



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**PUBLIC/PRIVATE PARTNERSHIPS WITH HAZARDOUS
MATERIAL MOTOR CARRIERS: CREATING
INCENTIVES TO INCREASE SECURITY THROUGH
ASSESSED RISK (STAR)**

by

Andrew E. Colsky, Esq.

December 2008

Thesis Advisor:
Second Reader:

Lauren Wollman
Thomas Mackin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Public/Private Partnerships with Hazardous Material Motor Carriers: Creating Incentives to Increase Security through Assessed Risk (STAR)			5. FUNDING NUMBERS	
6. AUTHOR(S) Andrew E. Colsky, Esq.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) On September 11, 2001, terrorists used commercial airliners as weapons of terror inside the United States, and America's approach to security was forever changed. While commercial airliners were the weapons of choice on that day, the 9/11 Commission recognized that Al Qaeda and other groups had, prior to the use of airlines, used suicide vehicles, namely, truck bombs, to commit terrorist acts. The threat from hazmat trucks continues today. There can be no doubt that terrorists are interested in using hazmat trucks as weapons within the borders of the United States. In 2004, Defense Secretary Donald Rumsfeld's visit to Iraq was punctuated by a fuel-truck attack that burned a section of Baghdad. More recently, terrorists in Iraq have used chlorine-based truck bombs repeatedly as a weapon in the Iraq war. The Department of Transportation (DOT) recognizes that hazmat trucks are "dangerous and ready-made weapons" and are "especially attractive" to terrorists. Stephen Gale, a University of Pennsylvania professor and terrorism expert, agrees that hazmat trucks are essentially ready-made bombs that are "tailor-made" for terrorists to conduct an attack at the lowest cost and with the greatest impact. In fact, terrorism experts consider trucks to be one of the best tools a terrorist can use to breach security measures and carry explosives since the U.S. airline industry significantly increased security procedures. The ability of the government to secure every hazardous materials motor carrier against terrorist attack is severely limited, yet the potential that hazardous materials trucks will be used in terrorist attacks is great. Therefore, it is important to consider whether the security of hazardous materials motor carriers can be improved voluntarily and quickly by realigning existing resources and instituting a plan that leverages market forces and other incentives. This thesis introduces a unique voluntary incentive-based program, Security Through Assessed Risk (STAR) that can be used to increase security for a vast number of presently under protected hazardous materials motor carriers. It explains how TSA can leverage existing resources as well as successful ideas from both private sector and governmental programs to rapidly and significantly enhance the security of hazardous materials motor carriers.				
14. SUBJECT TERMS Hazardous Materials Motor Carrier, Motor Carrier, Trucking, Hazardous Materials, Hazmat, Incentive, Partnership, Public/Private, Voluntary, Security, Risk Assessment			15. NUMBER OF PAGES 109	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**PUBLIC/PRIVATE PARTNERSHIPS WITH HAZARDOUS MATERIAL
MOTOR CARRIERS: CREATING INCENTIVES TO INCREASE SECURITY
THROUGH ASSESSED RISK (STAR)**

Andrew E. Colsky, Esq.
Civilian, Director of the Sensitive Security Information Office for the Transportation
Security Administration
B.A., University of Florida, 1986
J.D., University of Florida, 1989
LL.M. in Litigation, Emory University School of Law, 1990

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2008**

Author: Andrew E. Colsky, Esq.

Approved by: Lauren Wollman
Thesis Advisor

Thomas Mackin
Second Reader

Harold A. Trinkunas
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

On September 11, 2001, terrorists used commercial airliners as weapons of terror inside the United States, and America's approach to security was forever changed. While commercial airliners were the weapons of choice on that day, the 9/11 Commission recognized that Al Qaeda and other groups had, prior to the use of airlines, used suicide vehicles, namely, truck bombs, to commit terrorist acts.

The threat from hazmat trucks continues today. There can be no doubt that terrorists are interested in using hazmat trucks as weapons within the borders of the United States. In 2004, Defense Secretary Donald Rumsfeld's visit to Iraq was punctuated by a fuel-truck attack that burned a section of Baghdad. More recently, terrorists in Iraq have used chlorine-based truck bombs repeatedly as a weapon in the Iraq war.

The Department of Transportation (DOT) recognizes that hazmat trucks are "dangerous and ready-made weapons" and are "especially attractive" to terrorists. Stephen Gale, a University of Pennsylvania professor and terrorism expert, agrees that hazmat trucks are essentially ready-made bombs that are "tailor-made" for terrorists to conduct an attack at the lowest cost and with the greatest impact. In fact, terrorism experts consider trucks to be one of the best tools a terrorist can use to breach security measures and carry explosives since the U.S. airline industry significantly increased security procedures.

The ability of the government to secure every hazardous materials motor carrier against terrorist attack is severely limited, yet the potential that hazardous materials trucks will be used in terrorist attacks is great. Therefore, it is important to consider whether the security of hazardous materials motor carriers can be improved voluntarily and quickly by realigning existing resources and instituting a plan that leverages market forces and other incentives.

This thesis introduces a unique voluntary incentive-based program, Security Through Assessed Risk (STAR) that can be used to increase security for a vast number of presently under protected hazardous materials motor carriers. It explains how TSA can leverage existing resources as well as successful ideas from both private sector and governmental programs to rapidly and significantly enhance the security of hazardous materials motor carriers.

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	IDENTIFY PROBLEM.....	1
II.	TRANSPORTATION SECURITY	3
A.	AVIATION SECURITY	3
B.	HAZARDOUS MATERIALS MOTOR CARRIER SECURITY	4
1.	Context	4
2.	Statistics	7
C.	SUMMARY	7
1.	Research Question	8
2.	Methodology	8
3.	Literature Review	9
III.	RECOGNITION OF THE THREAT	19
A.	PRESIDENTIAL ACTION.....	19
1.	Homeland Security Presidential Directive Number 7	19
2.	Executive Order 13416	20
B.	TRANSPORTATION SECURITY ADMINISTRATION ACTION.....	22
1.	Testimony before Subcommittee on Homeland Security of the Committee on Appropriations of the United States House of Representatives	22
2.	Testimony before the United States Senate Committee on Commerce, Science, and Transportation.....	23
C.	SUMMARY	23
IV.	CLARIFYING ROLES	25
A.	DHS AND DOT	25
B.	SUMMARY	26
V.	ACTIONS ACCOMPLISHED	27
A.	CONGRESSIONAL ACTION	27
1.	The USA PATRIOT Act of 2001	27
2.	The 9/11 Commission Act of 2007	27
a.	<i>Truck Security Assessment.....</i>	<i>28</i>
b.	<i>Memorandum of Understanding</i>	<i>28</i>
c.	<i>Report on Trucking Security Grant Program.....</i>	<i>28</i>
d.	<i>Hazardous Materials Highway Routing</i>	<i>28</i>
e.	<i>Security-Sensitive Material Tracking.....</i>	<i>29</i>
f.	<i>Hazardous Materials Security Inspections</i>	<i>30</i>
3.	Hazardous Materials Endorsements and Transportation Worker Identification Credential.....	30
B.	DOT ACTIONS.....	31
1.	Safety and Security Plans	31
2.	Security Sensitivity Visits	32

3.	Hazardous Materials Safety Permits	33
4.	Technological Solutions for Hazmat Truck Security	33
a.	Wireless Satellite and Terrestrial Communications Systems	34
b.	Digital Pone without GPS.....	34
c.	Panic Buttons	35
d.	Global Login.....	36
e.	Biometric Global Login	36
f.	Electronic Supply Chain Manifest	37
g.	Intelligent On-Board Computers Initiating Remote Vehicle Disabling	38
h.	Internal Trailer Door Locking System.....	39
i.	External Electronic Seal.....	39
j.	Geofencing	40
k.	Tethered Trailer Tracking	40
l.	Untethered Trailer Tracking	41
m.	Overall Results	41
C.	TSA ACTIONS.....	44
1.	Corporate Security Reviews.....	44
2.	Security Grants	45
3.	Truck Tracking Pilot	46
4.	Security Action Items	49
D.	SUMMARY	51
VI.	GAP ANALYSIS	53
A.	IDENTIFIED GAPS	53
1.	Non-HSSM Haulers	53
2.	Security Action Items	54
3.	Statistics	54
4.	Grant Money	55
5.	Inclusiveness	55
6.	Duplicative Regulatory Requirements.....	56
B.	SUMMARY	56
VII.	PRIVATE SECTOR PROGRAMS.....	57
A.	RESPONSIBLE CARE®	57
B.	RESPONSIBLE DISTRIBUTION PROCESS SM	59
C.	SUMMARY	61
VIII.	GOVERNMENT INCENTIVE PROGRAM MODELS	63
A.	GOVERNMENT STAR PROGRAMS	63
1.	Energy Star.....	64
2.	OSHA Star	65
B.	OTHER GOVERNMENTAL INCENTIVE PROGRAMS	68
1.	National Park Service Historic Preservation Tax Incentives	69
2.	Virginia's Enterprise Zone Program	70
3.	Free and Secure Trade	70

4.	Port Security Grants Program	72
C.	SUMMARY	73
IX.	SOLUTION	75
A.	SECURITY THROUGH ASSESSED RISK (STAR) PROGRAM.....	75
B.	REQUIREMENTS TO EARN STAR STATUS	75
C.	BENEFITS TO PARTICIPANTS	77
D.	BENEFITS TO THE GOVERNMENT	79
X.	POST-SOLUTION (THE DAY AFTER)	83
	LIST OF REFERENCES	85
	INITIAL DISTRIBUTION LIST	91

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	NIPP Risk Management Framework	20
-----------	--------------------------------------	----

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Overall Results.....	43
----------	----------------------	----

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I must acknowledge my friends and family for their unwavering support throughout my Master's program and during the drafting of this thesis. My mother, Irene and father, Jacob, both highly regarded and successful individuals, instilled in me the importance of education and the need to keep challenging myself and moving forward. While I can never achieve all that they have achieved, I know I must continue to think, innovate, try a lot, fail a lot, learn, succeed as often as possible and repeat the cycle.

I wish to also acknowledge the leadership of the Transportation Security Administration for affording me the opportunity to pursue my education and for supporting me throughout my Master's program. My supervisor Kimberly Walton paved the way for my success by supporting my challenging schedule. Bill Arrington, General Manager, TSA Highway and Motor Carrier Programs supported my research by providing me the benefit of his experience as well as his professional time and friendship.

The entire staff of the Sensitive Security Information Office, my second family, worked hard, maintained a superior work product and supported each other during my many absences while I attended school. Individually and collectively they are high achieving, innovators and their positive attitude and perseverance to always 'find a way or make a way' helped guide me through the tougher times. I have no doubt that some of them feel as if they lived the experience with me.

No acknowledgement would be complete without a thank you to my new friends and teachers whom I met in my program. All of the members and educators of Cohort 0703/0704 have always been supportive, helpful and have proven they will always go above and beyond. As an American, I truly feel safer knowing the caliber of individuals that support our homeland's security.

A special acknowledgement goes to the Homeland Security Digital Library staff and its excellent content manager Greta Marlatt. It can be very difficult to find information about an emerging field like homeland security, but no matter the question, I

received full support on this project. And finally, I must give a big thank you to my primary thesis advisor Lauren Wollman. Lauren was always there for me through the good times and the bad. She helped me to keep my focus and provided assurance when all seemed to be going awry. Her knowledge, skill and good natured friendship, were essential elements to my success.

I. INTRODUCTION

A. IDENTIFY PROBLEM

It's 9:15 am on black Friday, 2009. Shoppers have been lined up at the malls since 7:30 am to take advantage of the special offers the retailers have advertised as incentives to encourage a full day of shopping. The malls are crowded and the holiday season has been festive.

It's 9:15 am on black Friday, 2009. Bud Wilson pulls his fuel tanker into a Shell station to make his first delivery for the day. He parks his truck near the fuel tanks and gets out to meet with the station manager to get his manifest signed.

It's 9:15 am on black Friday, 2009. Adham has been waiting by the pay phone for Bud to arrive. Bud always delivers on Friday and always on time. Adham quietly walks over to the unattended fuel truck, hops in the driver's seat, and proceeds to drive off.

Bud sees his truck is moving and begins to run towards it. By the time he gets to where the truck was, it is already too late. The truck is well on its way down the road. Bud quickly runs back to the station manager and tells him to call the police. The station manager calls 9-1-1 and Bud reports the theft. Bud is distraught and is not sure what to do next so he calls his supervisor.

While Bud was making calls, Adham completes his short trip to the mall and stops the truck outside the floor to ceiling glass walls of the mall's food court. The food court is crowded because the early shoppers have decided to stop for a break and newly arriving shoppers are eating breakfast. It is a good day for Adham, his plan has worked well. He has trained well and waited a long time for this day, the day he becomes a martyr. He reaches for the trigger to the suicide vest he is wearing and flips the switch. Adham knows that he will soon be joining the four other terrorist cell members who repeated the same plan in coordinated attacks in four other major American cities.

Almost a month later, on Christmas day, children all over America are met by scarce gifts under their trees because their parents were too afraid to go shopping. Retailers all across the country are reeling from their worst holiday season ever, and some are considering filing for bankruptcy. Even worse is the number of families who are suffering from the effects of the layoffs at the malls. Bills go unpaid, foreclosures are on the rise yet again, and the American government can place blame on no country. These events occurred not because of a lack of imagination; the government knew of the threat. These events occurred because the American government failed to act.

II. TRANSPORTATION SECURITY

A. AVIATION SECURITY

On September 11, 2001, the United States was attacked when a radical Islamic terrorist organization, Al Qaeda, sent nineteen followers on a suicide mission to hijack four domestic U.S. airplanes and crash them into the World Trade Towers in New York City and the Pentagon in Washington, D.C.¹ These buildings represented American culture and values and were recognized around the world. For purposes of this thesis, it is not as important to understand Al Qaeda as it is to understand the tactics it used to carry out its attack and America's lack of preparation for such an attack.

When the dust had settled, the United States Congress and President George W. Bush created the National Commission on Terrorist Attacks Upon the United States commonly known as the 9/11 Commission. This Commission was given the mandate to investigate "facts and circumstances relating to the terrorist attacks of September 11, 2001."² As a result of its investigation, the Commission found that one of the main reasons they believed that terrorists were able to use commercial aircraft as weapons against the United States was due to a failure of imagination.³ The report elaborated further that "imagination is not a gift usually associated with bureaucracies."⁴

If the events of 9/11 occurred in part due to a lack of imagination, because nothing of the sort had ever happened in the past, then once America had knowledge that terrorists would use airplanes in terror attacks, it becomes incumbent upon America to act so that similar events can never happen again. In response to these terror attacks, the President created the U.S. Department of Homeland Security (DHS) and specifically, the

¹ A fourth airplane did not make it to its intended target (to date still unknown) as the hijackers were overpowered by the passengers and the plane crashed into a field in Shanksville, Pennsylvania.

² National Commission on Terrorist Attacks upon the United States, preface to *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004), xv.

³ National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004), 339.

⁴ *Ibid.*, 344.

Transportation Security Administration (TSA). The Transportation Security Administration's stated mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce.⁵ As a result, numerous new initiatives have been developed to protect commercial airline passengers including federalization and enhancement of the passenger and cargo screening processes as well as the development of enhanced aircraft security regulations.⁶

B. HAZARDOUS MATERIALS MOTOR CARRIER SECURITY

1. Context

TSA's challenge is to imagine, assess, and mitigate all possible terrorist threat scenarios that may occur through the use of transportation vehicles or methods. One obvious threat involves using trucks hauling hazardous materials (hazmat) as a weapon. The 9/11 Commission recognized that Al Qaeda and other groups had, prior to the use of airlines, used suicide vehicles, namely, truck bombs, to commit terrorist acts.⁷ In fact, in the period from April 1983 to December 2007, terrorist groups have used commercial motor vehicles, including buses and hazmat trucks, more than 180 times as weapons of terror both internationally and domestically.⁸ For example, the following events all occurred in a two-month period in 2002.

- March 31, 2002: A 29-year-old driver for a propane distributor drove away with a 3000 gallon bobtail. He made a telephone threat stating that he wanted to kill President George W. Bush and that he would use the bobtail as a bomb.
- April 11, 2002: A terrorist driving a truck carrying liquefied natural gas ignited his cargo in front of a synagogue on the Tunisian Island of Djerba, killing 17 people, mainly German and French tourists. Al Qaeda claimed responsibility for the blast.

⁵ Transportation Security Administration Mission Statement, http://www.tsa.gov/who_we_are/mission.shtml (accessed December 11, 2008).

⁶ Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 STAT. 597 (2001).

⁷ National Commission on Terrorist Attacks, *9/11 Commission Report*, 344.

⁸ Anonymous government source.

- May 16, 2002: A tractor-trailer carrying 10 tons of deadly cyanide in 96 drums was stolen after three armed men held up the vehicle north of Mexico City. Six drums were never found.
- May 2002: A fully loaded tanker truck pulled into Israel's largest fuel depot and suddenly caught fire due to an explosive charge connected to a cellular phone. The fire was extinguished, but had the truck exploded, destruction and death would have resulted.⁹

The threat from hazmat trucks continues today. In 2004, Defense Secretary Donald Rumsfeld's visit to Iraq was punctuated by a fuel-truck attack that burned a section of Baghdad.¹⁰ More recently, terrorists in Iraq have used chlorine-based truck bombs repeatedly as a weapon in the Iraq war. For example, in the first three months of 2007, nine attacks using hazmat trucks were attempted and seven were successful.

