, the framework that developed these plans will be helpful in incorporating new strategies.

Nationally, the FHWA has partnered with the American Transportation Research Institute to measure truck travel times on interstates using global positioning systems.[8]

---

[5] Minnesota Department of Transportation. *Minnesota Statewide Freight Plan.* May 2005. Online. Available: http://www.dot.state.mn.us/ofrw/PDF/MN_SFP_Final_Report_05.pdf. Accessed December 8, 2007.

[6] Minnesota Department of Transportation, 5-8.

[7] Booz-Allen & Hamilton Inc. *Transportation System Performance Measures Compendium of Phase II Results.* California Department of Transportation. June 30, 1999. http://www.dot.ca.gov/hq/tsip/tspm/tspmpdf/pm6_99comp2.pdf. Accessed: July 21, 2006.

[8] Federal Highway Administration. *Freight Performance Measurement: Travel Time in Freight Significant Corridors.* Online. Available: http://www.ops.fhwa.dot.gov/freight/freight_analysis/perform_meas/fpmtraveltime/index.htm. Accessed: December 8, 2007.

Figure 1 shows a map color coding truck speeds on Interstate 10 developed through the analysis. Harrison et. al. reviewed FHWA and ATRI efforts and concluded that the initiative provided important data and would be useful for freight and general transportation planning.[9] Fundamentally, the work between FHWA and ATRI was a public-private partnership that utilized global positioning systems (GPS) to determine travel times for interstate corridors. ATRI had been given access to motor carrier data and the opportunity to analyze the data with assurances that individual motor carriers participating in the study would remain anonymous. The rise in freight planning efforts affects solutions offered by transportation planning agencies. More proposals that center on addressing freight transportation problems from the public sector are being considered as a result.

Figure 2.1. Truck Average Speed on Interstate 10.

[9] Robert Harrison, Mike Schofield, Lisa-Loftus Otway, Dan Middleton, and Jason West, *Developing Freight Highway Corridor Performance Measure Strategies in Texas*, Research Report 5410-1, 2006, 66.

2.2 INTELLIGENT TRANSPORTATION SYSTEMS

Intelligent Transportation Systems (ITS) are central to freight planning and general transportation planning. The use of loop detectors, GPS, and radio frequency identification (RFID) are becoming more common place in transportation. Transportation agencies have commonly used loop detectors to provide information to motorists. Transguide in San Antonio and Transtar in Houston are two ITS management systems in Texas that utilize loop detectors to provide travel times through dynamic message signs on major freeways.[10]

The information collected by these systems provides general travel times combining all vehicles. The emergence of freight transportation planning will require data for freight vehicles only that also captures intercity portions of trips. Technologies that have been tested to provide this information and support freight performance measure systems include GPS, RFID, and cellular phones. Harrison et. al. reviewed pilot tests for these technologies and evaluated how these technologies would work for Texas freight transportation planning efforts. Given the results of the tests, the study determined that the most applicable technologies were GPS, RFID, and cellular phones in decreasing usefulness.[11] This order could change when considering certain applications more specifically. For example, in Texas, regulatory agencies have not participated in electronic clearance programs that utilize RFID. Currently, the infrastructure is not in place to use RFID, so cellular phones would be more applicable. States that have extensive toll networks with RFID infrastructure and automated vehicle identification

[10] See website for each management system with Transguide at http://www.transguide.dot.state.tx.us/ and Transtar at http://traffic.houstontranstar.org/layers/.

[11] Robert Harrison, Mike Schofield, Lisa-Loftus Otway, Dan Middleton, and Jason West, *Developing Freight Highway Corridor Performance Measure Strategies in Texas*, Research Report 5410-1, 2006, 66.

(AVI) readers placed on non-toll highways would probably favor RFID over other sources.

