



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**CHEMICAL FACILITY PREPAREDNESS:
A COMPREHENSIVE APPROACH**

by

Daniel Pennington

September 2006

Thesis Advisor:
Second Reader:

Ted Lewis
Gary Ackerman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
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 September 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Chemical Facility Preparedness: A Comprehensive Approach			5. FUNDING NUMBERS	
6. AUTHOR(S) Lieutenant Daniel Pennington				
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 A	
13. ABSTRACT (maximum 200 words) Across the country thousands of facilities use, manufacture, or store large stockpiles of toxic and/or flammable substances. Many sites are clustered together in densely populated areas. If terrorists cause catastrophic chemical releases or explosions at these key facilities, large numbers of Americans will be put at risk of injury or death. Such attacks may also have a devastating impact on the U.S. economy. Surprisingly, in light of these risks most chemical sites have not implemented adequate measures to prevent, mitigate, deter, and/or respond to terrorist attacks. This thesis proposes that private and public sectors partner together to improve the preparedness of chemical facilities for acts of terrorism. More specifically, key stakeholders from both sectors need to forge Regional Defense Units (RDUs). Their primary purpose is to effectively reduce the attractiveness of regional chemical facilities as targets for terrorists. To achieve this goal, a mixture of mandates ("sticks") and incentives ("carrots") need to be regionally developed, implemented, and sustained by RDUs. Collaborative regional efforts using an appropriately balanced and community-governed "carrot and stick" approach can be the most effective option for federal policymakers and the Department of Homeland Security to improve chemical facility preparedness, and thus homeland security.				
14. SUBJECT TERMS Critical Infrastructure, Private – Public Partnerships, Department of Homeland Security, Chemical Facilities, Disasters, Mandates, Legislation, Incentives/Disincentives, Regional Defense Units, Vulnerabilities, Minimum Security Standards, Vulnerable Zone, Risk Management Plans, Local Emergency Planning Committees, Trade Associations			15. NUMBER OF PAGES 101	
			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 UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CHEMICAL FACILITY PREPAREDNESS: A COMPREHENSIVE APPROACH

Daniel W. Pennington
Lieutenant, City of Pasadena, Texas Police Department
B.S., University System of Texas, Houston University, 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
September 2006**

Author: Daniel Pennington

Approved by: Ted Lewis
Thesis Advisor

Gary Ackerman
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Experts agree that the nation's chemical facilities are attractive targets for terrorists. This consensus is due to several conditions. First, there are thousands of facilities scattered across the country that use, manufacture or store large stockpiles of toxic and/or flammable substances. Many sites are clustered together in densely populated areas and are poorly protected. If terrorists cause catastrophic chemical releases or explosions at these key facilities, large numbers of Americans will be put at risk of injury or death. Second, such attacks may also have a devastating impact on the U.S. economy because so many other industries are dependent on a properly functioning chemical sector. Surprisingly in light of these risks, most chemical sites have not implemented sufficient measures to prevent, mitigate, deter, and/or respond to terrorist attacks. Although governmental entities (local, state and federal) and the chemical industry have initiated some safeguards, they only apply to a limited number of chemical facilities. The vast majority is still not adequately prepared for terrorism.

This thesis proposes that private and public sectors should partner together to improve the preparedness of the chemical industry for terrorist acts. More specifically, key stakeholders from both sectors need to forge Regional Defense Units (RDUs). Their primary purpose is to effectively reduce the attractiveness of local chemical facilities as targets for terrorists without unduly hampering their operations. To achieve this goal, a mixture of mandates ("sticks") and incentives ("carrots") need to be regionally developed, implemented and sustained by RDUs. Collaborative regional efforts using an appropriately balanced and community-governed "carrot and stick" approach can be the most effective option for the Department of Homeland Security to improve chemical facility preparedness, and thus homeland security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	OVERVIEW.....	1
A.	INTRODUCTION.....	1
B.	DEFINING THE PROBLEM.....	1
1.	The Relevance of This Problem	3
2.	Thesis.....	3
3.	Literature Review	4
4.	Unexplored Areas.....	11
5.	Methodology	14
II.	EVOLUTION OF THE PROBLEM.....	17
A.	CHEMICAL FACILITY HISTORY	17
1.	Tragedy in Texas City, Texas	17
2.	Federal Safety Efforts.....	17
3.	The Catastrophe in Bhopal, India	18
4..	Private and Public Sector Responses to the Release in Bhopal	19
5.	Current Situation	20
6.	Lessons Learned from Disasters.....	21
III.	PUBLIC-PRIVATE PARTNERSHIPS	23
A.	INTRODUCTION.....	23
B.	CONDITIONS SUPPORTING PARTNERSHIPS.....	23
C.	PARTNERSHIP ALTERNATIVES	24
D.	INPUTS, OUTPUTS, & OUTCOMES	25
E.	SWOT ANALYSIS & STRATEGIC ISSUE DEVELOPMENT	27
1.	What can DHS do to Improve Chemical Facility Preparedness Nationwide?	30
2.	How does DHS Define a “Unified National Effort”?	30
3.	How can DHS Engage Public-Private Partners in Preparedness Efforts?.....	31
F.	PROPOSED STRATEGIC IDEA	31
G.	BENCHMARKING	34
H.	IMPLEMENTATION	36
I.	PILOT INITIATIVE	42
J.	SUMMARY OF JOINT PREPAREDNESS EFFORTS	43
IV.	COMPARATIVE GOVERNMENT ANALYSIS	45
A.	A MIXED BAG OF APPROACHES	45
B.	CURRENT MANDATES.....	45
1.	Local	45
2.	State.....	47
3.	Federal	48
C.	ANALOGOUS PROBLEMS	49

1.	Nuclear Facilities.....	49
2.	Public Health Security & Bioterrorism Preparedness & Response Act.....	51
D.	PROPOSED LEGISLATION.....	52
E.	SUMMARY OF APPROACHES	54
V.	INCENTIVES.....	57
A.	INTRODUCTION.....	57
B.	INDUSTRY TRADE ASSOCIATIONS	58
C.	BUFFER ZONE PROTECTION PROGRAM GRANT.....	60
D.	INSURANCE MEASURES.....	62
E.	TAX PROVISIONS	65
F.	MISCELLANEOUS PROGRAMS	67
G.	SUMMARY OF APPROACHES	69
VI.	CONCLUSION	71
A.	POSITION.....	71
B.	POLICY RECOMMENDATIONS	79
1.	Action Steps	79
C.	SUMMARY	81
	LIST OF REFERENCES.....	83
	INITIAL DISTRIBUTION LIST	89

ACKNOWLEDGEMENTS

While contemplating my acknowledgement comments, I had somewhat of an epiphany. I realized that I could dispense my words of appreciation to those who have helped me with my thesis much in the way that chemical facility security should be implemented----in a layered approach. First, there is an outer ring of people to thank. These are friends who have aided me through this entire body of work. In particular they include Ted Lewis, Gary Ackerman, Lauren Wollman and Greta Marlatt. All were very patient, instructive and readily available during my 18-month journey. Their guidance was critical to the completion of this project. Also of benefit were the entire CHDS staff, my classmates, and personnel at the Pasadena Police Department.

Next, I have an inner ring of family members to thank. They need to know that I am especially grateful for their love and understanding of my desire to undertake this challenge. I am extremely appreciative for the extra support my family provided to me over the last year and a half. I will attempt but probably never be able to make up for the concessions the three of them made for me. Allene, Kelsey, and Catie, I love you each so very much.

Last, there is a center core that deserves the greatest thanks. This encompasses my faith which I have relied on throughout not only this program, but my life as well. It nourishes and sustains me. It was of particular importance with completion of the thesis. Whenever I became overly stressed about pending milestones I reminded myself that the Bible says God will not give me more than I can handle. Somehow, the deadlines were always met. I am so appreciative of all that God has blessed me with. But most of all I am thankful for His son, Jesus Christ, and the gift of grace.

In summary, all three rings were vital to the completion of this thesis. Accordingly, I want to acknowledge the role that each played and express my sincere appreciation. In short, rings of thanks for my faith, family, and friends.

THIS PAGE INTENTIONALLY LEFT BLANK

I. OVERVIEW

A. INTRODUCTION

The events of September 11, 2001, ushered in a new paradigm for many Americans. In an instant, the threat of terrorism became the top public concern. Accordingly, it became necessary for government to identify and prioritize the country's vulnerable critical infrastructure. Afterwards, both the private and public sectors began to initiate efforts to safeguard the nation's highest risk targets.

It has been almost five years since 9/11, and many of the nation's most critical infrastructure vulnerabilities have been mitigated. However, little has been done to reduce the attractiveness of chemical facilities as targets of terrorism, even though some experts believe they are America's Achilles' heel. The fact that there are tens of thousands of chemical facilities scattered across the nation exacerbates this issue. Yet, there is not a national approach to chemical facility preparedness. Another problem is that sites are almost exclusively owned by the private sector. In addition, few mandates require owners/operators to institute safeguards, and incentives to do so are almost nonexistent. A final complicating factor is that the Department of Homeland Security (DHS) is the lead federal agency for the chemical sector, but they do not have the statutory authority to require implementation of preparedness measures. Obviously, this lack of enforcement power restricts what DHS can accomplish. Given these conditions, *how can the Department of Homeland Security ensure owners/operators of chemical facilities take the necessary actions to reduce the attractiveness of their sites as weapons of mass destruction?*

B. DEFINING THE PROBLEM

Government officials and industry observers agree the chemical sector constitutes a desirable target for terrorists. This point of consensus is based on several reasons. First, so many of the industry's facilities are extremely vulnerable to attack because of poor security. In fact, in a recent government report site security was described as ranging

from fair to very poor.¹ Some believe that even unsophisticated strikes on facilities have high probability of success. Second, hundreds of chemical sites are immediately adjacent to or located within highly populated areas. Because of this situation, a catastrophic chemical release or explosion at these facilities could kill thousands or tens of thousands of Americans. Third, a chemical plant attack could have devastating impacts on the U.S. economy because many other critical infrastructure sectors are extremely dependent on a functioning chemical industry for raw materials. Fourth, chemical facilities are often clustered together in industrial districts or near shipping ports. Therefore, an attack on one could set off a chain reaction of explosions at nearby plants and have a disastrous impact on trade. The final reason may involve symbolism. Terrorists may strike chemical sites (e.g., refineries) to send a symbolic message. Many believe that this rationale was the primary reason behind the thwarted White House/U.S. Capitol and successful Pentagon attacks.