- January 28, 2007: Sixteen people were killed in a chlorine truck explosion in Ramadi.
- February 19, 2007: A chlorine truck bomb killed 2 members of the Iraqi security force and wounded 16 others.
- February 20, 2007: A chlorine attack in Baghdad killed 5 and injured 140.
- February 21, 2007: A chlorine attack in Taji killed 9 and sickened 150.
- March 17, 2007: A three-pronged attack using chlorine bombs was staged in Ramadi, Fallujah, and Amiriya. Two people were killed and over 360 were poisoned as a result of the attacks.
- March 27, 2007: A truck packed with explosives and chlorine canisters exploded killing 1 Iraqi and wounding 7 in Ramadi. A second truck was found outside a police station and disarmed. The driver was captured before he could detonate the explosives.¹¹

With all of this evidence, there can be no doubt that terrorists are interested in using hazmat trucks as weapons within the borders of the United States. The Department of Transportation (DOT) recognizes that hazmat trucks are "dangerous and ready-made

⁹ *Hazardous Materials Safety and Security Technology Field Operational Test Volume I: Evaluation Final Report Executive Summary* (McLean, VA: SAIC, 2004).

¹⁰ Mark Clayton, "Hazardous-Materials Trucks: Terror Threat?" *Christian Science Monitor*, July 7, 2006, <http://www.csmonitor.com/2006/0707/p02s01-usgn.html> (accessed March 11, 2008).

¹¹ Bill Roggio, "Another Chlorine Truck Bomb Found near Ramadi," *The Long War Journal*, March 27, 2007, http://www.longwarjournal.org/archives/2007/03/another_chlorine_tru.php (accessed March 18, 2008).

weapons” and are “especially attractive” to terrorists.¹² Stephen Gale, a University of Pennsylvania professor and terrorism expert, agrees that hazmat trucks are essentially ready-made bombs that are “tailor-made” for terrorists to conduct an attack at the lowest cost and with the greatest impact.¹³ In fact, terrorism experts consider trucks to be one of the best tools a terrorist can use to breach security measures and carry explosives since the U.S. airline industry significantly increased security procedures.¹⁴ Although terrorists’ use of hazmat trucks in attacks within the United States is rare,¹⁵ the following events have taken place within the United States and are indicative of hazmat trucking security concerns.

- September 2001: The Federal Bureau of Investigation (FBI) arrested Nabil Almarabh, a man on their watch list who had obtained a hazmat license.¹⁶
- October 2001: The FBI charged 19 men with fraudulently obtaining Pennsylvania hazmat licenses. A driver’s license examiner in Pittsburgh helped at least 18 men get hazmat permits without taking the required tests. The examiner said he worked with a middleman named Abdul Mohamman and was paid \$50 to \$100 for each person he helped.¹⁷ When Mohamman was arrested, he had a newspaper clipping about Ahmed Ressam, an operative for Osama bin Laden who was convicted of an aborted millennium bomb plot.¹⁸
- August 2006: The FBI warned of a possible fuel-truck attack in a major U.S. city.¹⁹

¹² Roggio, “Another Chlorine Truck Bomb Found near Ramadi,” 2.

¹³ Dante Chinni, “America’s Roads May Be Just as Vulnerable as Its Skies,” *The Christian Science Monitor*, October 1, 2001, 1.

¹⁴ *National Hazardous Material Commercial Vehicle Tracking System Study* (Charlottesville, VA: Accelerated Solutions, 2006), 11.

¹⁵ Two important truck-based terror attacks in U.S. history were the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995 that killed 168 people and the February 26, 1993 bombing of Tower One of the World Trade Center in New York City that killed 6 people and injured 1,042. In each of these cases, terrorists used rental trucks filled with explosives as opposed to hazmat trucks to carry out their attacks. This thesis is not designed to address the security issues related to non-hazmat trucks such as those used in these two cases.

¹⁶ Chinni, “America’s Roads,” 2.

¹⁷ Ibid.

¹⁸ Brian Bloquist and Tracy Connor, “Cops Nab Ten in Haz-mat Scheme,” *The New York Post*, September 27, 2001, 011.

¹⁹ Clayton, “Hazardous-Materials Trucks,” 1.

2. Statistics

There is no doubt that the threat is real and the terrorists are acting on their desires. America needs to secure its hazmat motor carriers. To understand the gravity of the problem, one need only look at the statistics. Almost 15% of the total shipping tonnage in the U.S. is hazmat, which is almost exclusively moved by trucks.²⁰ Of the overall hazmat shipments by truck, 1.2% are considered to be toxic inhalation hazards (TIHs).²¹ Most motor carrier hazmat shipments involve flammable liquids, such as gasoline (82%), followed by gases (6.2%), and corrosive materials (5.1%).²²

These hazmat trucks, when full, cross America's roads approximately 800,000 times per day, and of those, 300,000 hauls are classified as extreme risk.²³ There are 57,714 hazmat carriers, 3,982,703 hazmat trucks, and 1,765,631 hazmat drivers registered with the DOT.²⁴ Half of all carriers' business is short hauls that occur entirely within a state.²⁵ Most of these shipments are hauled by local fleets that operate on thin profit margins.²⁶ Add to this the fact that 98% of the trucking industry is made up of small businesses, those companies with 28 or fewer trucks used in daily operations, 82% of which own fewer than 7 trucks,²⁷ and the enormity of the security challenge becomes clear.

C. SUMMARY

The threat is here and it is obvious. Terrorist organizations have used and their actions expose a continuing desire to use hazmat trucks as weapons of terror within the United States. A summary of prior attacks exposes a propensity for terrorists to use fuel

²⁰ *National Hazardous Material Commercial Vehicle Tracking System Study*, 11.

²¹ Anonymous government source.

²² *Ibid.*

²³ *National hazardous Material Commercial Vehicle Tracking System Study*, 12.

²⁴ Anonymous government source.

²⁵ *National Hazardous Material Commercial Vehicle Tracking System Study*, 10.

²⁶ *Ibid.*

²⁷ *Ibid.*

and propane trucks as well as trucks loaded with chlorine canisters. Perhaps this is the case because a great majority of hazmat shipments consist of flammable liquids like gasoline or liquefied gases. Of these shipments, 98% are short hauls transported by small carriers operating on thin profit margins and mostly within a single state. There can be no debate about the high level of risk these vehicles pose to America's transportation security.

1. Research Question

The ability of the government to secure every hazardous materials motor carrier against terrorist attack is severely limited, yet the potential that hazardous materials trucks will be used in terrorist attacks is great. Therefore, can the security of hazardous materials motor carriers of all types be improved voluntarily and quickly by realigning existing resources and instituting a plan that leverages market forces and other incentives?

This research will examine how, through the development of a unique voluntary incentive-based program, TSA can leverage existing resources as well as successful ideas from private sector and governmental programs to rapidly and significantly enhance the security of hazardous materials motor carriers.

2. Methodology

This thesis will examine a full range of government policies, statutes, and regulations affecting the security of hazardous materials motor carriers. Specifically it will review Homeland Security Presidential Directive number 7, Executive Order 11346, and testimony from the Administrator of the Transportation Security Administration. Statutes to be addressed are the USA PATRIOT Act of 2001 and the 9/11 Commission Act of 2007. Finally, TSA and DOT have issued numerous regulations addressing the problem, which will be explained.

A review of governmental action in this arena, including the DOT study on Hazardous Materials Safety and Security Technology and the TSA Truck Tracking Pilot,

as well as additional governmental programs, will enhance the reader's understanding of the efforts put forth to date. This information is supplemented by a series of in-person interviews with both government and industry officials.

Finally, a series of private and public sector programs will be analyzed. These programs include two examples from the private sector and six from the public sector. The private sector programs are the Responsible Care® program established by the American Chemistry Council and the Responsible Distribution ProcessSM established by the National Association of Chemical Distributors. The public sector programs are the Department of Energy and Environmental Protection Agency's Energy Star program; the Occupational Safety and Health Administration's OSHA Star program; the National Park Service Historic Preservation Tax Incentive program; Virginia's Enterprise Zone Program; Free and Secure Trade (FAST), a program developed by the United States Customs and Border Protection, Canada, and Mexico; and finally the United States Coast Guard's Port Security Grants Program.

After an analysis of hazmat motor carrier security and the existing gaps between what is desired and the current status, a model built upon successful elements of the private and public sector programs will be crafted to offer a viable incentive-based solution. This model will allow TSA to quickly and efficiently enhance its hazmat motor carrier security program.

3. Literature Review

The literature concerning the security of hazardous materials trucking is sparse. There is even less material concerning incentive-based approaches to address the problem. To best address the issue, it is necessary to review the literature first concerning the framework of the problem and then drawing upon other disciplines to extrapolate information that can be used as a basis for a solution. The literature can be divided into five distinct categories. First, there is information concerning government policy. Second is statutory language enacted by Congress. Third is information related

to agency actions. Fourth is literature describing unique programs developed by industry. And finally, the fifth category is made up of information concerning some unique governmental incentive programs.

Government policy consists of a Homeland Security Presidential Directive, Executive Order, and Agency testimony. Specifically, Homeland Security Presidential Directive number 7 “Critical Infrastructure Identification, Prioritization and Protection”²⁸ addresses the need to implement tactical security improvements to deter, mitigate, or neutralize potential attacks as well as the need to establish security programs incorporating risk management activities and metrics²⁹ for critical infrastructure sectors including chemical and ground/surface transportation systems.³⁰

Executive Order 13416 titled “Strengthening Surface Transportation” signed by the President on December 5, 2006 established the nation’s policy and sought the implementation of a comprehensive, coordinated, and efficient security program to protect surface transportation systems within and adjacent to the United States against terrorist attacks.³¹

Finally, in two different sets of testimony before Congress, Transportation Security Administration Administrator Kip Hawley addressed the Subcommittee on Homeland Security of the Committee on Appropriations of the United States House of Representatives to discuss the President’s fiscal year 2008 budget request for TSA.³² In his address, Mr. Hawley discussed funding for surface transportation security. He also explained that he encouraged an effective network of local security where each individual surface transportation stakeholder can make a strategic and deliberate decision when they develop their annual budgets as to where security-related investments should be made.

²⁸ President, “Critical Infrastructure Identification, Prioritization, and Protection,” Homeland Security Presidential Directive 7 (December 17, 2003).

²⁹ Ibid., 14.

³⁰ Ibid., 15.

³¹ President, Executive Order 13416, “Strengthening Surface Transportation Security,” *Federal Register* 71, no. 235 (December 7, 2006): 71033.

³² Statement of Kip Hawley, Assistant Secretary, Transportation Security Administration, before the Subcommittee on Homeland Security, Committee on Appropriations, United States House of Representatives.

Similarly, in testimony before the United States Senate Committee on Commerce, Science, and Transportation, on January 18, 2007, Assistant Secretary Hawley provided an update to Congress on TSA's hazmat motor carrier security programs. He explained that TSA's plan to address security gaps would include "a number of voluntary incentive programs and regulatory options."³³

Congress also plays an important part contributing to the literature in the field. Specifically, Congressional action through the USA PATRIOT Act of 2001 established the requirement for background checks on drivers applying for hazmat endorsements.³⁴ Additionally, the 9/11 Commission Act of 2007 established a series of motor carrier security requirements addressing issues including truck security assessments, a memorandum of understanding (MOU) between DOT and DHS, the truck security grant program, hazardous materials highway routing, security-sensitive material tracking, and hazardous materials security inspections.³⁵

The next category of literature is derived from Agency action in the field. Specifically, the DOT implemented various security actions related to hazmat motor carriers. It published a regulation requiring safety and security plans,³⁶ conducted security sensitivity visits,³⁷ implemented a requirement for hazardous materials safety

³³ Statement of Kip Hawley, Assistant Secretary, Transportation Security Administration, before the Committee on Commerce, Science, and Transportation, United States Senate (January 18, 2007), 8.

³⁴ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 49 USC § 5103a (2001).

³⁵ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266.

³⁶ Hazardous Materials Table, Special Provisions, Hazardous Materials Communications, Emergency Response Information, Training Requirements, and Security Plans, 49 CFR § 172.800 (2003).

³⁷ *Report on FMCSA's Security Sensitivity Visits to the House and Senate Committees on Appropriations* (January 31, 2002).

permits,³⁸ and studied security technologies in the three-volume report titled *Hazardous Materials Safety and Security Technology Field Operational Test* published in November 2004.³⁹

TSA issued the Hazardous Materials Endorsements and Transportation Worker Identification Credential regulation that provides for credentialing and security threat assessments of certain land transportation workers.⁴⁰ In addition, there exists scant information related to TSA's Corporate Security Review program,⁴¹ grants,⁴² truck tracking center program,⁴³ and voluntary Security Action Items.⁴⁴

The fourth area of the literature is information produced by industry trade groups. One example is the Responsible Care® program established by the American Chemistry Council (ACC). This is an internal quality assurance program developed for its members. A wide range of information concerning this program is published on the Internet.⁴⁵ Through its web site, ACC offers information about the program and its successes.⁴⁶ It publishes its security code, which addresses facility, cyber, and

³⁸ Safety Fitness Procedures, 49 CFR § 385.403 (1988).

³⁹ *Hazardous Materials Safety and Security Technology Field Operational Test Volume I: Evaluation Final Report Executive Summary*, 1; D. Stock et al., *Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis* (Washington, D.C.: Federal Motor Carrier Safety Administration, U.S. DOT, 2004); Volume III is unavailable as it contains sensitive security information.

⁴⁰ Credentialing and Background Checks for Maritime and Land Transportation Security, 49 CFR part 1572 (2003).

⁴¹ Transportation Security Administration, "Programs," http://www.tsa.gov/what_we_do/tsnm/highway/programs.shtml (accessed October 22, 2008).

⁴² Department of Homeland Security, Office of Inspector General, *Administration of the Federal Trucking Industry Security Grant Program for FY 2004 and FY 2005* (October 29, 2007).

⁴³ *Decision Support System for a National HAZMAT Truck Tracking Center* (Charlottesville, VA: The Accelerated Masters Program in Systems Engineering, 2007).

⁴⁴ Transportation Security Administration, "Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs)," http://www.tsa.gov/what_we_do/tsnm/highway/hssm_sai.shtml (accessed October 22, 2008).

⁴⁵ American Chemistry Council, "Responsible Care," http://www.americanchemistry.com/s_responsiblecare/sec.asp?CID=1298&DID=4841 (accessed October 14, 2008).

⁴⁶ American Chemistry Council, "Performance through Responsible Care," http://www.americanchemistry.com/s_responsiblecare/doc.asp?CID=1298&DID=5084 (accessed October 14, 2008).

transportation security and requires companies to conduct comprehensive security vulnerability assessments (SVAs) of their facilities, implement security enhancements, and obtain independent verification that those enhancements have been made. The code also requires companies to create security management systems, which are documented to provide quality control and assurances.⁴⁷ In addition to security, ACC requires strict standards in management systems and then reports details of the program and individual member compliance statistics to provide credibility to the program.⁴⁸

A similar program is the Responsible Distribution ProcessSM developed by the National Association of Chemical Distributors (NACD). This too is an internal quality assurance program aimed specifically at chemical distributors. Like ACC, NACD publishes information about its program on the Internet.⁴⁹ The program operates under eight guiding principles related to health, safety, security, and environmental performance.⁵⁰ It also publishes a twelve-part Code of Management Practice with which each member must comply.⁵¹ Additionally, information concerning third-party verification requirements⁵² and a compliance timetable are published.⁵³ Finally,

⁴⁷ American Chemistry Council, "Responsible Care Security Code," http://www.americanchemistry.com/s_responsiblecare/doc.asp?CID=1298&DID=5085 (accessed October 14, 2008).

⁴⁸ American Chemistry Council, "Ensuring Accountability Through Management System Certification," http://reporting.responsiblecare-us.com/reports/rcmsc_cmpny_rpt.aspx (accessed October 14, 2008).

⁴⁹ National Association of Chemical Distributors, "Responsible Distribution Process," http://www.nacd.com/dist_process/ (accessed October 14, 2008).

⁵⁰ National Association of Chemical Distributors, "Guiding Principles," http://www.nacd.com/dist_process/rdpguide.aspx (accessed October 14, 2008).

⁵¹ National Association of Chemical Distributors, "Code of Management Practice," http://www.nacd.com/dist_process/rdpcode.aspx (accessed October 14, 2008).

⁵² National Association of Chemical Distributors, "Third Party Verification," http://www.nacd.com/dist_process/rdpverification.aspx (accessed October 14, 2008).

⁵³ National Association of Chemical Distributors, "RDP Compliance Timetable for NACD Candidates," http://www.nacd.com/dist_process/rdp_compliance.aspx (accessed October 14, 2008).

membership and performance data are available for each year of the program, but this information is only available in the aggregate and is not attributable to specific members like the ACC Responsible Care® program.⁵⁴

Finally, the fifth category is made up of information concerning unique governmental incentive programs. These programs include the Department of Energy and Environmental Protection Agency's Energy Star program; the Occupational and Health Administration's OSHA Star program; the National Park Service's Historic Preservation Tax Incentive program; Virginia's Enterprise Zone Program; Free and Secure Trade, a program developed by the United States Customs and Border Protection, Canada, and Mexico; and finally the Homeland Security Port Security Grants Program.

The Department of Energy and Environmental Protection Agency's Energy Star program publishes significant information about its program on the Internet.⁵⁵ Examples of the information available include a history of the program, a detailed program summary, and links to annual reports memorializing major milestones.⁵⁶ There is also information about program partners, awards programs and recipients, and news clips related to the program.⁵⁷ Add to this a complete list of major milestones achieved by the program,⁵⁸ as well as a detailed newsletter,⁵⁹ and one can gain a complete understanding of the program.

⁵⁴ National Association of Chemical Distributors, "Measuring the Impact of the Responsible Distribution Process on Environmental, Health, Safety, & Security Performance," http://www.nacd.com/dist_process/rdp_indices_members.aspx (accessed October 14, 2008).

⁵⁵ U.S. Department of Energy and Environmental Protection Agency, "Energy Star," <http://www.energystar.gov/> (accessed October 14, 2008).

⁵⁶ U.S. Department of Energy and Environmental Protection Agency, "About Energy Star," http://www.energystar.gov/index.cfm?c=about.ab_index (accessed October 14, 2008).