Although many of the ITS applications have not been used for security purposes, these technologies will be necessary for when government agencies decide to enter into public-private partnerships with private sector transportation providers for security information sharing purposes. Horizon Services Group (HSG), a company that specializes in using advanced information technologies for the transportation industry and is a part of Horizon Lines, has demonstrated that similar technologies can produce information that is useful for both mobility and security freight policy objectives. HSG partnered with the Alaska Department of Transportation to deliver an RFID project. The purpose of the project was to provide visibility for container shipments throughout the state using RFID.[12] Visibility is also a security objective, and HSG partnered with the Port of Jacksonville to develop intermodal container tracking abilities using RFID.[13] Developing strategies that address cargo security will rely on information available through ITS systems owned by the private sector. Government agencies will have to develop public-private partnerships to obtain this data.

Using ITS applications in public-private information exchanges does not come without challenges. The primary challenge is properly acquiring, distributing and analyzing the data. In other words, the government agency must not lose the trust of its private sector partner. Some concerns outlined by Briggs and Walton regarding ITS data received by the public sector agency from the private sector include data anonymity, that the data is not used for enforcement or litigation against the private company, and that the

[12] Horizon Lines, "Alaska Division RFID Project: Concept of Operations", April 21, 2006, 1.

[13] Horizon Services Group, "Port of Jacksonville: Intermodal Container Tracking Project," September 2007. Presentation.

data will not be used for other purposes known as data creep.[14] The Intelligent Transportation Society of America's *Intelligent Transportation Systems Fair Information and Privacy Principles* can help transportation professionals responsible for sharing information for security purposes ensure the privacy and trust of their partners.[15]

2.3 PUBLIC-PRIVATE PARTNERSHIPS FOR FREIGHT SECURITY

Public-private partnerships are already used extensively in many sectors including transportation. These partnerships provide services, information, and financing. In the context of freight security, private-public partnerships are primarily about jointly providing security and information exchange. The responsibilities, opportunities, and challenges for public-private partnerships related to information sharing to support homeland security initiatives.

Public-private partnerships are founded on the basis that each partner has a responsibility. Security is a public good, and government is responsible for providing that good. As with any public good, the possibility for free-riding exists by transportation carriers and shippers, and the government can minimize its responsibility. Flynn argues that the Bush administration has made the private sector primarily responsible for security because of the belief that incentives exist in the market for the transportation industry to provide its own security.[16] Government agencies must realize that the private sector does not necessarily agree with this view.

Many obstacles make the private sector hesitant to make security investments and provide information to the government. Flynn summarizes the issues that deter the

---

[14] Valerie Briggs and C. Michael Walton, (2000), *The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data*, Research Report 472840-00075, 10-12.

[15] Briggs and Walton, 33.

[16] Stephen Flynn, *The Edge of Disaster*, (New York: Random House, 2007), 139.

private sector from making investments and working more closely with the public sector. First, the private sector is concerned that security investments will become obsolete with new laws passed by Congress in response to security incidents.[17] The private sector often finds that sharing information is a one-way exchange.[18] Governments are just as hesitant to provide threat information as the private sector is to offer information on its business activity. In addition, a security incident will likely occur where the freight transportation and international trade system is most vulnerable.[19] This vulnerability will probably be due to a member of the public sector or private sector not investing appropriately in security initiatives. The problem develops when companies that did make security investments are negatively affected by those companies that had vulnerable supply chains. Finally, the private sector is concerned that security investments that are not made by its competition or information exchange that is not properly secured by the government could lead to a competitive disadvantage.[20]

Branscomb and Michel-Kerjan add to this issue by pointing out that competitive advantage could be lost if the information being shared is proprietary.[21] Private companies may not also be able to participate because they have entered into agreements with clients not to share information. Industry officials want everyone to make similar investments to not incur costs that competitors do not make. Prieto provides even more concerns. First, it is not always clear with whom the private sector should share

---

[17] Stephen Flynn, 137.

[18] Ibid., 147.

[19] Ibid., 138.

[20] Ibid., 138.