Despite these risks, most chemical sites have not implemented adequate measures to prevent, mitigate, deter and/or respond to terrorist attacks. To make matters worse, nationwide mandates requiring all chemical facilities to assess their vulnerabilities to terrorism and to take steps to reduce them do not exist. Also, no government agency has comprehensively assessed the vulnerability of chemical facilities across the nation.² Although various levels of government and the chemical industry itself have initiated some security-related measures, they only apply to a limited number of chemical facilities. Most are still not adequately safeguarded. Glaring vulnerabilities continue to exist at sites, placing huge segments of the public in needless danger.

In an attempt to resolve this problem, several alternatives have been suggested. However, to date little substantive action has been taken to adequately reduce the attractiveness of chemical facilities as targets of terrorism. Therefore, the time has now come for the federal government to determine what steps to pursue to regulate the industry. But, how can the government effectively accomplish this goal without

¹ John Stephenson, "Federal Action Needed to Address Security Challenges at Chemical Facilities," *GAO Report to Congress* (Washington D.C.: General Accounting Office, February 23, 2004), 8.

² John Stephenson, "Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action Is Needed," *GAO Report to Congress* (Washington D.C.: General Accounting Office, April 27, 2005), 8.

significantly hindering the productivity, trade, or economic growth of an industry that officials are so dependent on for jobs, tax revenue, and moreover votes?

1. The Relevance of This Problem

Determining how U.S. officials should move forward will ultimately yield several practical benefits. The most obvious advantage is that chemical facilities will become better protected against acts of terrorism by deterring or preventing attacks. If an attack on a site is successful, however, its consequences could be mitigated if the research findings are implemented. For example, when working to resolve the research question, a review of disaster response and recovery efforts is likely. In all probability, this review will eventually identify areas that need improvement.

Conceptually speaking, resolving the research question may have applications that extend beyond the chemical sector. Findings could serve to form a template for how other critical infrastructure sectors, facilities, etc., facing the same or similar problems should proceed. In addition, efforts to resolve the research question could help to answer the larger theoretical question, who is in charge when it comes to critical infrastructure protection?³

2. Thesis

Nearly five years after the events of September 11, 2001, many of our nation's most dangerous chemical facilities remain inadequately prepared for acts of terrorism. Two primary reasons influence this situation. First, few requirements exist regarding how chemical facilities should be secured. For the most part, protection at many sites remains solely a corporate decision. Second, inefficiencies are present within the marketplace that fail to encourage the implementation of necessary safeguards. In other words, few incentives exist to motivate owners/operators of chemical facilities to sufficiently protect their sites. In order to remedy these problems, the following policy should be pursued:

- Enact federal legislation that provides DHS with statutory authority to ensure the attractiveness of chemical facilities as targets for terrorists is

³ Dr. Ted G. Lewis, *Critical Infrastructure Protection In Homeland Security: Defending A Networked Nation*, (Monterey, CA: Naval Postgraduate School, 2004), 73.

reduced to an acceptable level. To achieve this outcome, the new legislation must assert that DHS has to collaborate with the private and public sectors.

- Establish ongoing Regional Defense Units (RDUs) to aid DHS with accomplishing the new mandate.
- Utilize RDUs to craft, implement, and sustain regional chemical facility preparedness efforts.

3. Literature Review

As a whole, government officials are responsible for the vast majority of authoritative literature that exists relating to chemical facility preparedness. Other contributing sources include trade associations, industry experts, news agencies, think-tanks and environmental groups. Although all of these contributors have varying perspectives, there are some points of agreement among them. For example, most sources believe that catastrophic releases of toxic and/or flammable airborne agents from chemical facilities would cause many deaths. But the range of likely fatalities is of great debate. This lack of consensus represents a significant distraction to the discussion of how the federal government should proceed to reduce the attractiveness of chemical plants as targets for terrorists. Fueling the debate are disagreements about how to improve chemical facility protection. Even though this dispute is ongoing, there is widespread agreement among think-tanks like the Brookings Institute and intelligence sources from the Central Intelligence Agency and the Department of Justice that chemical sites are likely terrorist targets.

As proof of how deadly a chemical disaster can be, one only needs to review the history of such incidents. For example, in 1984, in Bhopal, India, a devastating accidental release of a toxic gas cloud from a Union Carbide plant killed almost 4,000 people and injured an estimated 150,000-600,000.⁴ Although this incident did not occur in the U.S., it served as the impetus for the passage of a series of new laws, including amendments to the Clean Air Act (CAA). Among other things, the new CAA changes require each facility with a designated minimum amount of certain toxic and/or flammable substances

⁴ Stephenson, "Federal and Industry Efforts Are Addressing Security Issues," 7.

to develop a Risk Management Plan (RMP). The RMP has to contain an off-site consequence analysis of an accidental release that entails a worst-case scenario. In it, the number of people considered “affected” by a worst-case release must be identified.

According to EPA data, 123 chemical facilities located throughout the nation have toxic “worst-case” scenarios where more than one million people could be at risk of exposure to a cloud of toxic gas.⁵ Also, about 600 sites could each potentially threaten between 100,000 and a million people, and about 2,300 plants could each potentially affect between 10,000 and 100,000 people within these facilities’ vulnerable zones (described below).⁶

Most government officials, think-tanks and media personnel use an RMP’s worst case scenario (i.e., the number of people affected) as THE standard for evaluating the lethality of a site. Some Department of Homeland Security documents and CRS Reports, however, suggest that this benchmark is not appropriate because it overstates the number of people that would actually be impacted. These proponents point out that the number of people considered affected in an RMP is calculated by drawing a circle around the plant. The radius (e.g., dispersion distance) of this circle is determined to be the distance a toxic vapor cloud, heat from a fire, or blast wave from an explosion could travel from the facility before dissipating to the point that serious injuries from short-term exposures would no longer occur.⁷ All those inside this circle or vulnerable zone are considered to be affected, which according to the EPA means anything from minor injuries to death. Industry proponents state that it is improper to assume that everyone in the vulnerable zone would be affected. This camp claims that in reality only those who are in the plume area (e.g., wedge shaped region within the vulnerable zone) would be impacted by a chemical release. Accordingly, since the plume area is much smaller than the vulnerable zone, the number of individuals actually affected would be considerably less than what is indicated in the RMP’s worst-case scenario.

⁵ John Stephenson, “Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown,” *GAO Report to Congress* (Washington D.C.: General Accounting Office, March 23, 2003), 4.

⁶ Ibid.

⁷ Stephenson, “Federal and Industry Efforts Are Addressing Security Issues,” 9.

On the other hand, many opponents such as environmental groups and some in government believe that RMPs' worst-case scenarios underestimate the number of people that could be affected. They claim this discrepancy occurs because of the EPA's loose definition of a worst-case scenario. It is defined as the maximum quantities of release from the rupture of the single largest vessel, or process line at a facility.⁸ Opponents feel that this definition is not inclusive enough. They demand that a worst-case scenario should encompass a catastrophic release of much more than the contents of only one vessel or process line. As demonstrated by the 9/11 attacks, terrorists are likely to strike multiple targets during a coordinated effort. Therefore, by only considering the loss of one vessel or process line, this camp claims an RMP's worst-case scenario is not really a worst-case scenario. They argue that in order to more accurately assess the number of those affected by a catastrophic chemical release or explosion, the rupture of all containers should be included.

Although there is some disagreement regarding the accuracy of RMPs' worst-case scenarios, there remains a general consensus that many chemical facilities pose a clear and present danger that terrorists might want to exploit. For example, a 2002 Brookings Institute report ranks attacks on toxic chemical plants behind only biological and atomic attacks in terms of possible fatalities.⁹ Most observers agree that terrorists face extreme difficulties when attempting to carry out biological or atomic attacks, but the same cannot be said for strikes on chemical facilities. As in the 9/11 attacks, terrorists could simply convert our productive assets into weapons of mass destruction. Furthermore, in 2002, the Director of the Central Intelligence Agency warned during testimony of the potential for an attack by al-Qaeda on chemical facilities.¹⁰ Even the Justice Department has concluded that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both "real and credible."¹¹

⁸ Stephenson, "Voluntary Initiatives Are Under Way at Chemical Facilities," 10.

⁹ Michael E. O'Hanlon, *Protecting the American Homeland: A Preliminary Analysis*, (Washington, D.C.: Brookings Institute Press, 2002), 7.

¹⁰ Stephenson, "Federal Action Needed," 6.

¹¹ Stephenson, "Voluntary Initiatives Are Under Way," 9.

The U.S. chemical industry booms as a \$450 billion annual business. It directly employs more than 1,000,000 workers and indirectly about 5,000,000.¹² The chemical sector supplies key outputs used to manufacture other crucial products (fuels, medicines, drinking water, etc.). The operation of many other critical infrastructure assets relies on the chemical industry remaining functional. This connection is so apparent that nearly all of the sources reviewed agree that a catastrophic attack on key chemical sites could have devastating ripple effects on other sectors. In all likelihood, many critical operations would grind to a halt, crippling the economy. A small glimpse of this interdependency was seen just after 9/11. Rail transportation of many hazardous materials including chlorine was disrupted in some states following the attacks, because of concerns about the potential for an intentional chemical release by terrorists.¹³ This temporary stoppage of rail service impacted drinking water facilities that relied on chlorine delivered by rail to purify water.¹⁴

A vast majority of experts in the chemical industry believe current security conditions at most chemical facilities are insufficient. But, how much more security should there be? Who should be responsible for providing additional security? What are the best ways to implement and sustain new preparedness measures? These are just a few of the central questions that many of the literature sources attempt to answer.

When trying to answer the question of how much more security is needed, standard protocol dictates conducting site vulnerability assessments. This process involves a comprehensive analysis of a facility, which includes a review of its procedures, plans, processes, threats and risks. Completing a vulnerability assessment will, among other things, identify security weaknesses. These deficiencies are then usually addressed to further safeguard the site. Although this process sounds straightforward, it is not. For example, an array of vulnerability assessment

¹² American Chemistry Council, *Protecting a Nation: Homeland Defense and the Business of Chemistry*, April 2002, http://www.americanchemistry.com/s_acc/sec_article.asp?CID=26&DID=1218 (Accessed July 22, 2005).

¹³ Jim Kouri, "Preventing Terrorist Attacks at Chemical Facilities," *Men's Daily News Home Page*, May 6, 2005, <http://mensnewsdaily.com/blog/kouri/2005/05/preventing-terrorist-attacks-at.html> (Accessed June 10, 2005).