⁵⁷ U.S. Department of Energy and Environmental Protection Agency, "Energy Star Partners," http://www.energystar.gov/index.cfm?c=news.nr_partners (accessed October 14, 2008).

⁵⁸ U.S. Department of Energy and Environmental Protection Agency, "Major Milestones," http://www.energystar.gov/index.cfm?c=about.ab_milestones (accessed October 14, 2008).

⁵⁹ U.S. Department of Energy and Environmental Protection Agency, "Fall 2008 Energy Star News," http://www.energystar.gov/index.cfm?c=news.nr_fall2008 (accessed October 14, 2008).

The Occupational Safety and Health Administration's OSHA Star program also maintains an active web presence.⁶⁰ Their web site provides background information under a section titled All About VPP.⁶¹ It also contains a full set of policies and procedures as well as information concerning *Federal Register* entries.⁶² Like the ACC's Responsible Care® program, OSHA provides a full list of participants and their status under the program.⁶³ It also provides details about other program initiatives and pilot projects.⁶⁴ A reader may also access news releases and a list of success stories as well as links to VPP Partners' web sites.⁶⁵ Finally, OSHA maintains an on-line library complete with data and statistics about the program and other related materials.⁶⁶

The National Park Service's Historic Preservation Tax Incentive program, like the other government web sites, hosts a great deal of information about its program. There is a detailed portion of the web site dedicated to information about the tax incentive program and its different tax incentives.⁶⁷ The site also provides another full section related to incentive programs for income-producing properties.⁶⁸ The certification application and guidance related to the application are also all available on the web.⁶⁹ While the amount of information available on this site is extensive, the portions mentioned supra are the most relevant to this thesis.

⁶⁰ U.S. Department of Labor, Occupational Safety and Health Administration, "Voluntary Protection Programs," <http://www.osha.gov/dcsp/vpp/index.html> (accessed October 14, 2008).

⁶¹ U.S. Department of Labor, Occupational Safety and Health Administration, "All about VPP," http://www.osha.gov/dcsp/vpp/all_about_vpp.html (accessed October 14, 2008).

⁶² U.S. Department of Labor, Occupational Safety and Health Administration, "Policies and Procedures," http://www.osha.gov/dcsp/vpp/vpp_policy.html (accessed October 14, 2008).

⁶³ U.S. Department of Labor, Occupational Safety and Health Administration, "Voluntary Protection Programs."

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ Ibid.

⁶⁷ National Park Service, "Historic Preservation Tax Incentives," <http://www.nps.gov/history/hps/tps/tax/brochure1.htm> (accessed October 14, 2008).

⁶⁸ National Park Service, "Incentives!" <http://www.nps.gov/hps/tps/tax/incentives/index.htm> (accessed October 14, 2008).

⁶⁹ National Park Service, "Historic Preservation Certification Application," <http://www.nps.gov/hps/tps/tax/hpcappl.htm> (accessed October 14, 2008).

Virginia's Enterprise Zone Program also offers a large amount of information related to its program on its own web site.⁷⁰ The site includes a description of the program and relevant links to guide readers through the process. It also offers links to forms, publications, and even text of relevant legislation.⁷¹

The Free and Secure Trade program is documented in several different places on the Internet. A detailed library of information is available from the United States Customs and Border Protection web site that contains a section dedicated to FAST.⁷² This web site contains information about the genesis of the program as well as its provisions related to Canada and Mexico. It also provides details about every element of the program, specifically about all aspects of the Customs-Trade Partnership Against Terrorism.⁷³ Additionally, the White House issued a press release offering details when the program was launched in partnership with Canada.⁷⁴ Even Canada's Border Service's Agency maintains its own web site with public information about the program.⁷⁵

Finally, the Port Security Grants Program (PSGP) offered through DHS is discussed on the Internet as part of the Federal Emergency Management Agency's (FEMA) web site.⁷⁶ FEMA manages and administers all homeland security grants for DHS. Unlike other government web sites, there is only one meaningful reference to the

⁷⁰ Virginia Department of Housing and Community Development, "Virginia Enterprise Zone Program," http://www.dhcd.virginia.gov/CommunityDevelopmentRevitalization/Virginia_Enterprise_Zones.htm (accessed October 14, 2008).

⁷¹ Ibid.

⁷² U.S. Customs and Border Protection, "FAST: Free and Secure Trade Program," http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/fast/ (accessed October 14, 2008).

⁷³ U.S. Customs and Border Protection, "What Is Customs-Trade Partnership against Terrorism (C-TPAT)?" http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ (accessed October 14, 2008).

⁷⁴ The White House, "United States – Canada Free and Secure Trade Program," <http://www.whitehouse.gov/news/releases/2002/09/20020909-3.html> (accessed October 14, 2008).

⁷⁵ Canada Border Services Agency, "Free and Secure Trade," <http://www.cbsa-asfc.gc.ca/prog/fast-expres/menu-eng.html> (accessed October 14, 2008).

⁷⁶ Federal Emergency Management Agency, "FY 2009 Port Security Grant Program (PSGP)," <http://www.fema.gov/government/grant/psgp/index.shtml> (accessed October 14, 2008).

PSGP. This is the Program Guidance and Application Kit published in February 2008. It provides a full explanation of the program and details concerning funding, the application and evaluation process, allowable expenses, and guidance for specialized applicants.⁷⁷

⁷⁷ Federal Emergency Management Agency, “Fiscal Year 2008 Port Security Grant Program Guidance and Application Kit,” http://www.fema.gov/pdf/government/grant/psgp/fy08_psgp_guidance.pdf (accessed October 14, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

III. RECOGNITION OF THE THREAT

The American government has been aware of the threat posed by hazmat trucks for decades. Prior to 9/11, however, the government primarily focused its hazmat lens on safety, rather than security issues. It was not until the events of 9/11 that the threat posed by these ready-made weapons became real. Since 9/11, the government has recognized and spoken out about the need to better secure America's entire critical infrastructure, including its transportation network. At this point, if a terrorist should succeed in using a hazmat truck as a weapon, it will not be due to America's failure to imagine the threat; it will be due to America's failure to act on that threat.

A. PRESIDENTIAL ACTION

1. Homeland Security Presidential Directive Number 7

The terrorist threat posed by a failure to secure America's hazmat trucks has been addressed by the President through Directive and Executive Order. On December 17, 2003, The President issued Homeland Security Presidential Directive number 7 (HSPD-7).⁷⁸ In this Directive, he made clear that "in addition to strategic security enhancements, tactical security improvements can be *rapidly* implemented to deter, mitigate, or neutralize potential attacks" (emphasis added).⁷⁹ He charged the Secretary of Homeland Security to establish security programs incorporating risk management activities and metrics⁸⁰ for critical infrastructure sectors including chemical and ground/surface transportation systems.⁸¹ He required the Secretary to work closely with other federal departments and agencies, state and local governments, and the private sector in

⁷⁸ President, Homeland Security Presidential Directive, 7.

⁷⁹ *Ibid.*, 5.

⁸⁰ *Ibid.*, 14.

⁸¹ *Ibid.*, 15.

accomplishing the objectives of the directive.⁸² He even specifically required the DOT and DHS to collaborate on all matters relating to transportation security and to regulate the transportation of hazardous materials.⁸³

As a result of HSPD-7, Michael Chertoff, the Secretary of DHS issued the National Infrastructure Protection Plan (NIPP) in 2006. The NIPP incorporated the HSPD-7 requirements and established a risk management framework as its cornerstone. The framework establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.⁸⁴ This framework is illustrated in Figure 1 and is the strategy to be followed by DHS components and partners when developing critical infrastructure management programs.⁸⁵

Figure S-2: NIPP Risk Management Framework

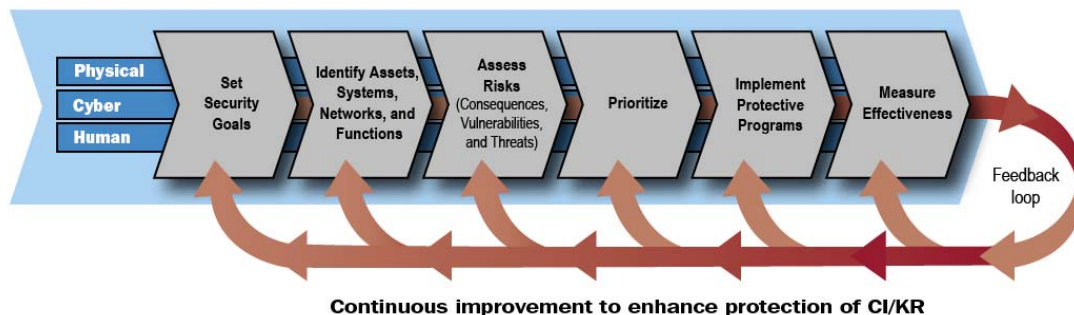


Figure 1. NIPP Risk Management Framework

2. Executive Order 13416

On December 5, 2006, the President signed Executive Order 13416 titled “Strengthening Surface Transportation.” In this Order, he established that federal, state,

⁸² President, Homeland Security Presidential Directive, 17.

⁸³ Ibid., 22(h).

⁸⁴ Department of Homeland Security, *National Infrastructure Protection Plan* (2006), 4.

⁸⁵ Ibid.

local, and tribal governments, as well as the private sector, all share the responsibility for surface transportation security.⁸⁶ He then expressed the nation's policy in this arena as follows.

It is the policy of the United States to protect the people, property, and territory of the United States by facilitating the implementation of a comprehensive, coordinated, and efficient security program to protect surface transportation systems within and adjacent to the United States against terrorist attacks.⁸⁷

In this Order, he assigned the Secretary of Homeland Security as the principal federal official responsible for protecting surface transportation infrastructure.⁸⁸ The Secretary was directed to work in coordination with the Secretary of Transportation to do the following.

- assess the security of each transportation mode
- develop a comprehensive transportation systems sector-specific plan
- develop an annex to the comprehensive transportation systems sector specific plan that addresses each surface transportation mode
- in consultation with state, local, and tribal government officials and the private sector, identify surface transportation modes or components thereof that are subject to high risk of terrorist attack and draft appropriate security guidelines or security requirements to mitigate such risks
- develop, implement, and lead a process to coordinate research, development, testing, and evaluation of technologies relating to the protection of surface transportation
- use security grants authorized by law to assist in implementing security requirements and security guidelines issued pursuant to law⁸⁹

⁸⁶ President, Executive Order 13416, § 1.

⁸⁷ Ibid.

⁸⁸ Ibid. § 3.

⁸⁹ Ibid.

B. TRANSPORTATION SECURITY ADMINISTRATION ACTION

1. Testimony before Subcommittee on Homeland Security of the Committee on Appropriations of the United States House of Representatives

The Assistant Secretary for the Transportation Security Administration, Kip Hawley, addressed TSA's implementation of the requirements in Executive Order 13416 when he addressed the Subcommittee on Homeland Security of the Committee on Appropriations of the United States House of Representatives to discuss the President's fiscal year 2008 budget request for TSA.⁹⁰ In his address, Mr. Hawley clarified that the budget request included \$41.4 million for surface transportation security. DHS, DOT, and TSA were all working together with surface transportation stakeholders to enhance security through partnerships, proposed regulations, and grant awards.

Mr. Hawley explained that TSA uses a risk-based model to rank priorities in this arena. Some of the highest priorities identified by TSA for fiscal year 2008 were grant priority for underwater and underground tunnels in mass transit and TIHs in the rail environment. He stressed that TSA implements its strategies through cooperation with stakeholders where appropriate, regulation and inspection where necessary, and the distribution of grants to assist the industry to implement the objectives set forth. In fact, while not funded by TSA, grant programs are an important element of DHS's approach to the surface transportation security strategy. By staying true to this plan, each individual surface transportation stakeholder can make a strategic and deliberate decision when they develop their annual budgets as to where security-related investments should be made. This model encourages an effective network of local security rather than relying on a larger federal workforce to address the same issues.

⁹⁰ Statement of Kip Hawley, Assistant Secretary, Transportation Security Administration, before the Subcommittee on Homeland Security, Committee on Appropriations, United States House of Representatives.

2. Testimony before the United States Senate Committee on Commerce, Science, and Transportation

Similarly, in testimony before the United States Senate Committee on Commerce, Science, and Transportation, on January 18, 2007, Assistant Secretary Hawley provided a status report on TSA's hazmat trucking security progress.⁹¹ In that statement he informed the Committee that TSA had been conducting Corporate Security Reviews (CSRs) to assess readiness and vulnerabilities of different motor carriers. TSA's analysis led them to focus security efforts on TIH chemicals and other hazardous chemicals of concern, including explosives.

He stated that TSA has been working with industry to establish baseline security standards for TIH and other chemicals of concern. These standards are expected to address issues such as vehicle tracking, vehicle attendance, vehicle alarm systems, truck cab access controls, and locking fifth wheel on tank trailers as well as security route and stop areas. Once the baseline is established, TSA plans to begin identifying and addressing gaps. The plan is to do so by use of "a number of voluntary incentive programs and regulatory options."⁹²

C. SUMMARY

The President and the Assistant Secretary for TSA recognize the risks posed by hazmat motor carriers and affirm their commitment to address those risks. They each espouse specific principles they expect to be followed when devising and implementing strategies to mitigate the risk. Specifically, there is an expectation that tactical security enhancements will be readily implemented. Security measures will be based on risk management strategies and metrics. The federal government will partner with state and local governments as well as the private sector to develop an effective network of security that is not reliant solely on the federal workforce. These plans will be enacted through the use of security grants, voluntary actions, and regulation.

⁹¹ Statement of Kip Hawley, Assistant Secretary, Transportation Security Administration, before the Committee on Commerce, Science, and Transportation, United States Senate (January 18, 2007).

⁹² *Ibid.*, 8.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CLARIFYING ROLES

A. DHS AND DOT

While DHS and DOT both recognize the need for action in securing America's hazmat motor carriers, a systemic failure to clarify their roles in terms of which agency held primary responsibility to address hazmat motor carrier security made it difficult to devise and implement a security plan. Prior to 9/11, DOT was responsible for hazmat truck safety and security issues. In response to the terrorist attacks of 9/11, Congress passed the Aviation and Transportation Security Act (ATSA) of 2001.⁹³ This Act assigned to TSA the responsibility to secure all modes of transportation. In 2001, TSA was a part of DOT. Shortly thereafter, in 2002, Congress established DHS through the Homeland Security Act.⁹⁴ This legislation transferred TSA into DHS and gave DHS responsibility for protecting the nation from terrorism, including the protection of the nation's transportation systems.

At this point, TSA was designated the lead agency responsible for the security of hazmat vehicles⁹⁵ while DOT maintained a regulatory role related to safety.⁹⁶ However, the Homeland Security Act also expanded DOT's responsibilities to include both the safety and security of hazardous materials transportation.⁹⁷ The DOT component Pipeline Hazardous Materials Safety Administration (PHMSA) was therefore responsible

⁹³ Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 STAT. 597 (2001).

⁹⁴ Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

⁹⁵ See Homeland Security Presidential Directive-7 (Dec. 17, 2003); Exec. Order No. 13416 (Dec. 5 2006); 71 Fed. Reg. 71033 (Dec. 5, 2006); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007); Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

⁹⁶ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 49 USC § 5103a (2001).

⁹⁷ Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

for the security plan requirements of hazmat carriers⁹⁸ while the Federal Motor Carrier Safety Administration (FMCSA) maintained inspectors to enforce security regulations through a periodic review of the content and implementation of the security plans.⁹⁹

In 2004, DHS and DOT entered into a MOU to clarify their respective roles and responsibilities regarding transportation security.¹⁰⁰ That MOU was further clarified by annex in 2006 to specifically address the transportation of hazardous materials. This annex establishes TSA as the lead federal entity responsible for the security of the transportation of hazardous materials and PHMSA as responsible for the promulgation and enforcement of regulations addressing safety and security of the transportation of hazardous materials.¹⁰¹ Unfortunately, the roles of the two agencies regarding motor carrier transportation security matters remain unclear. The Implementing Recommendations of the 9/11 Commission Act thus require the two to clarify their respective roles and delineate responsibilities, resources, and commitments by completing an additional annex to their MOU no later than 2008.¹⁰²

B. SUMMARY

While the confusion over DHS and DOT roles and responsibilities remains unclear, the threat continues to linger, time continues to pass, and opportunities for action continue to be lost. If these agencies complete an additional annex to their MOU as required by Congress, their roles may finally be clarified to the extent necessary for them to focus on security concerns. As of the writing of this thesis, the government has made little progress in securing hazmat trucks, especially those owned by smaller carriers who haul the highly vulnerable flammable liquids and gases.

⁹⁸ The term “hazmat carrier” refers to the transportation of hazmat through different modes and not specifically by motor carrier.

⁹⁹ Anonymous government source.

¹⁰⁰ This memorandum of understanding was signed by DOT and DHS on September 28, 2004.

¹⁰¹ Anonymous government source.

¹⁰² Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007).

V. ACTIONS ACCOMPLISHED

To better understand America's current security programs, it is important to review actions by Congress, DOT, and TSA.

A. CONGRESSIONAL ACTION

1. The USA PATRIOT Act of 2001

One of the first pieces of legislation passed by Congress after 9/11 that contained any provision addressing transportation security, other than ATSA, was the USA PATRIOT Act of 2001.¹⁰³ This legislation implemented a limitation upon the states prohibiting the issuance of a license to operate a motor vehicle transporting hazardous materials to any individual until that person has undergone and passed a satisfactory background check.¹⁰⁴ This same legislation extended the background check requirements to commercial motor vehicle operators registered to operate in Canada or Mexico who wish to transport hazardous materials in the United States.¹⁰⁵

2. The 9/11 Commission Act of 2007

The most recent legislation addressing hazmat motor carrier security contains a series of six specific provisions enumerated in the 9/11 Commission Act of 2007.¹⁰⁶ These provisions address the requirement for a truck security assessment, clarification of roles between DOT and DHS, a review of the trucking security grant program, highway routing of hazardous trucks, tracking of security-sensitive materials, and a study on hazmat security inspections.