[21] Lewis M. Branscomb and Erwann O. Michel-Kerjan, "Public-Private Collaboration on a National and International Scale" in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan, 398 (New York: Cambridge University Press, 2006)

information, leading to a confusing and frustrating experience for both the public and private sector.[22] Private companies are also concerned that they will be held liable for how the public sector uses the information. Finally, similar to the view that sharing information is mainly a one-way street, Prieto expresses that private companies do not always see the benefit in sharing information with the government.

Government agencies must take the initiative to overcome these hurdles and issues that the private sector has with information sharing. Before a government agency can take action, it must address the foundation of the partnership identified by Branscomb and Michel-Kerjan: trust. Trust is developed through information sharing.[23] Flynn includes information sharing in his three approaches that government agencies can use to address constraints for private sector involvement. First, government agencies must be more willing to share information, especially threat information.[24] The federal government must accept standards that are developed with an understanding of the industry and its perspective of the standards.[25] These standards must not just give the appearance of security but produce security in fact. Finally, Congress and government agencies need to resist changing laws and standards due to pressure from the aftermath of a security incident. The role of the federal government "…should be leading a truly

---

[22] Daniel B. Prieto III, "Public-Private Collaboration on a National and International Scale" in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan, 410 (New York: Cambridge University Press, 2006)

[23] Lewis M. Branscomb and Erwann O. Michel-Kerjan, "Public-Private Collaboration on a National and International Scale" in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, ed. Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan, 395 (New York: Cambridge University Press, 2006)

[24] Stephen Flynn, *The Edge of Disaster*, (New York: Random House, 2007), 138.

[25] Stephen Flynn,139.

collaborative national effort that taps extensive private-sector capabilities and assets in the face of ongoing risks of disasters."[26]

2.4 FREIGHT SECURITY AND THE TRANSPORTATION PLANNING PROCESS

Strategies are needed to successfully develop capabilities within government agencies to monitor cargo security. These strategies are needed because government agencies have not been able to incorporate security into the long term transportation planning process as effectively as other objectives like mobility and safety. Dornan and Maier believe that local planning organizations like MPOS have not been able to incorporate security as easily due to institutional culture.[27] Local transportation planning agencies rely on local law enforcement and emergency personnel to address security issues and that the federal government will address homeland security concerns. Transportation planning departments and goods movement program areas need senior leadership that is committed to security as an objective for the department and program area. Dornan and Maier state, "The lack of senior level sponsorship for security considerations in the planning and development of transportation programs and projects has left security in the shadows of safety…security remains more of an echo than a tangible consideration on its own merits in the development of traditional transportation program plans."[28] Other reasons that the authors give for the lack of freight security strategies is the lack of data and security performance measures.

The strategies in this report are intended to address this issue, but the question remains on what should be included in the strategies. The *Guidebook for Integrating*

---

[26] Ibid., 141.

[27] Daniel L. Dornan and M. Patricia Maier, "Incorporating Security into the Transportation Planning Process" in *Surface Transporation Security*, NCHRP Report 525, (Washington, D.C.: TRB, 2005), 19.

[28] Doman and Maier, 19.

Freight into Transportation Planning and Project Selection Processes was used to determine the components of a strategy. The strategies had five elements: Overview, Key Steps, Data Needs and Other Supporting Resources, Case Study Example, and Strategies to Link to the "Traditional" Process.[29] The strategies are rated on whether freight data is needed, how much involvement is needed from the private sector, how much knowledge on the industry is needed in the public sector, and whether strong support for freight planning is needed.[30] This approach for defining strategies is used to some extent in this study. Differences between this study and Cambridge Systematics, Inc. et. al.'s work include that a case study is not done for either strategy although context for the strategy is established using examples from the practice. Emphasis is also not given to linking to the "traditional" process. Therefore, only the first three elements will be examined in this report: Overview, Key Steps, and Data Needs.