¹⁴ Ibid.

methodologies is presently available, with more being developed every day. Depending on which methodology is used, varying outcomes are produced. Some have suggested that this situation could lead to a particular methodology being employed solely because it yields advantageous results for plant owners/operators, instead of the most accurate results. In order to overcome this problem, the Justice Department developed a single methodology that all facility managers can use. It is the DOJ's position that using one methodological tool will help remove bias and allow vulnerability assessment comparisons to be made across various chemical facility types (i.e., petroleum, chlorine, synthetic oils, etc.). But, facility managers and trade associations alike argue that a vulnerability assessment designed for a specific type of chemical plant would be optimal. They dismiss the "one size fits all" approach as it does not consider the key differences among various types of chemical facilities.

The bulk of the literature identifies the private sector as shouldering the majority of responsibility for providing additional preparedness measures at the nation's chemical facilities. This rationale seems entirely appropriate since the private sector owns the vast majority (85%) of critical infrastructure, which encompasses chemical facilities.¹⁵ Even the *National Strategy for Homeland Security* states that the private sector bears "primary and substantial responsibility for addressing the public risks posed by their industries..."¹⁶ There is, however, a call by industry for financial assistance from government to help cover some protection-related costs. Also, with regard to assigning responsibility to the private sector, consistent themes appear in the literature. Most government sources advocate that the public and private sectors should partner to develop the most cost-effective and comprehensive strategy to reduce the attractiveness of chemical facilities as targets of terrorism.

Several potential solutions to the issues described above emerge in the available literature. Those that merit evaluation fall into three broadly based categories. First, some observers believe that the chemical industry should be allowed to continue with its

¹⁵ National Commission on Terrorist Attacks, *The 9/11 Commission Report* (New York: Norton, 2004), 398.

¹⁶ *The National Strategy for Homeland Security* (Washington D.C.: Office of Homeland Security, February 2002), 33.

voluntary approach to the problem. The principal parties who subscribe to and advocate continuing this approach are plant officials, industry lobbyists and trade associations. Their position appears in industry newsletters, websites, journals and government reports (e.g., CSR, CBO, etc.). This group promotes the idea that market forces are sufficient to protect chemical facilities from terrorism without outside interference. As proof, they point to an array of voluntary efforts already instituted by the chemical industry to bolster plant security, especially since 9/11. In fact, according to the industry's largest trade association, the American Chemistry Council (ACC) its members have spent over \$2 billion safeguarding their sites following September 11, 2001.¹⁷ In addition, the ACC says more actions are forthcoming and that the trade association will continue to work with DHS to prevent chemical facilities and their products from being used to harm anyone.¹⁸

Second, there are those who believe that voluntary efforts and current requirements alone are not sufficient to adequately protect the nation's chemical facilities from terrorism.¹⁹ This group is largely comprised of environmental organizations, industry activists, emergency responders and some political leaders. They promote relying heavily on mandates to force plant officials to abide by a laundry list of tasks. Most of these tasks revolve around fortifying sites. The group's promotion of tighter restrictions is well recorded in various congressional testimony reports. These proponents state that this kind of regulation could mitigate lax security that continues at most chemical facilities, which they assert plant owners/operators refuse to properly address. Their claims appear to have some validity according to news reports, undercover investigations and cursory government inspection at several key facilities where security was found lacking.²⁰ This camp argues that without mandates, any added protective measures by the industry will likely not be effective. As a model for what stringent requirements can yield, supporters point to the high level of security at the nation's

¹⁷ American Chemical Industry, "ACC Supports Federal Chemical Security Legislation," October 2004, http://www.americanchemistry.com/s_acc/sec_policyissues.asp?CID=329&DID=1156 (Accessed July 9, 2005).

¹⁸ Ibid.

¹⁹ Stephenson, "Federal and Industry Efforts Are Addressing Security Issues," 14.

²⁰ Stephenson, "Voluntary Initiatives Are Under Way," 11.

nuclear and high-risk port facilities, which they consider as adequately “hardened.” They believe the same security can be achieved in the chemical industry. Their strategy primarily relies on mandates to force chemical facilities to improve protection of sites with “guns, guards and gates.”

A third group believes that neither course of action will effectively solve the problem. Instead, they argue for the need to create regional partnerships between the private and public sectors. It is recommended that these new “teams” work collaboratively with the Department of Homeland Security to reduce the attractiveness of chemical facilities as targets of terrorism. In short, key stakeholders should join together to define and craft an approach to ensure achievement of the desired outcome. Some industry experts and government officials promote this approach. They suggest that this cooperative solution will yield a more comprehensive and effective long-term result. Their claims have been made during several congressional hearings related to chemical facility protection. The *National Strategy for Homeland Security, National Infrastructure Preparedness Plan* (NIPP) and a series of CRS reports support this position. In addition, a joint approach is the foundation for the Department of Homeland Security’s Free and Secure Trade (FAST) program, Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT) program.²¹ All three establish private-public partnerships with the aid of incentives and mandates that improve shipping security and reduce inspection time.

The three courses of action described above emerge as the most likely alternatives to be implemented for several reasons. The first option (voluntary approach) enjoys strong industry-wide support since it is the current strategy and has been for decades. Policies, procedures and personnel are already in place to support this approach. It requires the least amount of change. The second option is viable because it has been successfully used in other areas to resolve similar problems. Furthermore, since 9/11, dominant themes in government espouse legislating remedies to homeland security issues. In fact, in every year since 2001, a national chemical facility security-related act

²¹ U.S. Department of Transportation, *U.S. International Trade and Freight Transportation Trends*, (Washington, D.C.: U.S. Government Printing Office, 2003). Appendix A, http://www.bts.gov/publications/us_international_trade_and_freight_transportation_trends/2003/html/appendix_a.html (Accessed June 16, 2006).

has been introduced. Margins of defeat for these bills are growing smaller with the passage of time. The third course of action is a practical solution for two reasons. First, it has key support from the Department for Homeland Security, and it is promoted in several government documents (CRS Reports, CBO papers, National Strategy for Homeland Security, NIPP, etc.). Also, creating partnerships among stakeholders sets the stage for effective cooperation, communication, innovation and collaboration that could produce “win-win” outcomes for both the private and public sectors. For these reasons, analyses of all three alternatives will be conducted to determine an effective course of action for policy.

4. Unexplored Areas

Although the literature is exhaustive in both breadth and depth, some unknown areas persist. For example, few sources address the topic of securing the transport of chemicals. It is as if hazardous chemicals magically and safely flow to and from facilities. Clearly this area deserves further investigation because if facilities do eventually become better prepared for attacks, a viable next alternative for terrorists is to target chemicals in transit. Thus efforts to protect chemical facilities may merely shift, or displace the terrorist threat to other vulnerable targets (transport vehicles, holding tanks, railroad cars, etc.) that move chemicals. That scenario happened a few years ago at Israel’s largest fueling station in Tel Aviv. Terrorists attached an explosive device to an unsecured tractor-trailer truck during the night while the driver was asleep.²² The perpetrators chose this tactic primarily because the facility had very tight security.²³ The next morning, as the truck entered the fortified site, the improvised explosive device (IED) was detonated.

Another area receiving little attention in the literature is that few sources exhaustively explore the likely effects of successful terrorist attacks on chemical facilities. Instead of conducting this kind of comprehensive and technical research, industry observers rely on two readily available sources to assess possible impacts. First, experts use the previously noted incident in Bhopal, India, for providing the standard model for understanding the actual consequences of a large-scale U.S. chemical release.

²² David Rudge, *Ben-Eliezer Warns of Bombing Wave*, Israelfacts.org, May 27, 2002, https://www.synapsenow.com/synapse/news/fullstory_public.cfm?articleid=4576&website=israelfacts.org (Accessed April 5, 2006).

²³ Ibid.

Some claim significant problems exist with the Bhopal model. For example, the plant where that incident occurred did not have the mitigating systems in place that facilities in the U.S. possess.²⁴ In addition, many of those killed in Bhopal lived in a shanty town immediately adjacent to the release site. Therefore, the outcome most likely encountered in America from a similar chemical release would be drastically different than what was experienced in India over 20 years ago. Second, many in the field use the RMPs' worst-case scenarios to determine probable consequences of chemical releases. As already mentioned, however, the underlying technical assumptions built into the worst-case scenarios contain several problems. As a result, the accuracy of their projections is highly suspect. It seems clear that more efforts should be directed at thoroughly calculating the realistic consequences of terrorist attacks on chemical facilities. Until risks are accurately known, priorities cannot be properly established. Therefore, it is critical that, to the extent possible, a program be developed to assess the likely consequences of terrorist attacks on chemical sites. If actions are taken before this step is complete, it may result in the proverbial mistake of "putting the cart before the horse."

Another topic that rarely appears in the literature has to do with managing the human element of security. Most research seems to assume attacks will emanate from outside rather than inside. But, "While fighting the enemy without, we must not forget the enemy within."²⁵ The few references to preventing "insider" attacks that do exist simply suggest conducting thorough pre-employment background investigations of key personnel, as well as periodic reviews. This process is primarily intended to screen out high-risk employees who may one day become saboteurs. Little consideration is given to preventing workers from unintentionally aiding attackers. It is generally assumed that these kinds of acts will not happen if appropriate security measures, procedures, technologies and systems are in place. Unfortunately, it does not matter how fortified the castle walls are if those who have the keys to the kingdom accidentally allow intruders inside.

²⁴ Richard Farmer, "Homeland Security and the Private Sector," *Congressional Budget Office*, (Washington D.C.: Congressional Budget Office, December 2004), 24.

²⁵ Gary Ackerman and Chery Loeb, "Watch Out For America's Own Extremists," *Christian Science Monitor Online*, October 19, 2001, <http://www.csmonitor.com/2001/1019/p11s3-coop.html> (Accessed May 29, 2006).

Regardless of whatever protective steps are implemented, people remain instrumental to their effectiveness. Ultimately rules and technologies alone do not execute policies—individuals do. This dependency creates a major vulnerability because the human factor is truly security’s weakest link.²⁶ This “chink in the armor” occurs for several reasons. First, people are susceptible to social engineering (e.g., being conned).²⁷ The public can misplace their trust if manipulated in certain ways.²⁸ Social engineering is all about manipulation. It involves using the art of deception, influence and persuasion to gain access to protected assets. Social engineers persuade people to do things they would not normally do for strangers.²⁹

Second, developers are continually improving security technologies. These improvements make exploiting technical vulnerabilities more difficult. As this happens, the human element will increasingly be targeted. They become the weak underbelly of security. In short, because of technological advances, the focus of attacks will more often than not be directed at people rather than trying to actually defeat physical safeguards for unauthorized access. Consequently, strengthening the human component becomes more critical. But how can this pursuit effectively be achieved?