¹⁰³ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 49 USC § 5103a (2001).

¹⁰⁴ *Ibid.*

¹⁰⁵ *Ibid.*

¹⁰⁶ Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007).

a. Truck Security Assessment

Section 1540 requires DHS, in coordination with DOT, to study certain trucks carrying specified hazardous materials in a quantity sufficient to require placarding and issue a report to Congress that includes the following.

- a security risk assessment of the trucking industry
- an assessment of actions already taken by public and private entities
- an assessment of the economic impact of security requirements on the industry
- an assessment of current research and the need for future research into security
- an assessment of industry best practices
- an assessment of the current status of secure truck parking

b. Memorandum of Understanding

In section 1541, DOT and DHS are required to execute an annex to the memorandum of understanding between the two agencies that delineates each of their specific roles, responsibilities, resources, and commitments to address security matters.

c. Report on Trucking Security Grant Program

The DHS Inspector General is required in section 1542 to submit to Congress a report on the trucking security grant program oversight and expenditures and to make recommendations regarding the future of the program, including options to improve the effectiveness and utility of the program and motor carrier security.

d. Hazardous Materials Highway Routing

Section 1553 requires the Secretary of Transportation, in conjunction with the Secretary for DHS, to document and assess the current and proposed routes for hazardous materials and develop a framework for using a geographic-information-system-based approach to characterize routes in the national hazardous materials route registry as well as identify measurable criteria for selecting routes. It also requires an

analysis of route-related regulations in the U.S., Canada, and Mexico and a review of safety and security concerns related to their routes. Additionally, it requires that guidance materials be prepared for state officials to assist them with safety and security concerns of hazardous materials routed through their state. Also, the safety and security benefits achieved under current route plans for explosives and radioactive materials must be assessed and reported to Congress.

An additional requirement provides that specified hazmat motor carriers must maintain, follow, and carry a route plan when carrying specified types and quantities of hazardous materials if the Secretary of Transportation determines that such a requirement would enhance security and safety without imposing unreasonable costs or burdens upon motor carriers.

e. Security-Sensitive Material Tracking

Section 1554 requires TSA to develop a program to facilitate tracking of motor carrier shipments of certain security-sensitive materials and to equip vehicles used in such shipments with technology that provides for frequent or continuous communication, vehicle position, location and tracking capabilities, and emergency distress signal capability. Congress also provides for funding of these requirements for fiscal years 2008, 2009, and 2010 in the amounts of \$7,000,000 each year, \$300,000 of which must be spent on equipment each year. However, Congress specifically prohibits TSA from mandating the installation or utilization of any related technology without additional Congressional authority.

In essence, Congress is providing for the development and further testing of a truck tracking program at the government's expense. The program will only apply to vehicles carrying what TSA defines as security-sensitive materials, which in essence are explosives and chemicals posing a toxic inhalation hazard.

f. Hazardous Materials Security Inspections

This section, 1555, was enacted to require DOT and DHS to address the problem of duplicative reviews of hazardous materials security plans and to assess the insurance, security, and safety costs associated with hazmat transport.

3. Hazardous Materials Endorsements and Transportation Worker Identification Credential

An additional federal regulation provides for credentialing and security threat assessments of certain land transportation workers.¹⁰⁷ In relevant part, applicants who are seeking to obtain or renew a hazardous materials endorsement (HME) to their commercial driver's license must provide specified information so that TSA can conduct a security threat assessment before issuing a Determination of No Security Threat to the appropriate state agency responsible for issuing a HME.¹⁰⁸ A security threat assessment includes a fingerprint-based criminal history records check (CHRC), an intelligence-related background check, and a final disposition.¹⁰⁹ If TSA determines that the individual poses a threat, the state must immediately revoke a current HME and refrain from issuing or renewing a HME.¹¹⁰ Similarly, an individual may seek to apply for or renew a Transportation Worker Identification Credential (TWIC) card. TWICs are tamper-resistant biometric credentials that will be issued to workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities, and

¹⁰⁷ Credentialing and Background Checks for Maritime and Land Transportation Security, 49 CFR part 1572 (2003).

¹⁰⁸ *Ibid.* at 49 CFR § 1572.9.

¹⁰⁹ *Ibid.* at 49 CFR § 1572.15.

¹¹⁰ *Ibid.* at 49 CFR § 1572.13.

all credentialed merchant mariners.¹¹¹ To obtain credentials, drivers must undergo and pass a security threat assessment.¹¹² In either case, applicants will be required to pay an information collection fee, threat assessment fee, and FBI fee.¹¹³

The security threat assessment requirements are designed to help the government ensure that individuals who pose a threat to security do not legally gain access to hazardous materials by working as a licensed driver or as a transportation worker that has unescorted access to secure areas of ports or vessels. Prior to the implementation of this regulation, an individual who may have been listed as a terrorist on an intelligence-related government database could have been legally licensed to transport or access hazardous materials. However, hazmat carriers often object to the apparent duplication of effort required when they are told they are required to undergo a background check to obtain an HME and then undergo a second background check to obtain a TWIC card.

B. DOT ACTIONS

In addition to Congressional action, DOT also implemented various security actions related to hazmat motor carriers. Specifically, DOT published a regulation requiring safety and security plans, conducted security sensitivity visits, implemented a requirement for hazardous materials safety permits, and studied security technologies.

1. Safety and Security Plans

On March 25, 2003, DOT issued a regulation addressing the security risks related to the transportation of hazardous materials in commerce. The regulation required that by September 25, 2003, each person who offers for transportation or who transports specified hazardous materials must develop and adhere to a security plan that meets

¹¹¹ Transportation Security Administration, “Transportation Worker Identification Credential (TWIC),” http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed April 2, 2008).

¹¹² Credentialing and Background Checks for Maritime and Land Transportation Security, 49 CFR part 1572 (2003).

¹¹³ *Ibid.*, at 49 CFR 1572.404, 1572.405.

specified requirements.¹¹⁴ The security plan must include an assessment of risks and measures to address those risks. Additionally, it must include elements addressing personnel security, unauthorized access, and en route security.¹¹⁵

The personnel security section of the plan must provide for measures to confirm information provided by job applicants hired for positions that involve access to and handling of the hazardous materials covered by the security plan.¹¹⁶ The unauthorized access provision must provide for measures to address the assessed risk that unauthorized persons may gain access to the hazardous materials covered by the security plan.¹¹⁷ Finally, the en route security provision must address the assessed security risks of shipments of hazardous materials covered by the security plan en route from origin to destination, including shipments stored incidental to movement.¹¹⁸

2. Security Sensitivity Visits

After 9/11, the FMCSA initiated a program to conduct on-site visits to motor carriers to discuss security enhancements. It states that its mission is “to increase the level of awareness of hazardous materials carriers to terrorist threats, identify potential weaknesses in carrier security programs, and report potentially serious security issues to the appropriate authorities.”¹¹⁹ Visits consist of face-to-face meetings by FMCSA or state investigators and top carrier officials to assess security vulnerabilities and countermeasures and make security recommendations.¹²⁰

¹¹⁴ Hazardous Materials Table, Special Provisions, Hazardous Materials Communications, Emergency Response Information, Training Requirements, and Security Plans, 49 CFR § 172.800 (2003).

¹¹⁵ 49 CFR § 172.802 (2003).

¹¹⁶ 49 CFR § 172.802(a)(1) (2003).

¹¹⁷ 49 CFR § 172.800(a)(2) (2003).

¹¹⁸ 49 CFR § 172.800(a)(3) (2003).

¹¹⁹ *Report on FMCSA’s Security Sensitivity Visits to the House and Senate Committees on Appropriations* (January 13, 2002).

¹²⁰ *Ibid.*

3. Hazardous Materials Safety Permits

As of January 1, 2005, the FMCSA started phasing in a hazardous materials safety permitting program. This program applies only to a limited community of high hazard materials including radioactive substances, explosives, materials poisonous by inhalation, and liquefied gases with a methane content of at least 85%.¹²¹ According to the program, such carriers must apply for and receive a safety permit from the FMCSA before they can transport these materials on America's roadways.¹²²

In order to obtain a safety permit, the motor carrier must have a satisfactory safety rating that is obtained by the carrier certifying that it has a crash rate in the top 30% of the national average, a total out-of-service rate in the top 30%, and a satisfactory security program that includes a security plan, a communications plan, and certification that all hazmat employees have completed security training.¹²³ Additionally, each carrier must be registered with the Research and Special Programs Administration.¹²⁴

4. Technological Solutions for Hazmat Truck Security

In 2004, the FMCSA published the results of a study it conducted of security technology options for hazmat motor carriers. This study began in September 2003 and ended in April 2004. The study results as published by FMCSA do not provide specific details of the products tested in terms of manufacturer or model numbers. Instead, the study focuses on technology as divided into twelve types.¹²⁵ Some motor carriers have made the independent business decision to install some of this technology, but there are no governmental requirements or incentives regarding the purchase, installation, or use of any of it. The technologies tested as divided by type are as follows.

¹²¹ Safety Fitness Procedures, 49 CFR § 385.403 (1988).

¹²² 49 CFR 385.401 (1988).

¹²³ 49 CFR 385.407 (1988).

¹²⁴ 49 CFR 385.407(c) (1988).

¹²⁵ D. Stock et al., *Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis* (Washington, D.C.: Federal Motor Carrier Safety Administration, U.S. DOT, 2004).

- wireless satellite and terrestrial communications systems
- digital phone without a global positioning system (GPS)
- panic buttons
- global login
- biometric global login
- electronic supply chain manifest
- intelligent on-board computers initiating remote vehicle disabling
- internal trailer door locking system
- external electronic seal
- geofencing
- tethered trailer tracking
- untethered trailer tracking

a. *Wireless Satellite and Terrestrial Communications Systems*

Wireless satellite technology is designed to function with a satellite-based global positioning system to provide reports of vehicle position through latitude and longitude readings. A terrestrial-based communications link is similar except that it is land-based and allows for two-way communications. Each system generates a message showing vehicle position upon automatic request generated from the dispatch computer. Such requests can be generated as often as desired.

b. *Digital Phone without GPS*

Special cellular wireless telephone handsets using Binary Runtime Environment for Wireless (BREW) technology permit dispatch and the driver to communicate. Dispatch can transmit integrated work order assignments to a driver and the driver can respond with status messaging. If the driver accepts the assignment, then the details are provided. After assignment, drivers can use one of five macros to report progress. Those macros are accept/reject assignment, arrived, started, stopped, and departed.

This system was assessed by the management of a single trucking company and determined to be a viable technology. However, no actual test was performed since the company who was supposed to test the devices could not accommodate the phones into their daily operational processes. Additionally, specific comments were offered to improve the device. Those comments were as follows.

- The display was too small
- The menu button was very hard to navigate, even after training
- Cellular coverage was spotty once the trucks left the highway
- The battery life of the phones was short and required them to be plugged into the charger most of the time
- The phones lacked GPS capability that would be useful to help validate the information being transmitted

Additional concerns may include the following.

- The driver can easily lose the phone
- Messaging required an active response where the dispatcher and driver had to initiate the action. Dispatchers or drivers could forget to send a message or consider it to be too time-consuming or difficult. Failure to generate required messages invalidates the system's usefulness.
- Even if all messages were sent as required, in the event of an emergency, dispatch had no control over the actual vehicle

c. Panic Buttons

Panic buttons allow a driver to send a panic message either via satellite or terrestrial communications system. Some remote systems even allow the driver to disable the vehicle. These systems are usually deployed in one of two ways; either the system is mounted inside the vehicle or via a wireless panic button carried by the driver. The wireless system studied operates within a distance of 250 feet from the vehicle.

This technology was well accepted by the motor carriers participating in the test. The technology worked well and was effective in providing notification of an event and accurately provided the location and time of an alert. In fact, some study

participants were already using panic buttons for their trucks and expressed excellent satisfaction with this technology. Additionally, certain defense and munitions carriers are already required to use these systems.

In some cases, panic buttons were paired with remote vehicle disabling available to the driver. The driver held a key fob with a button that allowed him to remotely disable the vehicle at a range of 250 feet. This technology also worked well and was received enthusiastically by drivers because control was put in their hands. The only drawback to this technology was that some drivers feared accidentally bumping the key fob and activating an alert. This issue could be resolved through the design of the key fob itself.

d. Global Login

On-board software enables global login technology that requires the driver to enter a user ID and password in order to operate the truck. The information is verified within the truck and remotely through a wireless communication system. If the login is accepted, the driver can use the truck. If the login fails, notice is sent to the dispatcher who can decide what action to take. One option is to remotely disable the truck.

Test results showed that this technology worked well and did not impede operations. On average, it took a driver 33 seconds to log into the system. The only drawback noted was that this system may be a burden to drivers who make multiple stops. The test carriers stated that biometric login may be more convenient than global login technology. Additional potential drawbacks include a driver forgetting his login ID and/or password.

e. Biometric Global Login

Biometric global login is similar to the global login system. In place of requiring a user ID and a password to start the truck, this technology requires the driver to possess a smart card and scan a fingerprint. This system operates through an on-board central processing unit run by proprietary firmware. Unlike the global login, there is no necessary link to the dispatcher.

The biometric login concept appealed to many carriers. Unfortunately, it exhibited many drawbacks upon actual testing. This technology required specific placement of fingers on a consistent basis to obtain accurate readings. Fingers that were either too hot or too cold could not be read. These issues caused a great deal of driver frustration and complaints. While logins took about 45 seconds to 1 minute to complete, many frustrated drivers stopped using the biometric login and opted for the global login feature as a more reliable back up. Additional concerns are that the biometric reader also requires that the driver use a smart card that the driver could lose and thus would make the biometric login inoperable. Also, while this technology prevents unauthorized users from starting a truck, once the truck is started, the dispatcher has no knowledge of its whereabouts and has no control over the vehicle.

f. Electronic Supply Chain Manifest

The electronic supply chain manifest is a system using several technologies to accomplish its task of tracking and maintaining a chain of custody for hazmat transport vehicles. This system relies upon biometric verification, smart cards, Internet applications and on-board wireless communications. To operate the system, a shipper using biometric systems and smart card technology logs in and creates an electronic manifest and identifies a load assignment. Once complete, the manifest is shipped to a central server. All authorized users then log into a centralized database to access this manifest. This combination of steps allows the computer to generate a chain of custody for the shipment.

This technology has the potential to offer several benefits to its users. It provides the precise commodity description and quantity for the dispatcher. Customer inquiries could be easily addressed. It could reduce paperwork errors and processing times since all members of the supply chain would use a single database. It could reduce the accounts receivable cycle by allowing simultaneous invoice creation with delivery confirmation. It could even help law enforcement or emergency response personnel in the case of an emergency because the dispatcher would have information about the contents of the truck.

Unfortunately, this technology suffers from some substantial drawbacks. First, all members of the supply chain must purchase and be plugged into the same interface in order to make this technology useful. Also, all who are plugged in would have to use the system correctly and consistently. Because there are too many different stakeholders involved in the process, during the test, the technology was not used or was not used correctly in many cases. The effectiveness of this technology requires a high level of attention and that appears to be unrealistic when dealing with numerous partners. An additional drawback from a security perspective is that even if used properly, this technology does not provide any mapping or control of the vehicle to the dispatcher. Thus if the truck is stolen, it would be difficult to locate and could not be shut down remotely.

g. Intelligent On-Board Computers Initiating Remote Vehicle Disabling

The on-board computer is designed to work in conjunction with the wireless communications/vehicle operating systems. In the event of a security breach, the vehicle could be disabled in one of several ways. One technique is to block fuel to the engine. Another is to send instructions wirelessly to the vehicle's data bus, instructing it to throttle down. In this study, the on-board computer was also instructed to shut down the vehicle if there was a loss of satellite signal strength due to cut cables or blocked signal. An alternative was to allow for local vehicle disabling whereby the driver would use a wireless remote panic button that would send a signal to initiate the disablement. The local vehicle disabling does not require the use of the on-board computer to disable the vehicle.

This technology was well received although participants expressed some reservations about shutting down a vehicle in the normal stream of traffic. They did say that it was an option in emergency situations, however. Participants expressed doubt that this technology would be approved for use in the real world due to these concerns.

h. Internal Trailer Door Locking System

An internal trailer door locking system provides access control to a remote dispatcher. Once a driver has reached a predetermined destination and is ready to deliver the contents of a cargo trailer, he contacts dispatch to request that the doors be unlocked. The dispatcher can then send an over-the-air signal to the trailer and unlock the doors. The driver receives a signal on the dashboard of the cab informing him when the signal has been received and the doors can be opened. The driver then has 20 seconds to open the doors before the process must be restarted.

This technology worked excellently during testing. It performed as specified and even comes with some additional safeguards. The design of the locking mechanism makes it difficult for the doors to be pried open by an unauthorized party. Additionally, if the doors are pried open, the system generates a tamper message and sends it to the network management center.

i. External Electronic Seal

An external electronic seal is a device attached to a seal on the outside of a trailer that automatically generates a short-range alert via wireless communication if the device is compromised without proper authorization. The signal is transmitted to an on-board wireless communications device that transmits a signal through a web-based application to the dispatcher.

This technology proved ineffective in real-world tests. Training was difficult due to the complexity of the technology and the many steps required to operate the seal. It took drivers several minutes to complete the cycle of assigning and locking an e-seal. Additionally, attempts to communicate with the seal from the cab of the truck to the back of the rear doors of the trailer were unsuccessful. It appeared that the signal was not strong enough to operate on newer more rigid trailers. Therefore, the e-seal did not prove to be operationally feasible. Additional issues are that this technology, if effective, could only notify a dispatcher if a seal was broken. It provides no control over the unauthorized movement of a truck.

j. Geofencing

An internet application allows a dispatcher to establish a specified route for operation and/or identify a specific risk area within which a truck is not allowed to operate. The technology defining the area within which the truck may operate is referred to as an electronic fence or geofence. The dispatcher can monitor the truck's route over the Internet. If a truck leaves its designated path or enters a risk area, then pre-established settings will notify the dispatcher of this event.