[29] Cambridge Systematics, Inc., Prime Focus, LLC and Kevin Heanue, *Guidebook for Integrating Freight into Transportation Planning and Project Selection Processes,* NCHRP Report 594, (Washington, D.C.: TRB, 2007), 21.
[30] Cambridge Systematics, Inc., Prime Focus, LLC and Kevin Heanue, 22.

CHAPTER 3: CARGO SECURITY STRATEGIES

The goal of this project is to identify strategies for using operational data from industry in public sector security decision making. The use of this data should accomplish security objectives for both the public and private sector. The main objective is shipment visibility. Shipment visibility can be obtained through GPS and RFID technologies. Cargo theft is the most common security related problem that shippers and carriers face today. Less common but arguably more problematic is detecting when freight shipments are being used for terrorism. The private sector has the capability to know where its freight is at all times. The public sector does not have full access to this proprietary information but can receive summaries of the compiled information and more specific information when necessary. Strategies are needed to make the data transfer from the private sector to the public sector. These strategies address different aspects of cargo security and provide information at different timetables. Nevertheless, each strategy is useful at the providing the overall objective of visibility through information sharing. The approaches are developed to specifically address cargo theft and terrorism that involves freight shipments. The strategies also utilize existing institutions to avoid "reinventing the wheel." Instead, the goal is to shape these institutions that have been developed for freight transportation planning purposes and physical security of freight facilities to also consider cargo security.

3.1 FREIGHT ADVISORY COUNCIL

Freight advisory councils are becoming more common place in MPOs. NCTCOG and the Southern California Association of Governments (SCAG) use these groups to hear from the private sector on transportation issues that involve the freight community and to integrate freight issues into long-term transportation planning. As mentioned

earlier, freight advisory councils rarely address security issues and, even less so, cargo security. A strategy that uses these important institutions is needed to improve cargo security that utilizes an existing form of a public-private partnership. Table 3.1 identifies the overall steps to this strategy.

3.1.1 Strategy Overview

Security should be added as new objective for local/regional freight planners monitored by a freight advisory council. Cargo theft is the primary issue related to security for freight stakeholders followed by terrorism. Adding security to the council's objective may increase participation because of the potential to produce intelligence that carriers and shippers do not have locally. Cargo theft rarely makes the local news and freight stakeholders in large regions may not be aware of regional and statewide vulnerabilities. Members to the council will be asked to provide information on cargo theft and security issues. MPO staff will corroborate data to produce reports and quarterly updates on cargo security within the MPO jurisdiction. The use of geographic information systems would provide a useful mechanism to display the location of cargo theft in the region.

3.1.2 Key Steps

Four steps are needed to accomplish this strategy: identify more participants, establish a security objective, develop regular agenda items, and monitor cargo security. Some MPOs like SCAG and NCTCOG have developed freight advisory councils. Participation at these meetings will largely depend on the agenda and commitment that members of the private sector have to public-private partnerships. Broad participation of shippers, transportation providers, and terminal operators is needed to accomplish the

security objective of increasing freight visibility and cargo theft vulnerabilities within the MPO jurisdiction. Too often, participation at these meetings is limited to major stakeholders and MPO staff.[31] The advisory councils also need to establish a security objective. The overall concern found in the literature for cargo security is cargo visibility and making cargo theft more difficult. The freight advisory council and goods movement program area can establish a close working relationship with security program areas within the MPO but outside of program area for assistance in accomplishing the objectives. Once participants are committed and security objectives are established, regular meeting agenda item can be developed. Potential agenda items can address physical facility security but the emphasis should be placed on cargo security and preparing feedback for the participants on information gathered from all participants. Taking this step will assure the private sector participants that the MPO is interested in security, in fact, and not just in the appearance of security. Finally, the goods movement program area can establish GIS maps that identify where security incidents occur and distribute the findings to members of the advisory council. Monitoring cargo security issues across all freight modes may require dedicated staff resources and interaction with law enforcement, federal agencies, and local industry members. Dealing with these issues will help the members of the freight advisory council to be prepared for major events other than cargo theft, when the possibility still exists that terrorism in the freight sector may occur with cargo theft first.