According to limited research, education represents an organization’s best tool for controlling the human element of security.³⁰ As a general rule, everyone needs to be trained since all are vulnerable to social engineering attacks. Every worker should receive a base level of training, and then each must also be trained based on his/her specific job assignment to adhere to certain protocols.³¹ People who work in sensitive areas should be given additional specialized training.³²

²⁶ Kevin Mitnick, *The Art of Deception: Controlling the Human Element of Security*, (Indianapolis, Indiana: Wiley Publishing, 2002), 3.

²⁷ Ibid., VII.

²⁸ Ibid., 41.

²⁹ Ibid., XI.

³⁰ Ibid., 73.

³¹ Ibid.

³² Ibid.

As one noted security consultant said, “Security is not a product, it is a process.”³³ It involves policies, technologies, system configurations, and more importantly, people. The effectiveness of the entire process hinges on individuals. Since the human element is often the Achilles’ heel of security, special consideration needs to be paid to strengthening this weak link. For now, this goal is best achieved through education, but further research is needed.

5. Methodology

In an attempt to help determine the road ahead, a comparative methodology will be utilized. This approach will occur on two levels. The first level involves evaluating mandates used by local, state and federal officials to safeguard some chemical sites. Each has instituted laws or acts requiring certain preparedness actions to be implemented. This “stick” approach could also be used by the federal government and DHS to better prepare the nation’s chemical facilities for attack. However if this mechanism is selected, what should enacted mandates include? How specific and comprehensive should they be? To answer these questions, as well as others, a review of current local, state and federal government efforts is needed because they vary considerably. Some statutes remain more prescriptive and far-reaching than others. Comparing the advantages and disadvantages of the various mandates will provide valuable clues as to the direction and potential effectiveness of a new federal approach for safeguarding the country’s chemical facilities.

The second level involves conducting a review of incentive programs that could motivate the private sector to voluntarily reduce the attractiveness of their sites as targets of terrorism. The purpose of this evaluation is to identify what factors encourage facility operators to institute chemical facility preparedness measures. For example, local, state and federal officials use grants, tax incentives, early provision options, equivalency alternatives and outreach programs for plants, and other facilities, to motivate owners/operators to strengthen their security. In addition, the industry promotes improved facility preparedness through memberships in trade organizations. These same “carrots” could become part of an overarching national approach. However, given the capabilities, resources, and constraints of the private and private sectors, which and how much of each incentive approach would be most effective, if any? Resolving this question necessitates

³³ Mitnick, *Art of Deception*, 4.

an evaluation of current voluntary and self-imposed efforts. The benefits and drawbacks of each carrot need to be weighed in light of the desired outcome.

Furthermore, a brief review of how analogous problems were resolved is included. Their solutions could provide some insight as to the likely success or failure of potential courses of action of how to reduce the attractiveness of chemical facilities as terrorist targets. For example, according to the literature, water purification and nuclear power facilities recently overcame some of the same kinds of issues now facing the chemical industry. Lessons from these efforts may be applicable to chemical facilities.

Water purification sites typically store large amounts of chlorine. This chemical is used to prepare water for human consumption. Following 9/11, many observers found that nearly all purification plants are located in densely populated areas, and most have lax security. Since chlorine is an extremely toxic substance, many in Congress believe these sites should be better prepared for acts of terrorism. This concern led to the passage of the Public Health Security & Bioterrorism Preparedness & Response Act.

Early on, the nuclear power facilities were recognized as extremely dangerous. A catastrophic accident at one of these sites could threaten the lives of a large number of Americans. As a result, a governing board, the Nuclear Regulatory Commission (NRC), was established. Prescribing an elaborate set of physical protection guidelines that the industry has to follow is chief among the NRC's duties. Examining these guidelines and evaluating their effectiveness could yield clues to for how policymakers should reduce the problem of chemical facility "insecurity."

THIS PAGE INTENTIONALLY LEFT BLANK

II. EVOLUTION OF THE PROBLEM

A. CHEMICAL FACILITY HISTORY

Chemical refineries were first introduced into the U.S. in the early 1920s. Initially, most were built along waterways to expedite the transportation of raw materials and refined products. At that time, only sparsely populated areas surrounded the newly constructed facilities. Most people were unaware of the dangers posed by this emerging sector and of the vulnerabilities that existed. That perception would soon change.

1. Tragedy in Texas City, Texas

On April 16, 1947, a French ship, the SS Grandcamp, docked in an industrial port in Texas City, Texas.³⁴ The ship had 2,300 tons of ammonium nitrate fertilizer onboard when a fire ignited. The crew made futile attempts to extinguish the fire, but it ultimately reached the ship's volatile cargo causing a massive explosion. The force of the blast was so strong it brought down two nearby aircraft and created a fifteen-foot tidal wave that swept through the port carrying debris and corpses with it.³⁵ The explosion also triggered a series of cascading fires. As a result, several businesses were set ablaze including a nearby Monsanto chemical refinery. The company had 1.5 million barrels of petroleum products on-site that burned out of control for days. This fire created an enormous black cloud of soot which could be seen for miles around. When the dust settled 576 people were dead, including all 26 members of the local volunteer fire department, and 3,500 were injured.³⁶ Aggregate property loss amounted to almost \$600 million in 1947 terms, equal to about \$4 billion today.³⁷ After this incident, some cargo handling procedures were modified, but for the most part the chemical industry operated as unusual.

2. Federal Safety Efforts

In the U.S., significant changes did not occur within the chemical sector until 1970 when the federal government established the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA). The EPA sought

³⁴ Mark Pandanell, *The Texas City Disaster: April 16, 1947*, <http://www.local1259iaff.org/disaster.html> (Accessed May 30, 2005).

³⁵ Ibid., 2.

³⁶ Ibid., 5.

³⁷ Ibid.

to protect the environment from pollution. OSHA focuses on “assuring, as far as possible, every working man and woman in the United States safe and healthful working conditions, and preserving our human resources.”³⁸ Now, for the first time, there were regulations and minimum operating standards for chemical facilities to follow. On the downside, both federal agencies primarily target accidents, not intentional acts. Consequently, plant officials followed suit and focused on measures to make their facilities safer from accidents. Willful destructive actions were not given much attention. With everyone concentrating on accidents, it is not surprising that chemical facilities became safer places to work. In fact, every year since the establishment of the EPA and OSHA, the number of industrial workers killed on the job has steadily declined.³⁹ However, as ironic as it may seem, this improvement had a serious drawback. It gave the public the perception that chemical facilities were not dangerous. That belief would soon be called into question.

3. The Catastrophe in Bhopal, India

As mentioned earlier, in 1984 in Bhopal, India, a Union Carbide plant unintentionally released a toxic pesticide ingredient.⁴⁰ As a result, a large toxic gas cloud quickly formed and passed through the city, killing almost 4,000 people and injuring another 150,000–600,000.⁴¹ Besides being deadly, this incident also had substantial monetary costs. Union Carbide eventually paid out an estimated half a billion dollars in compensatory damages to more than 566,000 survivors and dependents, including thousands of permanently disabled victims.⁴² Although this chemical release did not happen in the U.S., it served as the impetus for a series of actions by both the private and public sectors. But, these steps again narrowly focused both parties’ efforts towards reducing accidental releases or explosions. Preparing facilities for intentional acts, such

³⁸ Lafayette Technical College, *OSHA and Other Safety Regulations*, http://www.lafayettecampus.net/lafayette/loss_prevention_manual/osha_and_safety_and_health.htm (Accessed June 19, 2005).

³⁹ Thomas Kniesner, *Cato Handbook for the 105th Congress*, (Washington, D.C.: The Cato Publishing Institute, 1996), <http://cato.org/pubs/handbook/hb105-36.html> (Accessed June 13, 2005).

⁴⁰ Farmer, “Homeland Security and the Private Sector,” 24.

⁴¹ Ibid.

⁴² Ibid.

as terrorism or sabotage, did not receive consideration. Preventing purposeful attacks would not attract significant attention until the tragic events of 9/11.

4.. Private and Public Sector Responses to the Release in Bhopal

Following the disaster in India, the private sector became involved in improving safeguards at chemical facilities. In particular, the country's largest chemical industry trade association, the American Chemistry Council, developed and implemented the Responsible Care Code program. Basically, its tenets call for participating chemical facilities to abide by a series of guidelines and a code of conduct. Some of the more salient points of the Responsible Care Code program require member facilities to assess and address their vulnerabilities. Afterwards, third party verifications of implemented security measures must occur. While these measures are steps in the right direction, most experts agree that the program does not go far enough. Leading this charge is slew of government officials, most notable of whom is the Governor Jon Corzine of New Jersey. More importantly, the Administrator of EPA and the Secretary of DHS have gone on the record as saying that voluntary efforts alone are insufficient to assure the public of industry's preparedness.⁴³ Organizations including the Environmental Health Watch group, Natural Resource Defense Council and the Agency for Toxic Substances and Disease Registry support this position. Several government documents (GAO-05-631T, GAO-03-439, CBO Paper 12/04 and GAO-04-482T) and news reports have also raised serious concerns about the effectiveness of the Responsible Care Code program. This camp believes the program still falls short of the action needed to adequately reduce the attractiveness of chemical facilities as targets of terrorism. As proof, experts point to the fact that membership in the program is strictly voluntary, and most chemical facilities simply do not join. In fact, only approximately 7% of the nation's 15,000 RMP facilities have adopted the Responsible Care Code program.⁴⁴ In spite of the lack of participation, the industry and its trade associations still promote the program as THE model for how the sector can police itself. The Responsible Care Code is hailed by its proponents as the best alternative to legislative mandates, which they say will only create more bureaucratic red-tape without actually making plants, or the country, any safer. Opponents to the

⁴³ Stephenson, "Voluntary Initiatives Are Under Way," 23.

⁴⁴ Ibid., 5.

program believe that its establishment allows industry groups to deflect calls for more stringent regulation of chemical facilities. This stalemate remained relatively unchanged until September 11, 2001.