Geofencing worked well in tests. Minimal training was needed for a dispatcher to set a route on an Internet-based software package. It was received positively by the company testing its use and was determined to be an excellent technology to locate a vehicle that was off route or in an undesirable area. The testing participant noted that, besides security benefits, this technology might keep drivers from stopping for excessive periods of time at unauthorized locations. There were some noted limitations to this technology. During this test, a position signal was sent to the system only once every hour. Thus, if a truck left its allotted zone after its last signal, it could be off track for a full hour before the next signal was sent generating an alert. The signal interval can be shortened, but it increases the cost to the carrier. Ultimately, the interval between signals comes down to a cost/benefit decision for users. The preferred option would be for real-time notifications.

k. Tethered Trailer Tracking

Trailer connects and disconnects are monitored remotely by dispatchers using tethered trailer tracking. Software generates a record of the date, time, and location of each connect or disconnect event and transmits that data to dispatch using satellite communications technology.

l. Untethered Trailer Tracking

A wireless satellite tracking system was merged with geofencing capabilities in order to provide more geographic coverage by eliminating blackouts and dead zones.

Users found both tethered and untethered trailer tracking to be useful technologies. They liked to be able to detect trailer connects and disconnects and they also appreciated the ability to track an unconnected trailer as another authorized carrier moved it. There were no problems reported with these systems.

m. Overall Results

The study measured the effectiveness of each type of technology individually and as combined with others in terms of their ability to reduce security vulnerabilities based on theft, diversion, interception of bulk fuel, less than load–high hazard, bulk chemicals, and truckload explosives. The reduction in vulnerability achieved under the study was reported as a percentage of 100 where a score of 100 was a complete reduction in vulnerability. Values from 0 to 10% were considered to be nil, values from 11% to 25% were considered to be low, values from 26% to 50% were considered to be medium, and values over 50% were considered to be a high reduction in vulnerability.¹²⁶ The results are reported in the following tables.

Results Chart Legend	
Description in Results	Technology Type
Wireless Communications	Digital phone without GPS
GPS Position	Wireless satellite and terrestrial communications systems
Panic Alert	Panic buttons
Driver ID	Global login; biometric global login
Vehicle Disabling	Intelligent on-board computers initiating remote vehicle disabling
Cargo Seals	External electronic seal
Cargo Door Locks	Internal trailer door locking system
PSRC	Public sector reporting center
ESCM	Electronic supply chain manifest

¹²⁶ Stock et al., *Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis*, 53.

Percent Reduction in Vulnerability of <i>Theft</i> by Load Type (all numbers in %)				
Technology Countermeasure Scenarios	Bulk Fuel	LTL – High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	23	17	19	17
WC + GPS Position	26	24	27	20
Panic Alert + (WC + GPS Position)	42	37	42	33
Driver ID + (WC + GPS Position)	40	38	39	29
Vehicle Disabling + (WC + GPS Position)	42	39	44	31
Cargo Seals + (WC + GPS Position)	NA	37	NA	29
Cargo Door Locks + (WC + GPS Position)	NA	36	NA	29
PSRC + (WC + GPS Position)	37	36	39	31
ESCM + (WC + GPS Position)	41	39	39	29
Panic Alert + Vehicle Disabling + (WC + GPS Position)	52	47	52	40
Panic Alert + Driver ID + Vehicle Disabling + (WC + GPS Position)	58	54	57	43
Panic Alert + Driver ID + ESCM + (WC + GPS Position)	57	53	55	42
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals + (WC + GPS Position)	NA	53	NA	42
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks + (WC + GPS Position)	NA	52	NA	42

Percent Reduction in Vulnerability of <i>Diversion</i> by Load Type (all numbers in %)				
Technology Countermeasure Scenarios	Bulk Fuel	LTL – High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	14	13	11	11
WC + GPS Position	16	15	14	13
Panic Alert + (WC + GPS Position)	26	23	23	23
Driver ID + (WC + GPS Position)	24	23	21	19
Vehicle Disabling + (WC + GPS Position)	25	26	24	21
Cargo Seals + (WC + GPS Position)	NA	23	NA	19
Cargo Door Locks + (WC + GPS Position)	NA	22	NA	19
PSRC + (WC + GPS Position)	24	23	22	22
ESCM + (WC + GPS Position)	24	24	21	19
Panic Alert + Vehicle Disabling + (WC + GPS Position)	31	31	29	27
Panic Alert + Driver ID + Vehicle Disabling + (WC + GPS Position)	34	34	31	29
Panic Alert + Driver ID + ESCM + (WC + GPS Position)	34	33	30	29
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals + (WC + GPS Position)	NA	33	NA	28
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks + (WC + GPS Position)	NA	33	NA	29

Percent Reduction in Vulnerability of <i>Interception</i> by Load Type (all numbers in %)				
Technology Countermeasure Scenarios	Bulk Fuel	LTL – High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	7	5	5	6
WC + GPS Position	8	6	6	7
Panic Alert + (WC + GPS Position)	12	8	9	12
Driver ID + (WC + GPS Position)	11	8	8	9
Vehicle Disabling + (WC + GPS Position)	11	9	10	10
Cargo Seals + (WC + GPS Position)	NA	8	NA	9
Cargo Door Locks + (WC + GPS Position)	NA	8	NA	10
PSRC + (WC + GPS Position)	12	9	10	11
ESCM + (WC + GPS Position)	11	8	8	10
Panic Alert + Vehicle Disabling + (WC + GPS Position)	14	11	12	14
Panic Alert + Driver ID + Vehicle Disabling + (WC + GPS Position)	15	12	13	14
Panic Alert + Driver ID + ESCM + (WC + GPS Position)	15	11	12	14
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals + (WC + GPS Position)	NA	11	NA	14
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks + (WC + GPS Position)	NA	11	NA	14

Percent Reduction in Overall Vulnerability by Load Type and Technology (all numbers in %)				
Technology Countermeasure Scenarios	Bulk Fuel	LTL – High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	15	13	12	11
WC + GPS Position	17	16	16	12
Panic Alert + (WC + GPS Position)	27	25	25	21
Driver ID + (WC + GPS Position)	25	25	23	18
Vehicle Disabling + (WC + GPS Position)	26	27	26	19
Cargo Seals + (WC + GPS Position)	NA	25	NA	18
Cargo Door Locks + (WC + GPS Position)	NA	24	NA	18
PSRC + (WC + GPS Position)	24	25	24	20
ESCM + (WC + GPS Position)	25	26	23	18
Panic Alert + Vehicle Disabling + (WC + GPS Position)	32	32	31	25
Panic Alert + Driver ID + Vehicle Disabling + (WC + GPS Position)	36	37	34	27
Panic Alert + Driver ID + ESCM + (WC + GPS Position)	35	36	33	26
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals + (WC + GPS Position)	NA	36	NA	26
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks + (WC + GPS Position)	NA	35	NA	26

Table 1. Overall Results

C. TSA ACTIONS

While DOT focused on security as an integral part of its safety programs, TSA focused on security issues alone. There are four programs run by TSA that specifically focus on the security of hazmat motor carriers. Those are corporate security reviews, grant distribution, a truck tracking center pilot, and most recently the publication of voluntary security action items. Unfortunately, TSA has not met with much success for any of these programs.

1. Corporate Security Reviews

In order to assess the risk to commercial motor carriers, TSA implemented a CSR program. This program has three main goals: first to develop best practices for security through discussions with carriers and visits to their facilities, second to begin the collection of data that will allow TSA to assess security across the industry, and third to identify security gaps and opportunities for improvement.¹²⁷ Within its first two years from November 2005 through November 2007, TSA had only conducted reviews of 40 trucking companies. This small number of reviews can be accounted for due to the small number of full-time staff TSA is able to allocate to this project.

In an effort to revise the process, TSA partnered with the state of Missouri and FMCSA's Motor Carrier Safety Assistance Program to conduct additional CSRs.¹²⁸ This partnership greatly improved TSA's ability to collect data. The Missouri inspectors focused primarily on small firms, which are the most common in the industry. While hazmat carriers were only a part of the trucking companies surveyed, in an eleven-month period, Missouri was able to conduct 1,231 CSRs on trucking companies alone.¹²⁹

Missouri completed a report on their findings and concluded that their sample was not representative of the commercial vehicle industry in their state or of the industry nationwide. However, of the results they did reach, they reported that motor carriers of

¹²⁷ William Arrington, General Manager, TSA Highway and Motor Carrier Programs, interview by author, Arlington, VA, July 27, 2007.

¹²⁸ Anonymous government source.

¹²⁹ Ibid.

all types did not have extensive security procedures in place, smaller carriers had implemented few security measures, and hazmat carriers had implemented more security measures than others.¹³⁰ Of note were the conclusions that, generally, larger firms scored higher than smaller firms and interstate carriers scored higher than intrastate carriers.¹³¹ This data is important because half of all hazmat hauls occur intrastate,¹³² and 98% of the industry is made up of small businesses, 82% of which own fewer than seven trucks.¹³³

2. Security Grants

To date, DHS has spent more than \$60 million in grants targeted at trucking security. The money was spent by TSA, which signed a cooperative agreement with the American Trucking Associations (ATA) to develop and run a program called Highway Watch. The no-bid cooperative agreement began in fiscal year 2003 and was funded through a grant to ATA in excess of \$26 million per year from TSA. ATA was to provide the training, manage a Highway Watch call center, and promote the program. Training costs exceeded \$8 million per year and program administration exceeded \$9 million per year.

The program was designed to reach out to commercial truck and bus drivers, school bus drivers, highway maintenance crews, bridge and tunnel toll collectors, and others and recruit them as an additional layer of security for the nation's highways. The program's primary goal is to prevent attacks by teaching highway professionals to avoid becoming a target for terrorists who would use large vehicles or hazardous cargoes as a weapon. A secondary goal is to train highway professionals to recognize and report suspicious activity.¹³⁴ This program provided the training and communications infrastructure necessary to accomplish its goal by preparing 400,000 transportation

¹³⁰ Anonymous government source.

¹³¹ Ibid.

¹³² *National Hazardous Material Commercial Vehicle Tracking System Study*, 10.

¹³³ Ibid.

¹³⁴ Transportation Security Administration, "TSA Teams up with American Trucking Associations to Prevent and Respond to Terrorism," (March 23, 2004), http://www.tsa.gov/press/releases/2004/press_release_0405.shtm (accessed July 29, 2008).

professionals to respond in the event they or their cargo become the target of a terrorist attack and to share valuable intelligence with TSA if they witness potential threats.

In 2008, the Highway Watch agreement with ATA was not renewed and was instead awarded to a new firm, HMS Company of Alexandria, VA. The DHS Inspector General, in charge of reviewing allegations of fraud, waste, and abuse is now reviewing the program and expenditures¹³⁵ amid allegations that ATA spent more money on administration and marketing than it did on training.¹³⁶ To date, all of TSA's motor carrier grant money has been spent solely on this program. No other direct grant money has been made available to hazmat carriers for the installation of security devices or the development of other trucking security programs.

3. Truck Tracking Pilot

As part of its plan to address hazmat motor carrier security issues, TSA, in conjunction with The University of Virginia Accelerated Master's Program in Systems Engineering, deployed a Truck Tracking Center (TTC) Pilot Project in Buffalo, NY. The pilot was designed to put truck-tracking technology to the test under real-world conditions. It was launched in September 2005, and a final report on the program was published in 2008.

The objective of the TTC study was to develop the operational concept and functional requirements for processing truck tracking signals to identify real and potential transportation security incidents and use such data to demonstrate likely cost and performance estimates for a national system.¹³⁷ In short, the TTC was designed to serve as a management, monitoring, and prevention center for hazmat events.¹³⁸ The results of the study highlight numerous difficulties for the implementation of a nationwide program.

¹³⁵ Department of Homeland Security, Office of Inspector General, *Administration of the Federal Trucking Industry Security Grant Program for FY 2004 and FY 2005* (October 29, 2007).

¹³⁶ Samuel Loewenberg, "Truckers Lose DHS Contract," *Politico*, May 16, 2008, <http://www.politico.com/news/stories/0508/10412.html> (accessed September 12, 2008).

¹³⁷ *Decision Support System for a National HAZMAT Truck Tracking Center*, 12.

¹³⁸ *Ibid.*, 14.

Almost immediately, challenges facing such a national program became apparent. While the study acknowledged that primarily small operators in the U.S. handle hazmat transportation,¹³⁹ and companies with large fleets of 100 or more trucks account for less than 1% of the industry, TSA has been able to make progress installing tracking systems on trucks belonging to large operators, but acknowledged that it will have significant difficulty doing the same for small companies.¹⁴⁰

Nineteen months into the study, the following findings emerged.¹⁴¹

- The TTC was receiving a huge volume of data¹⁴²
- TSA received data only once hourly, making it slow to respond to hazmat events and unable to anticipate incidents
- The TTC was ill-equipped to manage the data in-flow even though the pilot includes a very small portion of current hazmat shipments

These findings were far from what TSA believes it would need to claim a successful TTC program. Ultimately, in the normative scenario, TSA would be able to rapidly collect data, enabling a rapid response to all hazmat events and prevent incidents through the use of risk profile development and geofencing,¹⁴³ a technology solution that restricts a truck's path of travel. In order to accomplish these goals, on-truck communications units would have to be installed on 420,000 hazmat trucks nationwide.¹⁴⁴

The authors realized that if a TTC program were to be effective, they would have to find a way to filter the incoming data so that only the relevant material could trigger action. Ultimately, if effective filtering were enabled, the center could serve four main purposes.¹⁴⁵

¹³⁹ More than 87% of the industry operates six or fewer trucks; Ibid., 10.

¹⁴⁰ Ibid.

¹⁴¹ Ibid., 16.

¹⁴² The report offers no quantitative data to support this finding.

¹⁴³ Geo-fencing consists of technology on board a truck that analyzes vehicle position data against restricted areas and can send an alert when the vehicle violates a restricted parameter.

¹⁴⁴ *Decision Support System for a National HAZMAT Truck Tracking Center*, 18, 39.

¹⁴⁵ Ibid., 20.

- disseminate information to first responders and facilitate interagency communication to mitigate risk in rescue and cleanup operations
- generate simple heuristics for detection of irregular behavior in hazmat movement
- aggregate and analyze data in the long term in order to gain insights into how to more safely transport hazardous materials
- provide added value to the carrier and goods shipper by mitigating risk associated with hazmat, thereby reducing long-term operating costs

Unfortunately, the study found that even if the data filtering issues could be resolved, the actionable data was not meaningful. Therefore, it was concluded that the TCC was not effective as an incident monitoring and first response center.¹⁴⁶

An additional significant detriment to the capture of actionable data was the generation of false panic signals. Such signals usually occur by accident, when a driver panics and overreacts to a situation or when the signal goes off due to a technical glitch. Over a period of one year, it was determined that the probability that a signal would be a false alarm was 99.37%.¹⁴⁷ Unresolved, the false signal problem effectively crippled the TCC program.

Due to these problems, even a simplified version of the TCC would not be feasible. It would cost in excess of \$3.5 million annually,¹⁴⁸ while the bulk of the man-hours would be spent responding to false panic alarms.¹⁴⁹ Even worse, the proposed model would actually delay¹⁵⁰ the normal emergency response time due to a process that incorporated additional steps between the call for help and dispatch.

While the results of this study do not fare well for a national truck-tracking center until some issues are resolved, it does not nullify the benefits of using technology in different ways. One possible alternative would be to encourage individual companies to

¹⁴⁶ *Decision Support System for a National HAZMAT Truck Tracking Center*, 33.

¹⁴⁷ *Ibid.*

¹⁴⁸ *Ibid.*, 40.

¹⁴⁹ *Ibid.*, 41.

¹⁵⁰ The study does not quantify the length of the delay.

install technology on their trucks and then have their own dispatch center track and monitor for panic signals. This model would severely reduce the truck-to-monitor ratio, so false alarms would be much less of a distraction.

4. Security Action Items

On July 16, 2008, TSA announced the publication of 23 recommended security action items (SAIs) for the transportation of hazardous materials on the nation's highways. According to TSA, the security action items have been divided into four categories 1) general security, 2) personnel security, 3) unauthorized access, and 4) en route security. General security measures pertain to security threat assessments, security planning, protecting critical information, and awareness of industry security practices. Personnel security and unauthorized access refer to practices affecting the security of the motor carrier's employees, contracted employees, and its property. En route security refers to the actual movement and handling of motor vehicles containing highway security-sensitive materials (HSSM).¹⁵¹

A list of specific materials that qualify as HSSM is divided by TSA into tier 1 and tier 2 materials. Generally, TSA is most concerned about explosives and inhalation hazard materials. Items such as gasoline and propane, for example, do not make this list because if ignited, they do not cause a hazard as high as the level as those materials on the list.

The first recommended action items apply to both tiers. Items 17–23 apply only to tier 1 HSSM. More specifically, the SAI categories include the following.

- A) General security
 - 1. Security assessment and security plan requirements
 - 2. Awareness of industry security practices
 - 3. Inventory control process
 - 4. Business and security critical information

¹⁵¹ Transportation Security Administration, "Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs)," http://www.tsa.gov/what_we_do/tsnm/highway/hssm_sai.shtm (accessed September 11, 2008).