[31] See SCAG's Goods Movement Program Webpage to view meeting rosters and agenda items for the SCAG Goods Movement Task Force.

Table 3.1. Freight Advisory Council Strategy

Action Item	Description
Step 1. Identify more participants	Incorporate a variety of shippers, transportation providers, and terminal operators to be involved.
Step 2. Establish security objective	Cargo visibility and theft reduction should be an area of concern.
Step 3. Develop regular agenda items	Program area staff can establish regular agenda items that communicate that cargo security and more generally
Step 4. Monitor cargo security incidents	Program area staff should track and report cargo theft incidents within there jurisdiction

3.1.3 Data Requirements

Data needs for this strategy will be identifying participants and arranging a way for stakeholders to provide information on security incidents that occur in the region including cargo theft or lost freight. Since MPOs vary widely, the guidelines for sharing information between the private sector and the MPO should be left flexible, but the process may be helped by having similar procedures as the Information Sharing and Analysis Centers.[32]

3.2 CARGO ELECTRONIC DATA COLLECTION PORTAL

Current U.S. DHS initiatives place an emphasis on physical and vessel security. In global shipping, answering the question, "What is in the box?" requires more information. The most pressing information needed is the identification of the box not only when it arrives or leaves a container terminal and when it will arrive at an U.S. port.

[32] See the Surface Transportation Information Sharing and Analyis Center at http://surfacetransportationisac.org/.

Port authorities improving physical security and shippers and carriers participating in U.S. DHS initiatives all help address cargo security but do not deliver end-to-end visibility. End-to-end visibility means that all container transactions are recorded and tracked according to an established trip plan.

3.2.1 Strategy Overview

The Horizon Services Group is a division of Horizon Logistics, LLC that has developed a method to provide end-to-end visibility to provide more complete cargo security through information available from carrier and shippers. Horizon Services Group calls the concept the "Electronic Data Collection Portal."[33] The strategy receives information from all partners and transportation providers and compares so that information is received on a real time basis. The approach establishes a container tracking system for security objectives.

3.2.2 Key Steps

The steps for this strategy were outlined by Horizon Services Group in a January 2008 presentation about their pilot tests for the container tracking system they were creating for the Port of Jacksonville or Jaxport. Those steps were:

- *Establish a central information repository for all information relative to cargo movement*
- *Set up electronic feeds (EDI) which already exist in much of the transportation industry*
- *Acquire information from all modes of transport and transportation partners*
- *Apply business rules which would generate alerts associated with freight, carriers and/or operators requiring inspection or contacting.*[34]

[33] Horizon Services Group, "Cargo Security: The Jaxport Approach," January 28, 2008. Presentation.

[34] Horizon Services Group, January 28, 2008. Presentation.

3.2.3 Data Requirements

The data needed for this strategy is the updated location of the container and the originally scheduled trip plan. Carrier participation is a requirement for this strategy. Ideally, the data Horizon Services Group needed to accomplish the strategy were:

- *Truck Gate-In/Gate-out*
- *Vessel Load/Unload*
- *Vessel Schedule*
- *Booking and Manifest*
- *Submit Tonnage*[35]

The data is used to update trip activity and to compare the trip in real-time against the trip plan. The alerts produced provide information on when the container is leaving the terminal or container freight station and is in route to the port. Alerts will be received on vessel activity and when the vessel arrives in port. In short, the container tracking project provides end-to-end visibility that current initiatives from the U.S. DHS do not allow.

[35] Horizon Services Group, "Port of Jacksonville: Intermodal Container Tracking Project," September 2007. Presentation.

CHAPTER 4: CONCLUSIONS

Strategies to address cargo security vulnerabilities must consider the challenge of obtaining information from the private sector. Some strategies like the freight advisory council may not require significant up front investments, but strategies like the container tracking project will more than likely require major up front investments. Before adopting a strategy, the commitment level of the private partners to share information must be evaluated. More commitment from the private sector may be needed before adopting certain strategies.