5. Current Situation

After the 9/11 attacks and the creation of the Department of Homeland Security, federal officials conducted cursory reviews of the chemical industry and subsequently found and reported an array of problems. First and foremost, glaring vulnerabilities were discovered at many chemical facilities that could easily be exploited by terrorists. Many of the inadequately protected sites store some of the nation's most lethal substances that, if released, would endanger the lives of millions of Americans. Second, relatively no mandates exist requiring chemical facilities to assess and address their vulnerabilities to attacks. Instead, security and protection of most plants are solely determined by their personnel with little or no third-party oversight. Compounding this issue, DHS is the lead federal agency for the chemical sector, but the department does not have commensurate statutory authority. In other words, DHS is unable to require facility owners/operators to take any actions. Last, no federal agency comprehensively assessed the vulnerabilities at the nation's chemical facilities against terrorism. Therefore, the extent of preparedness at sites is largely unknown. As described above, years of agencies focusing on accidental, rather than man-made disasters, likely fueled this problem.

Despite these well-documented deficiencies, substantial corrective action has yet to be undertaken. Even though government reports, congressional testimony and federal officials consistently state chemical facilities need to adequately assess and address their vulnerabilities to terrorism, most have not. As a result, large numbers of Americans are needlessly put in danger, and the federal government does not comprehensively know the size of the problem. Based on these shortcomings, it seems apparent a more effective approach needs to be developed, implemented and sustained to reduce the attractiveness of chemical facilities as targets for terrorists. However, what are the best ways to achieve this outcome? How should a new policy be structured? Who are the major stakeholders and what are their concerns? What trade-offs are created by a new policy? These are just a few of the key questions likely to be generated while evaluating alternative policies and are therefore discussed herein.

6. Lessons Learned from Disasters

Two primary lessons can be derived from the Bhopal and Texas City catastrophes. First, chemical facility disasters can be extremely lethal and financially costly. A major chemical release or explosion may injure or kill thousands, and economic losses could run into the billions. Recognizing the severity of these costs is important because history has demonstrated both are goals of terrorists. Accordingly, those sites that, if attacked, will likely produce both outcomes are attractive targets for terrorists. Understanding this relationship should encourage actions on the part of responsible parties to better prepare key chemical facilities for attacks.

Second, the two tragedies mentioned were the result of unintentional actions. This distinction is important to note because oftentimes accidents are much less disastrous than malicious acts. To illustrate, neither catastrophe involved a worst-case chemical release or explosion. In Texas City, the SS Grandcamp's volatile cargo had been partially unloaded and another burning ship was towed out of the port before either exploded. In the Union Carbide incident not all of the plant's deadly chemical vapors escaped. Only approximately 41 tons was released, roughly the half the amount that just one typical railcar tank holds.⁴⁵ However, a thinking adversary can choose to strike a facility based on time, place, weather, type and amount of substance stored on site and its economic impact. All of these factors could easily magnify the consequences of a successful attack.

It seems reasonable to assume that if terrorists were to strike a chemical facility, they would attempt to cause the greatest possible damage by releasing or igniting most, if not all, of the deadliest substances on site. In addition, a facility that is in close proximity to a densely populated area and one that would have a major affect on the economy would be chosen. Therefore, it can reasonably be inferred that a man-made disaster at a chemical plant will be much more costly than any accidental catastrophe of the past. This understanding should encourage stakeholders to undertake significant and concerted efforts to protect against future attacks at chemical facilities. It will not be easy to prevent a determined and "smart" adversary. Terrorists can circumvent, overpower and disable protective measures. They can also use ruses, find weaknesses, or conduct insider-

⁴⁵ J. P. Gupta, "The Bhopal Gas Tragedy: Could It Have Happened In A Developed Country?," *Journal of Loss Prevention in the Process Industries* (January 2002), 2.

operations to infiltrate sites. Accordingly, it will take a comprehensive and collaborative approach to resolve the complex issue of chemical facility preparedness.

III. PUBLIC-PRIVATE PARTNERSHIPS

A. INTRODUCTION

Imagine for a moment that thousands of bombs are lying on the ground within the United States. Some are clustered together while others are sparsely located. A few bombs are adequately protected from terrorists, but the vast majority is not. To make matters worse, many of the most lethal bombs are positioned near densely populated areas. If just one explodes, tens of thousands of Americans would likely be injured or killed. A blast of this magnitude could also have disastrous economic impacts.

This story may sound unbelievable, but many use it to describe the current condition of the U.S. chemical industry. They claim that one only needs to replace the words “chemical facilities” for “bombs” in the scenario above to get a clear understanding of the extreme risks now facing many Americans. Given these conditions, what can the lead federal agency tasked with chemical sector security, DHS, do to remedy this nationwide problem?⁴⁶

B. CONDITIONS SUPPORTING PARTNERSHIPS

It has been almost five years since 9/11, and many of the nation’s most critical infrastructure vulnerabilities have received some attention. However, according to government documents, news reports and other sources, little has been done to reduce the attractiveness of chemical facilities as targets of terrorism. Compounding this problem is that over 66,000 chemical facilities are spread across the country.⁴⁷ Within this universe the EPA has identified 15,000 as posing extreme dangers to the public. Furthermore, according to chemical facilities’ own records, 123 chemical sites are located throughout the nation that have toxic “worst-case” scenarios where more than one million people could be at risk of exposure to a cloud of toxic gas.⁴⁸ About 600 facilities could each

⁴⁶ *National Strategy For Homeland Security*, 32.

⁴⁷ U.S Department of Homeland Security, *The National Strategy For The Physical Protection of Critical Infrastructures and Key Assets* (Washington D.C.: Government Printing Office, February 2003), 9.

⁴⁸ Stephenson, “Federal Action is Needed,” 7.

potentially threaten between 100,000 and a million people, and another 2,300 sites could each potentially affect between 10,000 and 100,000 people.⁴⁹

Despite these risks, an effective national approach to chemical facility preparedness does not exist. The limited progress that has been made involves a patchwork of uncoordinated efforts. Additionally, chemical plants are almost exclusively owned and managed by the private sector. As a result, government has little control over their operations. Moreover, few mandates require chemical facilities to institute safeguards, and incentives to do so are almost nonexistent. A final complicating factor is that the Department of Homeland Security is the lead federal agency for chemical sector security, but it does not have the statutory authority to require most sites to implement measures to prevent, deter, protect against, mitigate from, and/or respond to terrorist attacks. Clearly, this lack of power limits what DHS can accomplish. Given these conditions, the Department of Homeland Security should consider the following proposals.

C. PARTNERSHIP ALTERNATIVES

In order to increase the readiness level of the country's chemical facilities for terrorist attacks, DHS needs to "reject past dogmas, to think anew and to act anew."⁵⁰ The problem of chemical facility preparedness is too large for the Department of Homeland Security to solve alone. In addition, it involves complex interdependencies that necessitate input from various key stakeholders. To overcome these issues, a collective public-private approach is needed, but what is the best way to bring both sectors together? There are at least three alternative courses of action for consideration.

As discussed earlier, DHS currently pursues voluntary avenues for forming public-private partnerships to improve chemical facility preparedness. In this approach DHS relies on a handful of incentives ("carrots") to encourage all levels of government, as well as facility owners/operators to participate in joint readiness efforts. Carrots primarily consist of limited DHS-led outreach programs and site visits. In addition, some

⁴⁹ Stephenson, "Federal Action is Needed," 7.

⁵⁰ U.S. Department of Homeland Security, *Remarks by Secretary Michael Chertoff U.S. Department of Homeland Security at the Commonwealth Club*, July 28, 2005, <http://www.dhs.gov/dhspublic/display?content=4700> (Accessed April 10, 2006).

grants and tax credits are offered. This voluntary approach has been used for several years. According to most industry experts, it has not been adequately successful.

In lieu of this situation, two other alternative courses of action are suggested. One alternative forces the establishment of partnerships through the use of laws (“sticks”). In all likelihood this tactic would entail the passage of federal mandates giving DHS the power to require the public sector and private industry to work together to better prepare facilities for attack. This approach was used to establish Local Emergency Planning Committees (LEPCs) to focus on emergency planning in communities near chemical plants. It is also a component of the proposed Chemical Security Act, discussed later. In short, this approach will force government and business to combine efforts to reduce the attractiveness of chemical facilities as targets of terrorism.

A second alternative uses a more balanced approach. It involves DHS employing a mixture of both carrots and sticks. DHS will also need to utilize a new type of leadership style. To initiate this alternative, legislation is first needed to provide DHS with the requisite authority to ensure that chemical facility operators/owners take adequate measures to reduce their sites’ attractiveness to attack. In addition, the enacted legislation will assert that DHS should join with key partners from government and business to work together to achieve the new mandate. DHS will rely on its new leadership position to establish collaborative regional public-private partnerships. In them, stakeholders will be granted significant roles and responsibilities. Ultimately, participants will determine the who, what, when, where and how of improving the regions’ level of preparedness at nearby chemical facilities for acts of terrorism. In essence, this option will establish a community-governance partnership of readiness efforts

D. INPUTS, OUTPUTS, & OUTCOMES

Listed below are the inputs (resources), outputs, and desired outcomes for the two described alternatives, including how each would be measured according to this author. Reviewing this information will help partially determine which alternative course of action should be adopted.

MANDATED (“STICK”) APPROACH

<u>INPUTS</u>	<u>ACTIVITIES</u>	<u>OUTPUTS</u>	<u>OUTCOMES</u>
<i>Resources</i>	<i>Services</i>	<i>Products</i>	<i>Intermediate</i>
Facilities	Training	Classes taught	New knowledge/abilities
Staff	Education	Audits performed	Increased skills
Volunteers	Compliance	Inspections conducted	Fewer enforcement actions
Funds	Reporting	Reports submitted	Reduced violations
Equipment	Rule-making	Requirements issued	Increased security measures
Computers	V.A.s conducted		<i>End</i>
Software	Participants trained		Vulnerabilities reduced
Supplies			Increased facility preparedness

MIXED (“CARROT & STICK”) APPROACH

<u>INPUTS</u>	<u>ACTIVITIES</u>	<u>OUTPUTS</u>	<u>OUTCOMES</u>
<i>Resources</i>	<i>Services</i>	<i>Products</i>	<i>Intermediate</i>
Facilities	Training	Classes taught	New knowledge/skills/abilities
Staff	Education	Sites visited	Increased skills/communications
Volunteers	Outreach	Meetings held	Changed attitudes/values
Funds	Mediation	Materials distributed	Increased network awareness
Equipment	Facilitation	Service hours	Increased # of participants
Computers	Help calls		<i>End</i>
Software			Modified behavior
Supplies			Increased facility preparedness

Improved network preparedness

Enhanced relationships

Increased productivity

Reduced costs and less oversight

Increased support/involvement

Measuring the performance of the Mandated Approach would primarily involve metrics associated with compliance and are generally quantitatively-based. For example, the number, ease, and magnitude of security breaches in a given year compared to the previous year. These breaches could be actual lapses or failures that occurred during tests (simulations, reviews, role-plays, etc.). Also, third-party audits of preparedness results could be conducted with grades being assigned to the different categories such as prevention, protection, mitigation, and response. Scores can be compared from year to year to track progress. Furthermore, the number of vulnerabilities addressed per period can be used as another measure. Finally, pre/post-effort questionnaires can be administered to detect changes in KSAs (e.g., knowledge, skills and abilities).