- B) Personnel security
 - 5. Possession of a valid commercial drivers license hazardous materials endorsement
 - 6. Background checks for highway transportation sector employees other than motor vehicle drivers with a valid CDL with hazardous materials endorsement
 - 7. Security awareness training for employees
- C) Unauthorized access
 - 8. Access control system for drivers
 - 9. Access control system for facilities incidental to transport
- D) En route security
 - 10. Establish communications plan
 - 11. Establish appropriate vehicle security program
 - 12. Establish appropriate cargo security program to prevent theft or sabotage of cargo containers
 - 13. Implement a seal/lock control program to prevent theft or sabotage of cargo
 - 14. High alert level protocols
 - 15. Establish security inspection policy and procedures
 - 16. Establish reporting policy and procedures
 - 17. Shipment preplanning, advance notice of arrival, and receipt confirmation procedures with receiving facility
 - 18. Preplanning routes
 - 19. Security for trips exceeding driving time under the hours of service of drivers regulation
 - 20. Dedicated truck
 - 21. Tractor activation capability
 - 22. Panic button capability
 - 23. Tractor and trailer tracking systems

These SAIs apply only to HSSM carriers¹⁵² and their adoption is strictly voluntary. TSA tells carriers that “no one solution fits all motor carriers and

¹⁵² Materials that are considered to be HSSM are generally explosives and those that are toxic inhalation hazards. The specific list is not available for public dissemination.

circumstances. These security action items allow for flexibility in implementation based upon the assessed vulnerability of a particular process or operation. Where appropriate, implementation of these action items to their fullest extent practicable should be the goal of the affected owner and operator.”¹⁵³ However, any owner or operator who chooses to comply with some or all of these recommendations, while potentially more secure, will receive no governmental benefit or recognition for compliance. There is no method in place by which TSA can monitor industry response other than through voluntary feedback provided by the industry.

D. SUMMARY

Congress, DOT, and TSA have all been working on the issue of hazmat carrier security, but success remains elusive. Current projects are focused primarily on HSSMs, a dangerous but very small portion of the hazmat motor carrier industry. Primarily, achievements focus on background checks for hazmat vehicle drivers and security education programs. There has been almost no progress made in securing non-HSSM or smaller carriers. Technology solutions exist and are proven, but due to a combination of factors including expense, perceived lack of need, lack of government grants, and lack of requirement or incentive, these solutions are rarely employed. Additionally, data collection and truck tracking projects have not yet met with any meaningful success.

¹⁵³ John Sammon to Highway and Motor Carrier Stakeholders, letter dated June 26, 2008, 2.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. GAP ANALYSIS

A. IDENTIFIED GAPS

Seven years after the 9/11 attacks, the United States government has made little progress in securing the 800,000 daily trips made by hazardous materials trucks on our nation's highways. Attempts to address the issue have been made, but progress has been slow. The issues are not easy and TSA is working to address the problems. After analyzing the salient programs and their reported results, we can posit six major gaps in current policy. First, there is no plan to further address security issues of hazmat carriers of non-HSSM materials. Second, TSA recently published a list of 23 security action items but has provided no requirement or incentive to encourage their use. Third, the government has failed to maintain any meaningful statistics related to hazmat carriers. Fourth, despite tens of millions of dollars spent in grant money, the use of the funds is being investigated and none of it has been spent on security technology. Fifth, despite calls from the President and the Assistant Administrator for TSA, state, local, and tribal governments, as well as the private sector, have not been significantly included in the security process. Sixth, the few regulatory processes that have been put in place have proven to be duplicative and unnecessarily burdensome on the industry.

1. Non-HSSM Haulers

TSA has focused its security efforts on hazmat truckers hauling what it classifies as highway security-sensitive hazardous materials. TSA determined these to be the most important risk because of the breadth of the harm they can cause. Applying the classic formula for risk $R=TVC$, where R is risk, T is threat, V is vulnerability, and C is consequence, TSA has made the determination that risk is highest for these materials. Unfortunately, history and data clearly point to a different conclusion. Applying the formula, the consequences of an attack using HSSM materials is very high, but the threat and vulnerability may actually be low since many of the companies hauling these HSSM

materials may already be exercising good security practices due to their own fears of liability. If the vulnerability is reduced due to company action, the threat may also be reduced for fear of the security measures that may exist.

Alternatively, non-HSSM haulers may be at higher risk for a terror attack. A simple survey of terrorist attacks using hazmat trucks worldwide demonstrates a propensity for terrorists to use smaller or more readily accessible hazmat loads. In recent years there have been many attacks using small non-HSSM loads of chlorine gas in cylinders, gasoline tankers, and others. Therefore, a revisit of the risk formula shows that this threat is certainly viable given worldwide experience. The vulnerability is higher as these non-HSSM materials are more plentiful and have minimal security requirements. The consequences of the threat, while not as large as HSSM materials, would still cause significant damage both physically and psychologically, especially if multiple such attacks using these materials were to occur.

2. Security Action Items

In June 2008, TSA issued a set of 23 voluntary security action items aimed only at HSSM carriers. Unfortunately, TSA provided no assistance or incentives for a hazmat carrier to adopt these items. Add to that the fact that TSA claims that these items may eventually become regulation and hazmat haulers are understandably afraid to act because they may expend funds to adopt their version of compliance and then find that an actual regulation requires something different. This would turn their security investment into a financial loss.

3. Statistics

The government has failed to keep statistics on hazmat security events. There is no national database and no known state databases containing any of this type of information. While it may be possible to cobble some data together by researching FBI and individual state law enforcement statistics, the data would be difficult to find. There is no definition of what data would qualify as a security event, no specific code used to identify it in a database, and no specific place for this type of data to be stored. Since

hazmat carriers are neither asked nor required to report this data to any central office, TSA is hampered in identifying trends exhibiting the need for particular security action. Additionally, even with the launch of the new SAIs, TSA has not introduced any mechanism to account for data collection. There is no way to determine which carriers may be voluntarily complying with the program or any issues or trends that may evolve.

4. Grant Money

TSA has spent over \$60 million in grant money solely for the Highway Watch program. It has not used any of this money to issue any other motor-carrier-security-related grants. Even if the program operated flawlessly and was highly successful, the best result would be that commercial truck and bus drivers, school bus drivers, highway maintenance crews, bridge and tunnel toll collectors, and others would be trained to look for security-related issues and report them to a call center. While this is a noble goal, it is highly probable that in today's security-conscious environment, these people and more are already conditioned to pick up their cell phone and dial 9-1-1 if they see something suspicious. TSA grant money can be better used to support the purchase and use of security technology that has a direct and meaningful payback. Such security technology most likely will not otherwise be put into use, especially by the smaller, more vulnerable carriers because of its expense.

5. Inclusiveness

Despite encouragement from the highest levels, state, local, and tribal governments, as well as the private sector, have been virtually left out of the security process. Each of these is an important partner in security and their knowledge, skills, and abilities should be harnessed. State, local, and tribal governments know their territory the best. They know of threats prone to their unique circumstances and it is their local first responders who will show up and manage the scene if a terrorist incident involving hazardous materials were to occur. Additionally, the private sector, including trucking

industry trade associations, the insurance industry, security technology companies, hazmat carriers, and more, can make valuable contributions if they are brought into the process.

6. Duplicative Regulatory Requirements

Due to the checkered processes by which government security regulations have evolved, there exists a web of unnecessary requirements for the industry. As an example, a single driver who wishes to legally haul hazardous materials must have his background checked once to obtain a hazmat endorsement to his driver's license, again to obtain a TWIC card, and a third time to obtain FAST approval. This is government bureaucracy at its worst.

B. SUMMARY

The six gaps in the hazmat security framework leave America vulnerable to terrorist attack. These very same gaps, however, present tremendous opportunity for TSA to build a strong and successful security framework. Simply by evaluating the factors necessary to fill these gaps and benchmarking with other successful public and private sector programs, TSA can develop and launch a security program that uses its existing resources, fosters any positive momentum, and builds a nationwide community of supportive participants.

VII. PRIVATE SECTOR PROGRAMS

Even before 9/11 and especially since that time, the hazardous materials industry has been proactive in enhancing its own security requirements. Two excellent examples of industry self-rule are the Responsible Care® program developed by the ACC and the Responsible Distribution ProcessSM developed by the NACD.

A. RESPONSIBLE CARE®

All ACC members as well as all partner companies must fully comply with the elements of the Responsible Care® program as verified by an independent auditor within strict timelines. Any members or partners who do not comply will lose their ACC status.

ACC carefully tracks its members' implementation of the program's Security Code and publicly discloses their performance.¹⁵⁴ Since September 11, 2001, Responsible Care® companies have invested more than \$6 billion to enhance security at their facilities.¹⁵⁵ The Security Code, which addresses facility, cyber, and transportation security, requires companies to conduct comprehensive security vulnerability assessments of their facilities, implement security enhancements, and obtain independent verification that those enhancements have been made. It also requires companies to create security management systems that include thirteen required management practices. Those requirements are as follows.

- Senior leadership commitment to continuous improvement through published policies, provision of sufficient and qualified resources, and established accountability
- Prioritization and periodic analysis of potential security threats, vulnerabilities, and consequences using accepted methodologies
- Development and implementation of security measures commensurate with risks and taking into account inherently safer approaches to process design, engineering and administrative controls, and prevention and mitigation measures

¹⁵⁴ American Chemistry Council, "Responsible Care."

¹⁵⁵ American Chemistry Council, "Responsible Care Security Code."

- Recognition that protecting information and information systems is a critical component of a sound security management system
- Documentation of security management programs, processes, and procedures
- Training, drills, and guidance for employees, contractors, service providers, value chain partners, and others, as appropriate, to enhance awareness and capability
- Communications, dialogue, and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers, and government officials and agencies balanced with safeguards for sensitive information
- Evaluation, response, reporting, and communication of security threats as appropriate
- Evaluation, response, investigation, reporting, communication, and corrective action for security incidents
- Audits to assess security programs and processes and implementation of corrective actions
- Third-party verification that, at chemical operating facilities with potential off-site impacts, companies have implemented the physical site security measures to which they have committed
- Evaluation and management of security issues associated with changes involving people, property, products, processes, information, or information systems
- Continuous performance improvement processes entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends, and development and implementation of corrective actions

ACC has determined that only members and partners who comply with all of these management practices may remain members and partners and can claim compliance with Responsible Care®. Partners have found that there are additional business-related benefits to belonging to ACC and complying with the Responsible Care® requirements. Those benefits are as follows.

- Promotes increased action and interaction between members and partners
- Fosters consistent terminology and streamlines communications throughout the chemical industry
- Improves dialogue with communities and other stakeholders about the safe handling of chemical products

ACC has worked hard to keep its program robust. In addition to its demand for strict adherence to program requirements, ACC supports the program by permitting use of its Responsible Care® logo to qualified companies, hosts an annual Responsible Care® leadership awards program, holds monthly teleconferences with its members and partners, and hosts an annual conference and exposition.¹⁵⁶

B. RESPONSIBLE DISTRIBUTION PROCESSSM

The Responsible Distribution ProcessSM (RDP) is an initiative of the NACD and its member companies designed to provide a system that promotes continuous improvement in the environmental, health, safety, and security performance of all member companies. It is designed to be sensitive and responsive to community needs and public concerns. The senior executive of each member company signs acceptance of the Guiding Principles and Code of Management Practice as a condition of membership.¹⁵⁷

RDP enumerates eight specific guiding principles by which member companies pledge to manage their business.¹⁵⁸ Those guiding principles are as follows.

- To recognize and respond to community concerns about chemicals, their handling, and transportation
- To make health, safety, security, and environmental considerations a priority in our planning for all existing and new operations, products, processes, and facilities
- To inform emergency response officials, employees, customers, and the public of manufacturer information on chemical-related health or environmental hazards and the manufacturer's recommendations on protective measures
- To work with customers, in accordance with manufacturer's recommendations, on product stewardship including handling, use, transportation, and disposal of chemical products

¹⁵⁶ American Chemistry Council, "Responsible Care Toolkit," http://www.americanchemistry.com/s_rctoolkit/index.asp (accessed October 22, 2008).

¹⁵⁷ *Responsible Distribution Process Code Coordinator Manual 2008* (Arlington, VA: National Association of Chemical Distributors, 2008), 3.

¹⁵⁸ *Ibid.*, 5.

- To operate our plants and facilities in a manner that protects the health and safety of our employees, the public, and the environment
- To cooperate in resolving problems created by past handling and disposal of hazardous chemicals
- To participate with government and others in creating responsible laws, regulations, and practices to help safeguard the community, workplace, and environment
- To promote the principles and practices of RDP by sharing experiences and offering assistance to others who produce, handle, use, transport, or dispose of chemicals

In addition to these eight Guiding Principles, the RDP maintains a twelve-part Code of Management Practice.¹⁵⁹ The categories outlining those practices are the following.

- risk management
- compliance review and training
- carrier selection
- handling and storage
- job procedures and training
- waste management and conservation practices
- emergency response and public preparedness
- community outreach
- product stewardship
- internal RDP audits
- RDP corrective and preventive action
- RDP document and data control

Each NACD member must prove its compliance with the RDP program. It does this by submitting to an independent third-party verification review. The verifier reviews a completed company profile, RDP questionnaire, and a self-assessment report. The third party also verifies the existence of company policies and procedures that are consistent

¹⁵⁹ *Responsible Distribution Process Code Coordinator Manual 2008. 7.*

with the spirit and intent of the RDP Code of Management Practice.¹⁶⁰ If a party does not obtain a favorable review, and does not correct any deficiencies, it will lose its membership.

In order to maintain a robust program, RDP holds twice-annual RDP Code Coordinator Workshops, peer-to-peer networking opportunities, publicly reports performance data, and presents an annual RDP Excellence Award for demonstrated outstanding performance of a company's RDP program based on the findings of NACD's two independent verification firms. Each of these incentives encourages member companies to maintain the highest standards. If a company does not comply, it will lose its NACD membership.

C. SUMMARY

The private sector felt the need to fill the gap left by the government in the security arena through its trade associations. Both of the cited programs are voluntary, rigorous, open, and supported by independent verification. Participants appreciate the value of the designation and this spurs the free market when they seek to do business only with other participants. When participants demand of their business chain the same adherence to rigorous security standards, those companies who do not comply can find themselves losing market share. Overall, the industry benefits because the better managed and more secure companies grow stronger while the less secure competitors wither away.

¹⁶⁰ *Responsible Distribution Process Code Coordinator Manual 2008*. 11.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. GOVERNMENT INCENTIVE PROGRAM MODELS

A. GOVERNMENT STAR PROGRAMS

An interesting phenomenon, referred to herein as the Star Effect, is beginning to emerge within government. Federal agencies are beginning to realize the value of public/private partnerships and develop beneficial programs by working with, rather than against market forces. A typical traditional approach to addressing issues used to be, and remains so today in many cases, that a problem was identified, the government developed its proposed response to fix that problem, and then set out on the lengthy and arduous path of developing regulations to require private sector compliance. This led to protracted regulation drafting processes, court battles, and, if the regulation was published, to exhaustive and expensive inspection and enforcement operations.

The fact remains that if industry does not embrace regulatory compliance, they may seek to meet the bare minimum level of compliance that will keep them from suffering a fine. Others will hedge their bets and ignore the regulation hoping not to get caught. It is safe to say that no industry will ever have any reason to put more money into regulatory compliance than necessary if they do not perceive any other value to their company. In essence, the metaphor for regulatory programs is pushing a boulder up a hill. No matter how much effort is exerted, if that effort is not continuously exerted, the natural tendency is for that boulder to roll backwards.

The metaphor for the Star Effect, on the other hand, is that of a boulder rolling down a hill while the government carefully manages its speed and direction. The government invites voluntary public/private partnerships where all parties together define the program and its goals. In the end, the government has an ever-growing number of partners who understand the benefits of participation in the program, and the government continues to assist the effort by sweetening the pot for those who participate.

Two examples of the Star Effect are the Energy Star program developed jointly by the U.S. Environmental Protection Agency (EPA) and the U.S. Department of Energy (DOE) and the OSHA Star program that is part of the OSHA's Voluntary Protection Programs (VPP).

1. Energy Star

The EPA launched the Energy Star program in 1992 as a voluntary labeling program designed to identify and promote energy-efficient products to reduce greenhouse gas emissions. The initial product categories were computers and computer monitors. Eventually the program expanded to additional office products and residential heating and cooling equipment. In 1996, EPA partnered with DOE to add additional product categories. The program now covers major appliances, office equipment, lighting, home electronics, new homes, and commercial and industrial buildings. It has also developed partnerships with more than 12,000 private and public sector organizations.¹⁶¹

In general, Energy Star works by dismantling identifiable and pervasive market barriers responsible for stifling investment in energy efficiency and by bringing practical solutions to the residential, commercial, and industrial sectors. Ultimately, businesses and consumers save money through lower utility bills and the government obtains lower greenhouse emissions, a reduced need to generate energy, improved energy independence, and security, as well as helping to grow the economy.

Through its programmatic efforts, more than 70% of the American public can identify the Energy Star label today. In 2007 alone, Americans purchased 500 million Energy Star qualified products across more than 50 product categories; more than 120,000 new homes were constructed to meet the guidelines, and states and localities have partnered with the program to offer benefits to local homeowners.¹⁶²

¹⁶¹ U.S. Department of Energy and Environmental Protection Agency, "History of Energy Star," http://www.energystar.gov/index.cfm?c=about.ab_history (accessed July 23, 2008).

¹⁶² U.S. Department of Energy and Environmental Protection Agency, "Energy Star Overview of 2007 Achievements," <http://www.energystar.gov/ia/partners/publications/pubdocs/2007%20CPPD%204pg.pdf> (accessed October 22, 2008).

The EPA states that the program's success is due, in part, to common market conditions surrounding energy efficiency. The program is designed to overcome market barriers and encourage the adoption of cost-effective energy efficiency products and services in a sustained manner and to help unleash the attendant savings for individuals and organizations. To do this, EPA does not fund the purchase of equipment, products, or services. Instead, it uses its funds to provide consumers and businesses with information and tools to break down major market barriers and alter decision making for the long term. This approach helps drive private capital toward energy efficiency investments and provides environmental and economic payback for the government's investment.

Energy Star remains relevant and successful in part due to its following attributes.