A hesitant private sector partner has legitimate concerns that the public sector can address through well-crafted strategies. The strategies must not threaten the competitive advantage that a company may have spent many years developing. The public sector must not use the information for more than what it was originally intended. The government agency needs to also have ideas of what information or intelligence it can provide to the private partner for their participation and end the "one-way street" of information exchange experienced by many in the private sector. Government agencies need to be specific when requesting information from the private sector and only ask for what it needs.

Research that gathers the input from both private and public sector representatives will help further develop the strategies suggested in this report. The general strategies need to be presented to these representatives to understand what views they have on improving cargo security, but whatever approaches are accepted, delays for implementation should be avoided. Lessons learned from implementation will provide the most useful feedback as government agencies and the private sectors partner to address cargo security.

REFERENCES

Booz-Allen & Hamilton Inc. *Transportation System Performance Measures Compendium of Phase II Results.* California Department of Transportation. June 30, 1999. Available at: http://www.dot.ca.gov/hq/tsip/tspm/tspmpdf/pm6_99comp2.pdf.

Cambridge Systematics, Inc., Prime Focus, LLC and Kevin Heanue. *Guidebook for Integrating Freight into Transportation Planning and Project Selection Processes,* NCHRP Report 594. Washington, D.C.: TRB, 2007.

Dornan, Daniel L. and M. Patricia Maier. "Incorporating Security into the Transportation Planning Process" in *Surface Transporation Security*. NCHRP Report 525. Washington, D.C.: TRB, 2005.

Lewis M. Branscomb and Erwann O. Michel-Kerjan. "Public-Private Collaboration on a National and International Scale" in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, edited by Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan, 395-403. New York: Cambridge University Press, 2006.

Briggs, Valerie and C. Michael Walton. *The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data*. Research Report 472840-00075. 2000.

Federal Highway Administration. *Freight Performance Measurement: Travel Time in Freight Significant Corridors.* Online. Available at: http://www.ops.fhwa.dot.gov/freight/freight_analysis/perform_meas/fpmtraveltime/index.htm.

Flynn, Stephen. *The Edge of Disaster*. New York: Random House, 2007.

Harrison, Robert, Mike Schofield, Lisa-Loftus Otway, Dan Middleton, and Jason West. *Developing Freight Highway Corridor Performance Measure Strategies in Texas*. Research Report 5410-1. 2006.

Horizon Lines. "Alaska Division RFID Project: Concept of Operations." April 21, 2006.

Horizon Services Group. "Port of Jacksonville: Intermodal Container Tracking Project." September 2007. Presentation.

Horizon Services Group "Cargo Security: The Jaxport Approach." January 28, 2008. Presentation.

Meyer, Michael. "The Role of the Metropolitan Planning Organization in Preparing for Security Incidents and Transportation System Response." Available at: http://www.planning.dot.gov/Documents/Securitypaper.htm.

Minnesota Department of Transportation. *Minnesota Statewide Freight Plan.* May 2005. Available at: http://www.dot.state.mn.us/ofrw/PDF/MN_SFP_Final_Report_05.pdf.

Prieto III, Daniel B. "Public-Private Collaboration on a National and International Scale" in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, edited by Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, Erwann O. Michel-Kerjan, 404-428. New York: Cambridge University Press, 2006.

Charles G. Raymond, "World Trade Security is Imperative and Attainable," *TR News*, September-October 2006, 18-23.

Siperco, Ian (2006) "Marshalling the Great Arsenal of Democracy: Engaging the Private Sector to Secure the Public Good," *Journal of Homeland Security and Emergency Management*: Vol. 3 : Iss. 4, Article 5. Available at: http://www.bepress.com/jhsem/vol3/iss4/5.

U.S. Department of Justice. "The Clinton's Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." May 22, 1998. Available at: http://www.fas.org/irp/offdocs/paper598.htm.