In addition to the measures described above, determining the performance of the Mixed Approach requires a more comprehensive and qualitative evaluation. For example, various survey instruments will be distributed to stakeholders eliciting their input regarding the achievement of certain outcomes (behavior changes, perception of relationships, opinion regarding facility and network preparedness, etc.). Proxies will also be analyzed to measure results in nebulous areas. For more definitive outcomes, performance indicators can be calculated and reviewed. Continuous benchmarking against best practices will be a necessity.

E. SWOT ANALYSIS & STRATEGIC ISSUE DEVELOPMENT

In order to identify strategic issues for DHS, a Strength, Weakness, Opportunity and Threat (SWOT) analysis is necessary. Conducting this kind of an evaluation helps an organization make sense of its internal and external environment.⁵¹ A better understanding of one's context sets the stage for effective strategy development since the inside can now be productively linked with the outside.⁵² In general, a SWOT analysis helps to paint a picture of the organization as a whole, not a collection of parts, in relation to its internal and external environment.

Based on an assessment of DHS's internal and external environment, the below listed strengths, weaknesses, opportunities and threats/challenges were identified:

⁵¹ John M. Bryson, *STRATEGIC PLANNING for Public and Nonprofit Organizations*. (San Francisco, CA: Jossey-Bass, 2002), 123.

⁵² Ibid.

STRENGTHS

- Comprehensive understanding of network interdependencies
- Strong industry reputation
- Expertise in assessing and mitigating vulnerabilities
- Nationally disbursed staff
- Partnering and collaborating ability
- Unique modeling tools
- Holistic view of homeland security
- Significant resources
- Access to threat information

WEAKNESSES

- Turnover of personnel
- Repeated departmental restructuring
- Lack of statutory authority
- Need to rely on voluntary efforts
- Lack of consensus regarding problem identification
- Nebulous metrics
- Rapidly changing assessment methodologies
- Information assurance issues
- Legacy cultures

OPPORTUNITIES

- Collaboration and partnerships
- Strong public desire to secure nation's critical infrastructure
- Political acceptability for action (Political acceptance of action?)

- Increase effectiveness and efficiency through integrated approach
- Need for local and state government involvement
- Desire for private-public support
- Teach (train and educate) stakeholders
- Build stronger communities
- Need to develop self-sufficient stakeholder operated programs
- Become leaders in homeland security efforts

THREATS/CHALLENGES

- Decreased agency political and public support
- Loss of legitimacy
- Overstretching of resources
- Political support/focus shifts to new priorities
- More need than resources
- Loss of industry lobby support
- Outperformed by private sector
- Downturn in economy
- Lack of understanding of what DHS does
- Loss of quality personnel
- Shrinking budget

After completing a SWOT analysis, the next step in the strategic planning process is to focus attention on organizational mandates, mission and values. Accordingly, DHS's mission statement reads, "We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation. We will ensure safe and secure borders, welcome lawful

immigrants and visitors, and promote the free-flow of commerce.”⁵³ In addition, DHS has three core values. Of particular interest is *Respect: Honoring our Partners* which states, “We will value highly the relationships we build with our customers, partners and stakeholders.”⁵⁴ Equally important when developing strategic issues, DHS must consider its product and service level, product mix, clients, users and payers, cost, financing, structure, processes and management. Having weighed these factors, DHS seems to be facing three critical challenges. Each can build upon or take advantage of DHS’s strengths and opportunities while minimizing or overcoming its weaknesses and threats identified in the SWOT analysis. Below is a summary of the selected policy challenges, framed as questions, as well as a brief description of what made them strategic issues.

1. What can DHS do to Improve Chemical Facility Preparedness Nationwide?

As already discussed, many believe chemical facility preparedness for acts of terrorism is currently inadequate. An attack resulting in a catastrophic release could prove deadly for a large number of Americans and have severe economic impacts. Complicating matters is the fact that over 66,000 chemical facilities are spread throughout the U.S. and nearly all of them are privately owned. Resolving these enormous issues without bankrupting the industry that DHS is trying to protect will be no small feat.

2. How does DHS Define a “Unified National Effort”?

This phrase appears in DHS’s mission statement and it is implicitly referred to in the department’s core values. Also, the *National Strategy for Homeland Security* promotes the formation of public-private partnerships for critical infrastructure protection.⁵⁵ In addition, the *National Infrastructure Protection Plan* echoes the same sentiment.⁵⁶ However, in spite of the lip service paid to this collaborative concept, it has

⁵³ U.S. Department of Homeland Security, *DHS Organization*, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0413.xml (Accessed June 14, 2006).

⁵⁴ U.S. Department of Homeland Security, *The 5 DHS Core Values: Guiding Our Work Life*, <http://www.dhs.state.or.us/training/corevalues.pdf> (Accessed June 14, 2006).

⁵⁵ *National Strategy For Homeland Security*, 64.

⁵⁶ U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington D.C.: Government Printing Office, June 2006), 32.

not yet come to fruition in the chemical sector. In its absence, some cities, counties and states have taken it upon themselves to implement security measures, but a majority has stood idle on the sidelines. Consequently, a patchwork of efforts to protect chemical facilities has evolved creating gaps in some areas and “stovepipes” in others. Many say that this kind of disjointed approach is what made America vulnerable to the attacks of September 11, 2001.

3. How can DHS Engage Public-Private Partners in Preparedness Efforts?

As stated above, DHS is the nation’s lead federal agency for the chemical sector. The department is specifically tasked with integrating and coordinating federal, state, local and private sector critical infrastructure protection efforts. However, DHS was never given the requisite authority to carryout its mandate. For example, DHS must generally obtain owners’/operators’ permission to enter into their chemical facilities. Without consent, DHS officials are unable to gain access. In addition, most sites are not required to cooperate with DHS nor comply with its recommendations or requests. While some facility managers have heeded DHS’s advice and implemented adequate preparedness measures, many have not. As long as this condition exists, a large number of American lives will be at risk. Next, properly preparing the chemical industry for acts of terrorism is a massive undertaking. Securing the thousands of lethal facilities scattered across the country dwarfs DHS’s capabilities. The fact that portions of the chemical industry are highly networked complicates matters. Because of this situation, it is unlikely that DHS alone can resolve the problem without causing unintended consequences elsewhere. Accordingly, a collective public-private effort is needed, but what is the best approach that can be used to bring these partners together?

F. PROPOSED STRATEGIC IDEA

Based on the analyses above, it is proposed that DHS lead a movement to forge new regional public-private sector partnerships. To bring governments (local, state and federal) and businesses together to ensure chemical facility preparedness, DHS can use a proper mixture of regionally developed, implemented and sustained mandates and incentives. This kind of collaborative arrangement is more likely to produce seamless, flexible and effective solutions while promoting creativity, innovation and imagination.

In addition, a well-managed partnership and division of labor may create a synergy and a co-producer relationship yielding results which neither sector could achieve alone.

Conducted properly, regional public-private partnerships can better prepare chemical facilities for acts of terrorism, thereby protecting Americans and improving their quality of life. Similar joint efforts have already proven their effectiveness by solving analogous homeland security problems while simultaneously benefiting businesses. These kinds of “dual-purpose” benefits are more likely to be produced when the two sectors truly work together to create win-win solutions (e.g., increased security and improved productivity). For example, in 2002, the Customs Trade Partnership Against Terrorism (C-TPAT) initiative was launched with just seven participating companies.⁵⁷ C-TPAT is a cargo partnership where member companies agree to implement robust screening and security protections to assure that goods and services are not a threat. In exchange, DHS offers expedited processing, streamlined movement of products, and a more productive result at the end of the day. So many companies have seen the tangible benefits of C-TPAT, both from a security and business standpoint, that as of 2005 its membership stood at more than 9,000.⁵⁸

Although DHS will lead and facilitate regional public-private efforts, the partnerships will intentionally lack a traditional “pyramid” structure. This step is bypassed to help create an environment where partners think and behave differently. Instead, a disintermediated (e.g., networked) command hierarchy will be put into place. In this design, “decision-makers are embedded within a network structure that encourages point-to-point movement of data, discussions and decisions.”⁵⁹ As a result, flexibility, speed and decision-making capability are increased.⁶⁰ However, a disintermediated structure requires new kinds of leadership to be exercised. In the absence of a “command and control” design, DHS will need to build a vision, a hope for the future that can attract legitimacy, credibility, commitment and results. For those who still refuse to participate,

⁵⁷ Brian J. Wilkins, *C-TPAT on a Roll*, December 2005, http://www.cargosecurity.com/ncsc_dotnet/press/C-TPAT_SpecialPressRelease.pdf (Accessed June 17, 2006), 1.

⁵⁸ Ibid.

⁵⁹ Dr. Ted G. Lewis, *Critical Infrastructure Protection*, 19.

⁶⁰ Ibid.

DHS can rely on a more conventional approach of incentives (carrots) and/or mandates (sticks). However, the later action should only be used as a tool of last resort.

Another advantage is that establishing cooperative relationships aligns with DHS's current strategy to "coordinate and integrate federal, state, local and private sector efforts to protect critical infrastructure," such as the chemical industry.⁶¹ The partnerships' new mission will be to reduce the attractiveness of chemical facilities as targets of terrorism while at the same time complement their (private businesses') operations. Both outcomes can be achieved by jointly working towards strengthening chemical facilities' ability to prevent, deter, protect against, mitigate from and respond to terrorist attacks. All of these pursuits are also strategic goals of DHS.⁶²

To initiate this proposal, the Department of Homeland Security should lobby Congress for the requisite authority to collaborate with stakeholders so as to ensure that chemical facilities reduce their attractiveness as targets of terrorism. Accomplishing this task requires DHS to use its expertise, resources, political clout and credibility. The time for this move could not be better. The Homeland Security and Governmental Affairs Committee just completed a series of hearings entitled *Chemical Facility Security: What Is The Appropriate Federal Role* without taking any action.⁶³ Once the necessary legislation is passed, DHS can move on to the next step of identifying the nation's high-value sites. This task is easily and quickly accomplished by using current Risk Management Plan data that the Environmental Protection Agency (EPA) already possesses. Afterwards, critical chemical facilities' vulnerable zones can be clustered together, based on proximity, to form regions. Next, DHS will identify and invite key stakeholders from both the private and public sectors in every identified region to form a Regional Defense Unit (RDU). In other words, each region will have its own RDU. Once in place, participating members will determine, implement, and oversee specific measures to reduce the attractiveness of key chemical facilities as targets of terrorism. In

⁶¹ *National Strategy For Homeland Security*, 32.