- market-based approach
- benefits for all parties
- voluntary nature
- public/private partnerships
- corporate- and citizen-based pledge and involvement
- inclusive nature
- branding
- effective national campaign
- annual awards program
- openness
- willingness to embrace international partnerships

2. OSHA Star

The U.S. Department of Labor through its OSHA arm launched VPP in 1982 modeled after an experimental program in California begun in 1979. The VPP program is designed to promote effective worksite-based safety and health. It works through the

development of voluntary public/private cooperation that fosters relationships between management, labor, and OSHA. To date, the average VPP worksite has a days away, restricted, or transferred case rate of 52% below the average for its industry.¹⁶³

VPP sets performance-based criteria for managed safety and health systems, invites sites to apply, and assesses applicants against program criteria. The verification process includes an application review and a rigorous on-site evaluation by a team of OSHA safety and health experts.¹⁶⁴ Applicants can be approved into one of three possible programs: Star, Merit, or Star Demonstration.

- Star - The Star program is the elite of the three designations. It is reserved for exemplary worksites with comprehensive, successful safety and health management systems. A company must demonstrate an injury and illness rate at or below the national average in its industry. These sites prove they are self-sufficient in their ability to control safety and health issues at their workplace. Incident rates are reviewed annually, but participating companies are only reevaluated every three to five years.
- Merit - Merit is designed as a stepping stone to the Star designation. Merit companies have good safety and health programs, but they are still in need of some improvement before they can be considered excellent. These companies are judged to have the desire and real potential to achieve star quality performance in three years. Merit companies are evaluated on-site every 18–24 months. They are entitled to one three-year term to reach star status unless the Assistant Secretary of Labor for Occupational Safety and Health approves a second three-year term.
- Star Demonstration - Companies that have achieved Star status may choose to test alternatives to the current Star eligibility and performance requirements. This allows for and encourages innovation in the industry. Programs that show promise or have proven to be successful may result in changes to the Star requirements.

OSHA has also introduced three additional programs: the OSHA Challenge, VPP Corporate, and VPP Construction programs.

- OSHA Challenge - OSHA challenge can be considered an equivalent to a set of training wheels designed to guide, assist, and challenge companies to improve their performance so they can graduate to Merit or Star levels of performance. The Challenge program lays out a series of incremental steps a company can follow to develop and implement effective safety and

¹⁶³ U.S. Department of Labor, Occupational Safety and Health Administration, “All About VPP.”

¹⁶⁴ Ibid.

health management systems. Each step of the process requires certain action, documentation, and outcomes related to VPP criteria. Participants receive recognition at the completion of each stage.

- VPP Corporate - While the VPP program was successful, companies with multiple facilities were still required to submit new applications for each of its locations. The VPP Corporate program was designed to reduce these duplicative requirements. The program is designed to eliminate the redundancy in the VPP application and onsite evaluation processes while maintaining the quality and integrity of the VPP program. Through an application, a company can request acceptance into the VPP Corporate program and, if accepted, all of that company's eligible facilities will follow a streamlined application and on-site evaluation process.
- VPP Construction Program - America's construction industry has unique needs when it comes to occupational safety and health. OSHA recognizes this and has been evaluating pilot programs to develop alternative VPP criteria for construction employers. The goal is to make VPP more accessible to construction employers, especially small employers.

OSHA Star Benefits

- Employers - Employers who earn VPP status reap the rewards of lower workplace injuries and illnesses as well as reduced oversight. Their profits rise as their workers remain more productive and their worker's compensation and insurance-related costs go down. The positive benefits of the program tend to have a ripple effect and VPP sites evolve into models of excellence that influence practices industry-wide.
- OSHA - The government benefits from the VPP programs as well. OSHA reports that it gains a corps of ambassadors who enthusiastically spread the message of safety and health management. These ambassadors also share valuable input into program improvements and augment its limited resources. VPP companies require reduced oversight and resources due to reduced workplace injuries and a reduced potential for such injuries. An additional outgrowth from the program includes the emergence of a non-profit advocacy group, the Voluntary Protection Program Participant's Association. This organization works closely with OSHA and states in the development and implementation of additional cooperative programs. It also provides expertise by commenting and offering stakeholder feedback on agency rulemaking and policies and by providing testimony to Congress on related issues.

OSHA Star remains relevant and successful in part due to its following attributes.

- market-based approach
- benefits for all parties
- voluntary nature
- public/private partnerships
- corporate-based involvement
- inclusive nature
- branding
- effective national campaign
- rewards in the form of public praise
- openness
- willingness to support international inquiries

B. OTHER GOVERNMENTAL INCENTIVE PROGRAMS

The government routinely uses incentive-based programs to encourage certain behaviors and to shape social policy. While the federal income tax system is often a source of frustration, the use of tax incentives has had, and continues to have, significant impact on personal and corporate fiscal practices. A thorough review of the myriad of incentive programs would be a monumental task and is unnecessary for the issue at hand. Instead, four specific programs are good examples that can be used to further this discussion of hazmat motor carrier security programs. The four programs are the National Park Service Historic Preservation Tax Incentives, the Virginia Enterprise Zone program, the Customs-Trade Partnership Against Terrorism (C-TPAT)¹⁶⁵ and its FAST program, and the Port Security Grant Program, which supports requirements of the Maritime Transportation Security Act.

¹⁶⁵ U.S. Customs and Border Protection, “C-TPAT: Customs-Trade Partnership against Terrorism,” http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/ (accessed September 12, 2008).

1. National Park Service Historic Preservation Tax Incentives

The U.S. government encourages the preservation of historic buildings for many reasons. Historic buildings are our link to the past and help give a community a sense of identity, stability, and orientation.¹⁶⁶ One particular program makes federal tax incentives available to those who rehabilitate historic structures.¹⁶⁷ The Federal Historic Preservation Tax Incentives program is one of the federal government's most successful and cost-effective community revitalization programs.¹⁶⁸ In addition to federal tax benefits, some states will increase the incentive by providing state tax benefits as well.

In this program, the federal government has chosen to offer a 20% tax credit for certified rehabilitation of certified historic structures and a 10% tax credit for the rehabilitation of non-historic, non-residential buildings built before 1936. It is important to note that owners are receiving a tax *credit*, not a tax *deduction*. The difference is substantial. Where a tax deduction lowers the amount of income subject to taxation, a tax credit lowers the amount of tax owed dollar for dollar.

To obtain the tax credit, before they start work, owners must submit an application describing the rehabilitation projects they plan to complete and receive a certification decision that the plans fall within the requirements of the program. Once the work is completed, the applicant must submit a request for certification of completed work along with a full accounting of the money spent on the project as independently verified in writing by a licensed accountant. If all work meets program requirements and the applicant pays the requisite processing fees, then the program office will issue the paperwork necessary to claim the tax credit.

¹⁶⁶ National Park Service, "Historic Preservation Tax Incentives," <http://www.nps.gov/hps/tps/tax/index.htm> (accessed September 12, 2008).

¹⁶⁷ Treasury Regulation Section 1.48-12.

¹⁶⁸ National Park Service, "Historic Preservation Tax Incentives."

2. Virginia's Enterprise Zone Program

The state of Virginia established the Virginia Enterprise Zone Act¹⁶⁹ in 1982 to encourage new business activity in specified geographic areas by providing state and local tax relief and grants, regulatory flexibility, and local infrastructure development.¹⁷⁰ Typically, an enterprise zone will be formed in an economically depressed area with few jobs and crumbling infrastructure. The program seeks to spur private investment to rehabilitate structures and create new jobs by encouraging the opening of new businesses. To date, qualified enterprise zone applicants have created more than 39,000 jobs and spent more than \$800 million in qualified investments within the enterprise zones.¹⁷¹

The enterprise zone program is designed to complement other local, state, and federal economic development activities and is not intended as a stand-alone program.¹⁷² In general, the state offers Job Creation grants and Real Property Investment grants. The state will allocate a specific amount of grant funds for each fiscal year. To be eligible for these funds, investors must apply for the program, follow the rules, and submit accounting records certified by an independent certified public accountant licensed in the state. If all requirements are met, the applicant will receive a grant check reimbursing him for his qualified expenses. If the sum total of qualified applicant spending exceeds the amount of grant funds allocated for that year, the funds will be distributed on a prorated basis.¹⁷³

3. Free and Secure Trade

The governments of Canada and Mexico each worked with the U.S. Department of Customs and Border Protection (CBP) to design a border accord initiative to ensure

¹⁶⁹ Section 59.1-270 through 59.1-284 of the Code of Virginia.

¹⁷⁰ Virginia Department of Housing and Community Development, "Virginia Enterprise Zone Program," http://www.dhcd.virginia.gov/CommunityDevelopmentRevitalization/Virginia_Enterprise_Zones.htm (accessed September 12, 2008).

¹⁷¹ Ibid.

¹⁷² Virginia Economic Development Partnership, "Virginia's Enterprise Zone Program," www.virginiaallies.org/pdfs/Articleonlocalenterprisezones.pdf (accessed September 12, 2008).

¹⁷³ Ibid.

security and safety while also enhancing each others' economic prosperity. Each country started with its own processes for clearing commercial shipments at the border with the United States and then developed the FAST program to streamline those processes so that freight could move more quickly between the countries. The program is completely voluntary and addresses all phases of the commercial shipping process including commercial drivers, carriers, importers, and manufacturers.

- **Commercial Drivers** - To participate in the FAST program, drivers must undergo a background check and be admissible to the U.S. and Canada. If approved, the driver is issued a FAST driver card that provides such benefits as expedited processing and the use of a dedicated FAST lane where available.
- **Approved Carriers** - Carriers who participate in the FAST program can gain expedited clearance into the United States if they demonstrate a history of complying with all legislative and regulatory requirements, enter into an agreement with CBP, provide a completed security profile to CBP, and make a commitment to security-enhancing business practices as required by C-TPAT.
- **Approved Importers** - Importers can take advantage of the FAST program if they develop a sound plan to enhance security procedures throughout their supply chain. If an importer does not control a facility, conveyance, or process, they must make reasonable efforts to secure compliance by the responsible parties. Importers must successfully pass a C-TPAT risk assessment before acceptance into the program.
- **Manufacturers** - Manufacturers exporting to the United States from Mexico who pack and prepare their own materials for shipping in a facility that they own and control are eligible for C-TPAT approval. Manufacturers must successfully pass a C-TPAT risk assessment before acceptance into the program.
- **Program Benefits** - FAST participants gain access to dedicated FAST lanes for clearance of trans-border shipments, are subject to a reduced number of examinations for continued compliance, and receive secondary priority processing. These process efficiencies can add up to increased profits for participants. The government also benefits through increased security assurances and the ability to preprocess participants so that it can allocate resources to higher risk cargo at border crossings.

4. Port Security Grants Program

In 2003, DHS, through the United States Coast Guard (USCG), issued regulations supporting the Maritime Transportation Security Act of 2002.¹⁷⁴ Section 104 of these regulations establishes security requirements for maritime vessels. In many respects, maritime vessels are similarly situated to highway motor carriers in that they are privately owned, rely on the use of governmental conveyances such as ports or roads, and are responsible for implementing their own security measures. While USCG issued vessel security requirements similar to what DOT has issued for motor carriers, USCG has supported the implementation of those requirements through its PSGP.

The PSGP recognizes that the vast bulk of U.S. critical infrastructure is owned and/or operated by state, local, and private sector partners and that each port area has specific individual needs and tested experience about how best to reduce risk within their region.¹⁷⁵ The grant investment strategy establishes two priorities: risk-based funding and regional security cooperation.¹⁷⁶ Therefore, it makes federal funds available not only to governmental actors such as maritime terminals, facilities, port authorities, and other state and local agencies that provide layered security protection for federally regulated facilities, but also directly to federally inspected passenger vessels or stakeholders required to provide services as specified in a vessel security plan.¹⁷⁷

In order to receive funds, an application must be filed by a published cut-off date. Applications received will be reviewed according to port area for compliance with security plan requirements and funding priorities articulated by the government. Next, a National Review Panel will convene to identify a prioritized list of projects for funding. This list will be run through a risk-based algorithm and returned to the National Review Panel for completion of a final ranked list from which funds distribution will be made.¹⁷⁸

¹⁷⁴ Maritime Transportation Security Act of 2002, Pub. L. No. 107-295 (2002).

¹⁷⁵ U.S. Department of Homeland Security, *Fiscal Year 2008 Port Security Grant Program, Program Guidance and Application Kit* (February 2008), 1.

¹⁷⁶ *Ibid.*, 2.

¹⁷⁷ *Ibid.*, 7–8.

¹⁷⁸ *Ibid.*, 16–18.

In this model, public sector applicants are required to provide matching funds of at least 25% and private sector applicants must provide matching funds of at least 50%. Grant awards of \$25,000 or less do not require matching funds.¹⁷⁹ In this program, funds are allocated based on application and prior approval of a given project, not application and reimbursement after the fact. This process, while fiscally responsible, does have one drawback, which is that it can cause a delay in security project implementation while paperwork is processed.

C. SUMMARY

There are virtually unlimited options available to the government to steer public policy and participation. In a capitalistic market-driven economy, incentives through benefits work well. Benefits range from monetary, such as tax incentives, credits, or grants, to non-monetary means, such as faster processing or less oversight. Each of these options can be employed in multiple ways. Monetary benefits can be pre-approved, reimbursed after the fact, or show up as tax incentives or grants. They also can be used to stretch the government's budget dollars by requiring some form of direct or indirect matching funds from private investors. Most government programs can be improved when driven by incentive-based options.

¹⁷⁹ U.S. Department of Homeland Security, 20.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. SOLUTION

A. SECURITY THROUGH ASSESSED RISK (STAR) PROGRAM

Hawley supports a risk-based approach to security.¹⁸⁰ He applies this approach to new initiatives¹⁸¹ and when revisiting old problems.¹⁸² A risk-based approach essentially requires first that one assess the risk associated with a particular security issue and then craft a response tailored to address the higher risks first. If developed, a TSA STAR program could apply a risk-based model to the hazmat carrier security issue in a way that fills gaps. While no answer can be perfect, the STAR program as proposed allows TSA to provide for a reasonable degree of security through individually tailored risk reduction programs.

Small intrastate companies hauling flammable liquids and liquefied gases are arguably at high risk for exploitation by terrorists. Current hazmat security programs offer little protection for these carriers. Therefore, it is important to develop a security program that does not require increased cost or staffing for government or industry and that can be implemented rapidly.¹⁸³ The STAR program as proposed addresses all of these issues and more. The program is voluntary but provides that certain rigorous requirements be met to earn the STAR status.

B. REQUIREMENTS TO EARN STAR STATUS

Hazmat carriers transporting any type of hazardous materials will be encouraged to participate in the STAR program on a strictly voluntary basis. To participate, the following will be required:

¹⁸⁰ Transportation Security Administration, “Risk Management,” <http://www.tsa.gov/approach/risk/index.shtm> (accessed October 22, 2008).

¹⁸¹ Transportation Security Administration, “Where We Stand,” http://www.tsa.gov/press/where_we_stand/training.shtm (accessed October 22, 2008).

¹⁸² Transportation Security Administration, “DHS Traveler Redress Inquiry Program (DHS TRIP),” <http://www.tsa.gov/travelers/customer/redress/index.shtm> (accessed October 22, 2008).

¹⁸³ HSPD-7 requires rapidly implemented tactical security enhancements.

- Application - Each carrier must submit an application and receive written verification from TSA that they are eligible to participate in the STAR program.
- Security Threat Assessment - Applicants must then contract with an independent consultant approved by TSA to conduct a security threat assessment of their operation, including drivers, vehicles, and facilities incidental to transport. Such assessments can also be completed by state inspectors if TSA develops agreements with states to do so. The consultant will follow guidelines established by TSA¹⁸⁴ and will draft a report noting any security deficiencies and include recommendations to correct those deficiencies. All deficiencies must be corrected before acceptance into the program. An example of a requirement could be that a carrier with certain risks must install a panic alarm system in their trucks.
- Background Check - Carriers must ensure that background checks on drivers and plant personnel are completed and up to date. Background checks must meet the standards set by TSA. Most personnel will already have gone through a background check, as it is a requirement to obtain a hazmat endorsement or TWIC card. Only individuals with successful background checks will be afforded access to hazmats.
- Security Training - All personnel will be required to complete security training designed for their particular type of operation. This requirement will be a good way to start accomplishing the original goals of the Highway Watch program.
- Insurance - All participants must maintain a specified amount of liability insurance or prove that they are successfully self-insured for that same amount.
- Reporting - Participants will agree that as a condition of membership they will report any security incidents¹⁸⁵ to TSA. Reporting can be anonymous, but participants will have to sign an annual certification that they have reported all security incidents that have occurred over the previous year. This allows TSA to begin to build a database that eventually can be useful in determining security trends and in assessing best practices.
- Signed Pledge - The CEO of each carrier will be required to sign a pledge of support for the STAR program and display that document in an area viewable by all employees. This reaffirms corporate support for the program.

¹⁸⁴ TSA can readily establish these guidelines based on its current voluntary Security Action Items.

¹⁸⁵ TSA will need to provide guidance and a definition of a “security incident.”

- Independent Certification of Compliance - The independent individual conducting the security threat assessment must provide a signed document certifying that the particular carrier has complied with all elements of the program as the final step of the application process before a carrier can earn STAR status.
- Bi-annual Recertification - Participants will be required to recertify their compliance every two years. This maintains the integrity of the program.

In order to encourage industry participation, TSA should not charge an application fee, although the option exists to charge a fee to offset the costs of program administration. Carriers will not be exempt from any current processing fees, such as those required for background checks, and will also have to pay for the threat assessment and certification of compliance.