⁶² U.S. Department of Homeland Security, *DHS Organization*, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0413.xml (Accessed April 20, 2006)

⁶³ Susan M. Collins, *Chemical Facility Security: What Is the Appropriate Federal Role?*, Testimony before the Committee on Homeland Security and Government Affairs, July 27, 2005, <http://hsgac.senate.gov/files/072705SMCOOpen.pdf> (Accessed June 17, 2006), 1.

short, stakeholders will be deeply engaged in self-governance of preparedness efforts. To keep the entire process transparent and to improve accountability, RDU members will provide periodic reports and testimony to local, state and federal governing boards/committees reducing the likelihood that RDUs become co-opted.

G. BENCHMARKING

A major reason behind the strategic goal of forming regional public-private partnerships is to improve the preparedness of chemical facilities against acts of terrorism and thereby strengthen homeland security for the entire nation. Accordingly, it seems appropriate to benchmark the preparedness levels of public-private partnerships to assess if the goal is being achieved. But how can this goal effectively be accomplished?

Measuring preparedness often proves to be a difficult task. The process can be nebulous, tending to be more of an art than a science. To help ease and improve this effort, various organizations have already produced widely accepted standards that can be used to benchmark partnerships' progress towards preparedness. One such example is NFPA 1600 *Standard on Disaster/Emergency Management and Business Continuity Programs*. NFPA stands for National Fire Protection Association, which is an international nonprofit codes and standards organization. NFPA's title can be a bit misleading. It is made up of over 60,000 members from all over the world, and less than a quarter are affiliated with fire departments.⁶⁴ The majority of members are representatives from the private and public sectors, and they come from various disciplines.

The NFPA 1600 standard is considered by many to be an excellent benchmark for continuity and emergency planners in both public and private sectors.⁶⁵ The standard addresses methodologies for defining and identifying risks and vulnerabilities and provides planning guidelines. NFPA 1600 truly takes a total program approach. It has been adopted as an organizational preparedness standard by FEMA and the American National Standards Institute (ANSI). Moreover, the 9/11 Commission recommended in its final report that NFPA 1600 be recognized as THE national preparedness standard.⁶⁶

⁶⁴ Steven Davis, *NFPA 1600*, <http://www.davislogic.com/NFPA1600.htm> (Accessed April 30, 2006).

⁶⁵ *Ibid.*

⁶⁶ *The 9/11 Commission Report*, 398.

NFPA 1600 lists and defines 13 key preparedness components: (1) laws and authorities, (2) hazard identification, risk assessment, and impact analysis, (3) hazard mitigation, (4) resource management, (5) mutual aid, (6) planning, (7) direction/control/coordination, (8) communications and warning, (9) operations and procedures, (10) logistics, facilities and training, (11) exercises, evaluations, and corrective actions, (12) crisis communications and public information, (13) finance and administration.⁶⁷ These preparedness components apply to both the public and private sectors. Accordingly, each of these 13 components can be used to evaluate the progress of readiness efforts for the proposed regional public-private partnerships. For example, “hazard mitigation” (#3) involves the reduction of *Risk* which is a function of *Vulnerabilities X Consequences*. Lowering either of these two factors results in decreased risk and improved readiness.

Using the above relationship (e.g., $Risk = Vulnerabilities \times Consequences$) as a guide, Step 1 in a proposed evaluation process is to select and direct a composite team of stakeholders (e.g. first responders, facility personnel, DHS, etc.) to identify the total number of chemical facilities within a region. Sites are then grouped (low, medium, and high) and ranked (highest to lowest) based on their likely consequences (lethality, economic, symbolic, etc.). Tracking this data will provide the baseline information needed for subsequent metrics and actions. In Step 2, the team will conduct vulnerability assessments (VAs) for all sites in order of their priority (group and rank). A VA identifies weaknesses in a facility’s operation that can be exploited to allow a disaster to occur. The percentage of facilities that have completed these analyses will be tracked (Step 2 divided by Step 1). This information will help determine the process of identifying where the most need exists for preparedness programs. Once Step 2 is completed, a new grouping and ranking will be performed based on risk, since consequences and vulnerabilities are now known. In addition, the total number of vulnerabilities for all sites will be summed up. Step 3 involves the team focusing on reducing identified vulnerabilities. As this is being accomplished, progress will be tracked by dividing the number of vulnerabilities addressed by the total derived in Step 2. In Step 4, the team will turn its attention to

⁶⁷ Gunnar Kuepper, *The NFPA 1600 Standard on Emergency/Disaster Management: New Edition Expected in 2004*, IAEM Bulletin, July 2003, http://www.emergency-management.net/pdf/iaem/IAEM_July_Bulletin.pdf (Accessed June 15, 2006).

lowering the potential consequences initially determined in Step 1. This improvement could be accomplished in a variety of ways (implementing warning systems, mitigation equipment, training, etc.). While this action is being taken, hazard mitigation progress can be tracked by comparing initial consequences identified in Step 1 to reduced consequences yielded in Step 4. In Step 5, the team will regroup and re-rank chemical facilities that have been the subject of the hazard mitigation efforts. This process is necessary because facilities' vulnerabilities and/or potential consequences have been decreased. Reduction progress can be gauged by calculating the percentage of facilities that were "downgraded" (e.g. moved from a higher to a lower risk group). Another way to evaluate partnership efforts is to divide a facility's mitigated risk by its initial risk.

These examples are but a few of the performance indicators that can be used to benchmark hazard mitigation efforts. The same could be accomplished for the other 12 preparedness components of NFPA 1600. Most of the raw data for performance indicator calculations will come from various works conducted by stakeholder teams. However, separate accountability committees from within the public-private partnerships will actually perform the calculations and track the teams' progress. These committees will need to instill transparency and credibility in their benchmarking processes. They can achieve this goal by making their efforts publicly available, providing findings in open hearings/meetings and having third-party audits of results.

H. IMPLEMENTATION

The proposed strategic idea of forming regional public-private partnerships to focus on chemical facility protection represents a significant departure from the status quo. As discussed earlier, plant owners/operators alone currently determine what safeguards their sites enact. Selection is usually based on a facility's individual situation and need. Clearly, the strategic idea radically changes this narrow view of preparedness and isolated decision-making process. If adopted, command and control of preparedness related issues at chemical facilities will now be more participatory, involve additional stakeholders and take on a region-wide perspective.

When entities, both public and private, attempt to translate change of this magnitude into action they often encounter four key organizational hurdles:

- Cognitive – waking employees (partners) up to the need for a strategic shift;
- Resources – convincing employees (partners) that major change does not require additional resources;
- Motivation – encouraging employees (partners) to voluntarily embrace and execute the strategic shift; and
- Political – tackling opposition from powerful vested interests.⁶⁸

These obstacles represent significant challenges for DHS. Overcoming them will be critical. This situation is made even more difficult by the presence of two common constraints. There is usually great pressure to effectuate the strategic shift quickly and at low costs. Therefore, given both of these conditions and faced with the four organizational hurdles, how can DHS effectively implement regional public-private partnerships?

A potential solution to the challenges described above is for DHS to use *tipping point leadership*. This leadership approach rests on the premise that all organizations have people, acts and activities that exercise disproportionate influence on performance.⁶⁹ As a result, change-agents should direct their efforts at transforming these “extremes.” If done properly, a tipping point eventually will be reached where widespread toppling of the four key organizational hurdles happens at an accelerating pace until the masses are changed. As this process occurs, the strategic idea moves from thought to action and ultimately to institutionalization. Accordingly, the key to expedient and inexpensive strategic implementation is to identify and leverage disproportionate influence forces.⁷⁰ Herein lies the challenge for the Department of Homeland Security. In other words, what are the extremes (people, acts and activities) and how can they be used to overcome the four key organizational hurdles?

⁶⁸ W Chan & Renee Mauborgne, *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant*, (1st Edition 2005: Harvard Business School Press), 150.

⁶⁹ Ibid., 151.

⁷⁰ Ibid., 152.

To answer this question, it may be helpful for DHS to first understand how each obstacle will likely impact the implementation of regional public-private partnerships. Some barriers may have more or less influence on the adoption of the strategic idea than others and therefore require extra or little attention. In addition, some may be closer or further from their tipping points and as a result need little or extra effort from DHS.

Invariably, initiating major changes will encounter political roadblocks. Generally, overcoming them is difficult. Fortunately for DHS, the political winds seem to be blowing in its favor. As mentioned earlier, the Senate Committee on Homeland Security and Governmental Affairs just completed four hearings entitled “*Chemical Facility Security: What Is the Appropriate Federal Role?*”. According to transcripts committee members share a consensus that federal legislation is needed to shore up safeguards at dangerous sites. In fact, several competing bills are now being considered. Most prescribe a laundry list of security measures for chemical facilities to abide by, as well as various punishments for those who refuse to comply.

Political support also comes from the chemical sector’s largest and most powerful trade association, the American Chemical Council (ACC). The ACC has repeatedly asked for industry regulation to strengthen the protection of facilities.⁷¹ This group is not alone in its call for government intervention. Several other trade, environmental and professional organizations are currently seeking political action to improve chemical facility security. Moreover, the Secretary of DHS believes legislation is necessary to address the problem. In addition, Secretary Chertoff has repeatedly stated that FLEXIBILITY is the key to any effective and long-term federal proposal.⁷² Flexibility is exactly what the strategic idea provides. While it is likely that the proposal will include some national minimum security standards and common procedures, regional partnerships will have substantial flexibility to tailor operations to their specific needs.

Since the political landscape is already close to a tipping point, it seems intuitive that Secretary Chertoff should seize the opportunity and promote the strategic idea as a

⁷¹ Martin Durbin, *Chemical Facility Security: What Is The Appropriate Federal Role?*, Testimony before the Committee on Homeland Security and Governmental Affairs, July 13, 2005, 7.