C. BENEFITS TO PARTICIPANTS

Those carriers who choose to participate in the program and who earn STAR status will be entitled to the following benefits of membership:

- TSA STAR Contact Desk - Allocated TSA employees will be available to all participants to assist them with program compliance issues.
- One Stop Background Checks - TSA will arrange for a single background check that will be sufficient for a hazmat driver's license endorsement, TWIC card application, and the FAST program, as well as any future programs that require a background check.
- Grants - Carriers who were required to spend money to purchase security equipment to comply with the requirements of a security threat assessment will be eligible to apply for TSA grant money. This program can be administered in multiple ways. Three suggestions are the following:
 - Direct reimbursement after the fact for installation of security devices whose installation was pre-approved by TSA. All expenses up to a certain amount per truck will be fully reimbursable and any expenses beyond the predetermined amount will require a matching contribution from the carrier. The certification of compliance will serve as a receipt and proof of installation.
 - Direct reimbursement for installation of security devices in a manner similar to the Enterprise Zone model. A predetermined fund will be allocated each fiscal year to support the program. All

applications for reimbursement will be due by a certain date and all successful applications will receive reimbursement from the fund in full or on a prorated basis based on the available funds.

- Tax credits equal to a specified percentage of the cost to install security devices. The credit can be for any amount from 1% to 100% of the cost. This option is a good option if TSA does not have direct grant funds available but the government makes a policy decision that offers a tax credit, which is an effective and desired way to encourage installation of security devices.

A very effective tactic here under any option would be to reimburse only a percentage of costs. This model effectively increases the overall amount of money spent on security and encourages the actual user to pay a portion of the bill. This is a useful way to stretch TSAs security budget.

- Insurance Discounts - Members could receive discounts on their insurance coverage for STAR compliance and earning preferred risk status. Alternatively, they could receive discounts equal to the amount they were required to pay for the security threat assessment and the certification of compliance. This should be acceptable to insurance companies because, if a carrier earns STAR status, the insurer can be confident that they are purchasing a preferred risk. This same model is already in place for members of the Responsible Distribution Process.SM Members currently receive a discount on their insurance premiums equal to the amount of money they were required to pay to comply with the verification process.¹⁸⁶ Additionally, insurance companies have already spoken with TSA about offering these discounts to carriers who practice security measures in line with TSA's standards.¹⁸⁷
- STAR Security Panel Membership - Each STAR member will become a member of the state or federal (or both, depending on where they conduct their business) security panel. These panels will be made up of colleagues and state and local officials and may choose to invite members of supporting communities when appropriate, such as the insurance industry or the security technology industry. The panels will meet to discuss issues members have with federal, state, or local policies or programs and security issues relevant to their area and to share best practices. This program starts to bring the state and local governments back into the process.

¹⁸⁶ Mike Lang, PMP Director, Responsible Distribution Process, National Association of Chemical Distributors, interviewed by author.

¹⁸⁷ William Arrington, General Manager, TSA Highway and Motor Carrier Programs, interview by author, Arlington, VA: July 27, 2007.

- STAR Seal of Approval - Members can proudly display the STAR seal of approval and use the status to build their business. Currently, members of the Responsible Distribution ProcessSM and the Responsible Care® programs report an increase in business from manufacturers and distributors who seek them out because they know they are doing business with responsible, secure partners. This factor lowers liability concerns for all parties. This single aspect of the STAR program will take advantage of free-market economics by decreasing business to non-members due to the desire of members to switch their business relationships to do business with other members. This free-market effect will eventually drive non-secure or less secure carriers to either step up to the plate and enhance their security or be marginalized.
- Awards - Members will be eligible for one or more annual awards recognizing superior security practices. Recognition from rewards programs is coveted by many and again is a good business builder. A recent winner of a similar award from the Responsible Care® program reported an increase in employee morale when the employees realized that they belonged to an elite company.¹⁸⁸
- Secure Workforce - Once a carrier completes the requirements for membership, it can be confident that it employs a better-trained and more secure workforce. This is likely to result in reduced negative incidents and thus reduced liability costs.
- Individual Control - Carriers that adopt their own security measures and install their own security devices will maintain better and closer control of their security. There will be no need for a federal truck tracking center because carriers who require tracking will be able to either do so themselves or contract with a private sector carrier who will track their trucks for them.

D. BENEFITS TO THE GOVERNMENT

TSA will also benefit in numerous ways from the STAR program. Benefits include the following:

- Risk-Based Security - A key factor in securing any industry against terrorism is to adopt random security measures. Regulations are detrimental to security sometimes because they inform all people, including terrorists, about what security measures are in place and thus inherently about what security measures are not in place. Also terrorists can learn the vulnerabilities and develop workarounds for mandated

¹⁸⁸ David P. Gleason, Senior Director, Responsible Care, American Chemistry Council, interviewed by author, July 15, 2008.

security measures. When individual carriers have to comply with individual risk-based security threat assessments, they will each develop security plans and install security devices unique to their needs. This randomness has an effect much greater than just the security of STAR members. It actually provides a broad net of security for all. This is true because terrorists will be unsure of which companies are STAR members and even if they know that, they will not know which companies have installed which security devices. This randomness puts too much risk into planning a terror attack and the terrorist will be encouraged to look elsewhere.

- Broad Coverage - Because all hazmat carriers will be entitled to become members, the non-HSSM carriers will be brought into the security fold. While TSA may choose to pursue additional security requirements for HSSM carriers, all carriers will continue to benefit from membership.
- Rapid Implementation - TSA maintains that it would like to eventually issue regulations for HSSM carriers. This model is certainly workable, but due to the nature of the regulatory process, it is highly unlikely that any regulation will be issued soon. The STAR program will require some setup time, but because it is voluntary, does not rely on government regulation or Congressional action, takes advantage of personnel and processes already in place, and the industry has expressed a desire to participate in such a program,¹⁸⁹ it should be relatively easy to implement.
- Metrics - Because members will be required to submit certifications of compliance, TSA will be able to track how many members they have and what types of security are being implemented. Also, because carriers will be required to report security incidents, TSA can begin to collect data on such incidents that they can use to evaluate security programs, trends, and best practices.
- Training - Since security training is a requirement under the program, TSA will be assured that the type of training it hoped to accomplish with the Highway Watch program is continuing. TSA can verify this because completion of the training requirement will be certified by an independent certifier.
- Public/Private Partnerships - Various aspects of the STAR program rely on partnerships. The program will establish the need for partnerships with independent threat assessors and certifiers, certified trainers, and security equipment dealers and installers. The state can also choose to use their inspectors as certifiers because this process can complement other state duties. There will also be a need for a partnership with the insurance industry to develop the insurance requirements. Additionally, the

¹⁸⁹ Mike Lang, PMP Director, Responsible Distribution Process, National Association of Chemical Distributors, interviewed by author, June 25, 2008.

background check program will foster partnerships with state and federal agencies who work with hazmat driver's license endorsements and the TWIC and the FAST programs. Finally, the STAR security panel will require partnerships with federal, state, local, and tribal governments; hazmat carriers; and assorted members of industry. All of these relationships help impress upon the industry its role as an active part of a national security program.

- Public Confidence - TSA will gain public confidence in its security abilities when news of the expanded security coverage for all HSSM and non-HSSM carriers is announced. Additionally, if a concerted effort is made to build the STAR brand, this will also serve well as a positive public face for TSA's efforts.

THIS PAGE INTENTIONALLY LEFT BLANK

X. POST-SOLUTION (THE DAY AFTER)

It's 9:15 am on black Friday, 2009. Shoppers have been lined up at the malls since 7:30 am to take advantage of the special offers the retailers have advertised as incentives to encourage a full day of shopping. The malls are crowded and the holiday season has been festive.

It's 9:15 am on black Friday, 2009. Bud Wilson pulls his fuel tanker into a Shell station to make his first delivery for the day. He parks his truck near the fuel tanks, takes his keys, gets out, and locks his door before he meets with the station manager to get his manifest signed.

It's 9:15 am on black Friday, 2009. Adham has been waiting by the pay phone for Bud to arrive. Bud always delivers on Friday and always on time. Adham quietly walks over to the unattended fuel truck, tries the door, and finds it locked.

Adham pulls his knife and approaches Bud demanding the keys to the truck. A struggle ensues. The station manager calls 9-1-1 to report the incident, but Bud is hurt, and Adham manages to get the keys, start the truck, and begins to drive off. Fortunately, Bud's company underwent a security threat assessment and installed remote panic buttons on their trucks in order to become a TSA STAR member. Bud reaches for his transmitter and pushes the panic button. A signal is sent to his dispatcher and the engine of the truck slowly winds down. The police are now just down the block and Adham cannot get the truck to restart. He tries again and again, but the engine is dead. Soon, a police officer is pulling him from the cab and wrestling him to the ground. The same scenario is repeated in four other major American cities.

Almost a month later on Christmas day, children all over America are smiling at the abundance of gifts under their trees. Retailers all across the country are reporting record profits. Life is good. Things didn't have to turn out this way, but the government knew of the threat and the government decided to act.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- American Chemistry Council. "Ensuring Accountability through Management System Certification." http://reporting.responsiblecare-us.com/reports/rcmsc_cmpny_rpt.aspx (accessed October 14, 2008).
- . "Performance through Responsible Care." http://www.americanchemistry.com/s_responsiblecare/doc.asp?CID=1298&DID=5084 (accessed October 14, 2008).
- . "Responsible Care." http://www.americanchemistry.com/s_responsiblecare/sec.asp?CID=1298&DID=4841 (accessed October 14, 2008).
- . "Responsible Care Security Code." http://www.americanchemistry.com/s_responsiblecare/doc.asp?CID=1298&DID=5085 (accessed October 14, 2008).
- . "Responsible Care Toolkit." http://www.americanchemistry.com/s_rctoolkit/index.asp (accessed October 22, 2008).
- Arrington, William. General Manager. TSA Highway and Motor Carrier Programs. Interview by author. Arlington, VA, July 27, 2007.
- Bloquist, Brian, and Tracy Connor. "Cops Nab Ten in Haz-mat Scheme." *The New York Post*, September 27, 2001.
- Canada Border Services Agency. "Free and Secure Trade." <http://www.cbsa-asfc.gc.ca/prog/fast-expres/menu-eng.html> (accessed October 14, 2008).
- Chinni, Dante. "America's Roads May Be Just as Vulnerable as Its Skies." *The Christian Science Monitor*, October 1, 2001.
- Clayton, Mark. "Hazardous-Materials Trucks: Terror Threat?" *Christian Science Monitor*, July 7, 2006. <http://www.csmonitor.com/2006/0707/p02s01-usgn.html> (accessed March 11, 2008).
- Decision Support System for a National HAZMAT Truck Tracking Center.* Charlottesville, VA: The Accelerated Masters Program in Systems Engineering, 2007.
- Department of Homeland Security, Office of Inspector General. *Administration of the Federal Trucking Industry Security Grant Program for FY 2004 and FY 2005* (October 29, 2007).

———. *Fiscal Year 2008 Port Security Grant Program Guidance and Application Kit* (February 2008).

Federal Emergency Management Agency. “Fiscal Year 2008 Port Security Grant Program Guidance and Application Kit.”
http://www.fema.gov/pdf/government/grant/psgp/fy08_psgp_guidance.pdf
(accessed October 14, 2008).

———. “FY 2009 Port Security Grant Program (PSGP).”
<http://www.fema.gov/government/grant/psgp/index.shtm> (accessed October 14, 2008).

Gleason, David P. Senior Director, Responsible Care. American Chemistry Council.
Interview by author. July 15, 2008.

Hawley, Kip. Assistant Secretary, Transportation Security Administration. Statement
before the Committee on Commerce, Science, and Transportation, United States
Senate (January 18, 2007).

———. Statement before the Subcommittee on Homeland Security, Committee on
Appropriations, United States House of Representatives.

*Hazardous Materials Safety and Security Technology Field Operational Test Volume I:
Evaluation Final Report Executive Summary*. McLean, VA: SAIC, 2004.

Lang, Mike. PMP Director. Responsible Distribution Process, National Association of
Chemical Distributors. Interview by author.

———. Interview by author, June 25, 2008.

Loewenberg, Samuel. “Truckers Lose DHS Contract.” *Politico*, May 16, 2008.
<http://www.politico.com/news/stories/0508/10412.html> (accessed September 12,
2008).

National Association of Chemical Distributors. “Code of Management Practice.”
http://www.nacd.com/dist_process/rdpcode.aspx (accessed October 14, 2008).

———. “Guiding Principles.” http://www.nacd.com/dist_process/rdpguide.aspx (accessed
October 14, 2008).

———. “Measuring the Impact of the Responsible Distribution Process on Environmental,
Health, Safety, & Security Performance.”
http://www.nacd.com/dist_process/rdp_indices_members.aspx (accessed October
14, 2008).

- . “RDP Compliance Timetable for NACD Candidates.” http://www.nacd.com/dist_process/rdp_compliance.aspx (accessed October 14, 2008).
- . “Responsible Distribution Process.” http://www.nacd.com/dist_process/ (accessed October 14, 2008).
- . “Third Party Verification.” http://www.nacd.com/dist_process/rdpverification.aspx (accessed October 14, 2008).
- National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004.
- National Hazardous Material Commercial Vehicle Tracking System Study*. Charlottesville, VA: Accelerated Solutions, 2006.
- National Park Service. “Historic Preservation Tax Incentives.” <http://www.nps.gov/hps/tps/tax/index.htm> (accessed September 12, 2008).
- . “Historic Preservation Tax Incentives.” <http://www.nps.gov/history/hps/tps/tax/brochure1.htm> (accessed October 14, 2008).
- . “Historic Preservation Certification Application.” <http://www.nps.gov/hps/tps/tax/hpcappl.htm> (accessed October 14, 2008).
- . “Incentives!” <http://www.nps.gov/hps/tps/tax/incentives/index.htm> (accessed October 14, 2008).
- President. “Critical Infrastructure Identification, Prioritization, and Protection.” Homeland Security Presidential Directive 7 (December 17, 2003).
- . Executive Order 13416. “Strengthening Surface Transportation Security,” *Federal Register* 71, no. 235 (December 7, 2006): 71033.
- Report on FMCSA’s Security Sensitivity Visits to the House and Senate Committees on Appropriations* (January 31, 2002).
- Responsible Distribution Process Code Coordinator Manual 2008*. Arlington, VA: National Association of Chemical Distributors, 2008.
- Roggio, Bill. “Another Chlorine Truck Bomb Found Near Ramadi.” *The Long War Journal*, March 27, 2007. http://www.longwarjournal.org/archives/2007/03/another_chlorine_tru.php (accessed March 18, 2008).
- Sammon, John. Letter to Highway and Motor Carrier Stakeholders, June 26, 2008.

Stock, D., et al. *Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis*. Washington, D.C.: Federal Motor Carrier Safety Administration, U.S. DOT, 2004.

Transportation Security Administration Mission Statement.

http://www.tsa.gov/who_we_are/mission.shtm (accessed December 11, 2008).

Transportation Security Administration. "DHS Traveler Redress Inquiry Program (DHS TRIP)." <http://www.tsa.gov/travelers/customer/redress/index.shtm> (accessed October 22, 2008).

———. "Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs)." http://www.tsa.gov/what_we_do/tsnm/highway/hssm_sai.shtm (accessed October 22, 2008).

———. "Programs." http://www.tsa.gov/what_we_do/tsnm/highway/programs.shtm (accessed October 22, 2008).

———. "Risk Management." <http://www.tsa.gov/approach/risk/index.shtm> (accessed October 22, 2008).

———. "Where We Stand." http://www.tsa.gov/press/where_we_stand/training.shtm (accessed October 22, 2008).

———. "Transportation Worker Identification Credential (TWIC)." http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed April 2, 2008).

———. "TSA Teams Up With American Trucking Associations to Prevent and Respond to Terrorism." (March 23, 2004) http://www.tsa.gov/press/releases/2004/press_release_0405.shtm (accessed July 29, 2008).

U.S. Customs and Border Protection. "C-TPAT: Customs-Trade Partnership against Terrorism." http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/ (accessed September 12, 2008).

———. "FAST: Free and Secure Trade Program." http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/fast/ (accessed October 14, 2008).

———. "What Is Customs-Trade Partnership against Terrorism (C-TPAT)?" http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ (accessed October 14, 2008).

U.S. Department of Energy and Environmental Protection Agency. "About Energy Star." http://www.energystar.gov/index.cfm?c=about.ab_index (accessed October 14, 2008).

- . “Energy Star.” <http://www.energystar.gov/> (accessed October 14, 2008).
- . “Energy Star Overview of 2007 Achievements.” <http://www.energystar.gov/ia/partners/publications/pubdocs/2007%20CPPD%204pg.pdf> (accessed October 22, 2008).
- . “Energy Star Partners.” http://www.energystar.gov/index.cfm?c=news.nr_partners (accessed October 14, 2008).
- . “Fall 2008 Energy Star News.” http://www.energystar.gov/index.cfm?c=news.nr_fall2008 (accessed October 14, 2008).
- . “History of Energy Star.” http://www.energystar.gov/index.cfm?c=about.ab_history (accessed July 23, 2008).
- . “Major Milestones.” http://www.energystar.gov/index.cfm?c=about.ab_milestones (accessed October 14, 2008).
- U.S. Department of Labor, Occupational Safety and Health Administration. “All About VPP.” http://www.osha.gov/dcsp/vpp/all_about_vpp.html (accessed October 14, 2008).
- . “Policies and Procedures.” http://www.osha.gov/dcsp/vpp/vpp_policy.html (accessed October 14, 2008).
- . “Voluntary Protection Programs.” <http://www.osha.gov/dcsp/vpp/index.html> (accessed October 14, 2008).
- Virginia Department of Housing and Community Development. “Virginia Enterprise Zone Program.” http://www.dhcd.virginia.gov/CommunityDevelopmentRevitalization/Virginia_Enterprise_Zones.htm (accessed October 14, 2008).
- Virginia Economic Development Partnership. “Virginia’s Enterprise Zone Program.” www.virginiaallies.org/pdfs/Articleonlocalenterprisezones.pdf (accessed September 12, 2008).
- White House, The. “United States – Canada Free and Secure Trade Program.” <http://www.whitehouse.gov/news/releases/2002/09/20020909-3.html> (accessed October 14, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California