⁷² Darren Goode, *Chertoff Wants Flexibility in Managing Chemical Plant Safety*, March 21, 2006, <http://www.govexec.com/dailyfed/0306/032106cdpm1.htm> (Accessed March 26, 2006).

potential solution for improving chemical facility preparedness. As discussed above, the proposal provides the necessary flexibility that DHS seeks. It is also likely to yield more effective long-term protection results for sites than that which static federal mandates can achieve. Furthermore, facility owners/operators will probably embrace the regional public-private partnership approach, as compared to strict federal regulations, since they will be significantly involved in the proposal's development and execution. In essence, the strategic idea can create a "win-win" situation for the private and public sectors.

The next challenge for DHS is overcoming the resource hurdle. The chemical industry encompasses nearly 66,000 facilities scattered across the country. At first glance, securing all of them seems like an insurmountable task. However, many experts agree that only a small percentage of this universe presents enough of a danger to warrant regulation. In fact, most of the current legislative proposals now up for consideration in Congress concentrate protection efforts on approximately 5%-20% of sites. Safeguarding between 3,000-15,000 sites will obviously necessitate fewer resources than what is needed to protect all 66,000.

In addition, since portions of the chemical sector are highly interconnected, the resource obstacle can further be minimized by focusing on protecting the most critical nodes (e.g., hubs). This is a point in a network which represents where an attack would cause the greatest damage. If a network's hubs are sufficiently defended, then the entire network is protected with the least cost.⁷³ This approach reduces the problem of size and complexity to a more manageable task of selective investment.⁷⁴ As a result, fewer resources are required.

Other resource reductions will be produced by the strategic idea since much of the work for carrying it out is "outsourced" to regional partners. DHS will simply be in charge of initiating, overseeing and facilitating the proposal. Obviously, in the long-term this strategy requires much less effort than if the Department of Homeland Security alone actually had to perform all the necessary functions.

⁷³ Dr. Ted Lewis, *Critical Infrastructure Protection*, 21.

⁷⁴ Ibid.

Further resource reductions can be achieved by multiplying the value of current assets. This represents one of the powerful benefits of the strategic idea.⁷⁵ Its region-wide approach to chemical facility protection encourages the pooling of assets and efforts through partnerships. For example, facility owners/operators currently implement security measures according to their own individual needs. Little thought is given as to the environment outside one's fenced borders. Generally, this kind of micro perspective and isolated decision-making leads to wasted resources. To illustrate, many facilities now have their own security force. However, due to economies of scale, it is likely that fewer personnel would be needed if security functions were shared among sites within a geographical region. Also, each facility would not need its own security center. Technology costs would be reduced since fewer items are needed. Equipment such as radios, cameras and recording equipment would be interoperable instead of being incompatible. Region-wide joint training and common operating procedures could yield additional efficiencies.

Breaking through the cognitive barrier primarily entails having facility managers realize their current security efforts are insufficient to protect them against terrorism. Currently, most of them have the opinion that reasonable safeguards are already in place and that additional steps are not needed. Facility owners/operators apparently feel they have a grasp of the threat against them as well as an accurate understanding of their own vulnerabilities. Based on these perceptions, plant officials believe they have implemented adequate security measures to have driven risk down to an acceptable level. Accordingly, to overcome these cognitive hurdles, plant officials must acknowledge that gaps exist in their summations. One way this can be accomplished is to have facility owners/operators come face-to-face with poor performance.⁷⁶ For example, they can conduct surprise tours of each others' plants to see weaknesses first hand. Recently, several similar site visits were conducted by undercover news investigators and their findings shocked both the public and politicians. Plant owners/operators responded by saying the reports were only representative of a small percentage of the industry and more of an anomaly than the norm. Actually seeing the problems firsthand may change their perceptions. Another way

⁷⁵ Chan and Mauborgne, *Blue Ocean Strategy*, 156.

⁷⁶ *Ibid.*, 153.

to cause the necessary paradigm shift is to have plant officials accompany “red-teams” who test sites’ security. In the past, these exercises have discovered major soft spots in protective measures and served as the impetus for changes in their operations. Combined, the results of these two efforts could persuade owner/operators that additional chemical facility preparedness efforts are needed.

After overcoming the political, resource and cognitive hurdles, the stage will be set to maneuver around motivational obstacles. Facility owners/operators exert the primary resistance to improvements in chemical facility security. Their opposition is based on three key arguments. First, most managers believe additional protective measures will cost them too much. However, by taking a regional approach and pooling resources, security cost concerns can be greatly reduced. Second, a majority of plant officials simply say they are not required nor encouraged to upgrade their sites’ current security. No laws or incentives exist to drive additional changes but both are created with the implementation of the strategic idea. Third, many facility owners/operators feel they have already put into place reasonable safeguards. They claim that extra measures are not necessary and will result in wasted resources if implemented. However, as discussed above, the proposal will likely cause this viewpoint to shift in favor of new efforts. By immersing plant managers in the process of developing and carrying out the strategic idea, they should come to understand that individual security efforts are inadequate to deal with the challenge of terrorism. Plant officials will also learn that a regional public-private partnership approach is much more effective than current efforts.

Motivation can be further enhanced by promoting the regional aspect of the strategic idea. It tackles the problem of chemical facility “insecurity” incrementally, one region (e.g., “atom”) at a time, plant by plant. Using this approach, the challenge appears much more attainable and actionable. Accordingly, motivation should be high and eventually lead to a strategic shift in the perceptions of stakeholders. A second way to jumpstart motivation is to focus on key influencers (e.g., kingpins) within a region. Motivation can be achieved by empowering and elevating kingpins to execute the strategic idea. Performed properly, this step can trigger a movement of the masses. One way the proposal accomplishes this outcome is that it uses key influencers within a geographical area to meaningfully participate in partnership efforts. They are assigned

significant roles and responsibilities. With key influencers having position and power, conditions are ripe for motivation to spread throughout the organization. Last, motivation can be instilled by increasing the transparency of actions. This visibility represents one of the strong points of the strategic idea. It calls for kingpins to provide public reports and open testimony, and to hold meetings in which citizens can actively participate. This process also ensures key influencers are held publicly accountable.

I. PILOT INITIATIVE

The strategic idea represents a significant departure from the status quo. Therefore, its implementation will likely cause DHS to face major technical difficulties. As such, a pilot project should first be initiated as part of a staged implementation process. By doing so, DHS will be able to determine or prove the cause and effect relations between particular solutions and desired effects.⁷⁷ This step allows DHS to decide what proposed techniques do and do not work so that modifications can be made before going nationwide with the strategic idea. Also, staging implementation involves organizing a series of small wins on the way to full-scale implementation of the proposal.⁷⁸

A pilot initiative to test the proposal will involve the following steps:⁷⁹

- *Determining the validity of proposed changes utilizing quasi-experimental designs.* For example, pre-post design tests can be applied to regions where the proposal is piloted. By conducting analyses (using surveys, observations, interviews, reasoning, etc.) causal inferences can be made.
- *Performing tests in a quasi-controlled environment.* For example, non-equivalent groups design (NEGD) can be used. This test involves selecting two regions, or groups of regions, that are as similar as possible so fair comparisons can be made between the treated one (e.g., where the proposal is pilot tested) and the controlled one.

⁷⁷ John M. Bryson, *STRATEGIC PLANNING for Public and Nonprofit Organizations*. (San Francisco, CA.: Jossey-Bass, 2004), 263.

⁷⁸ Ibid.

⁷⁹ Ibid., 260.

- *Testing several possible proposal variations, and searching for their different strengths and weaknesses.* This process simply involves applying altered versions of the strategic idea in different regions. Afterwards, outcomes are measured and deductions are made as to what form of the proposal caused the most effective results.
- *Using experimental specialists to evaluate “cause and effect” relationships.* Here, experts are brought into the experimental region during the early stages of proposal implementation to ensure evaluation experiments are valid and reliable. In addition, these professionals will improve the credibility and objectivity of test results.
- *Designing tests to measure effectiveness of proposed changes, not their efficiency.* One way this goal can be achieved is to use red-teams in both experimental and controlled regions. The purpose of red-teams is to surreptitiously penetrate a facility’s security. The results of their attempts are then used to evaluate the effectiveness the proposal.

J. SUMMARY OF JOINT PREPAREDNESS EFFORTS

To better safeguard Americans from suffering a Bhopal-like catastrophe, it is imperative that a new approach to public-private partnering be designed, implemented and sustained. Current voluntary efforts have not yet produced adequate results. In addition, based on various environmental conditions, relying on strict mandates is not likely to be DHS’s optimum long-term alternative. According to the above analyses, the option which uses a mixture of mandates and incentives should result in the most effective outcome. In addition to its utility, the Department of Homeland Security’s adoption of a balanced approach will exemplify its commitment to the belief that homeland security is a shared responsibility. The proposal also illustrates that the DHS truly values its homeland security partners.

Determining how the public and private sectors should join forces to improve chemical facility preparedness is just one piece of the puzzle. It is also important to fully understand what tools the new partnerships can use to reduce the attractiveness of sites as targets of terrorism. For the most part, these instruments fall into two broad categories—

mandates and incentives. Deciding the proper mix of each will be critical to the outcome of the strategic idea. Just as important is how these tools are ultimately developed, implemented and sustained by regional partnerships. This process will be key to the long-term success of the proposed effort.

IV. COMPARATIVE GOVERNMENT ANALYSIS

A. A MIXED BAG OF APPROACHES

As it stands now, chemical facility security efforts include a mixture of local, state and federal laws.⁸⁰ Not surprisingly, this composite of approaches yields varying outcomes. Reviewing each of these methods and comparing their strengths and weaknesses may provide insights for how to proceed to ensure the preparedness of the nation's chemical facilities for acts of terrorism. Also, mandates have been used in other sectors (water and power/energy) to address similar critical infrastructure protection concerns. Solutions to these analogous problems may be applicable to chemical sites. Furthermore, several chemical facility security bills are now being considered for passage. The front-runner is the Chemical Securities Act (CSA). It includes a variety of mandates that, if passed, plants will have to comply with. Assessing the likely advantages and disadvantages of the CSA could provide additional direction for preparedness efforts.

B. CURRENT MANDATES

Some believe that current voluntary efforts alone are not sufficient to adequately protect the nation's chemical facilities from terrorism.⁸¹ This group is largely comprised of environmental organizations, activists, emergency responders and many in government. This camp proposes relying heavily on mandates to force plant owners/operators to adhere to specific measures. Most of these tasks focus on fortifying sites. In accordance with this position, some mandates have been enacted on a limited basis by local, state and federal officials to better prepare chemical facilities for acts of terrorism.

1. Local

A handful of local jurisdictions have taken aggressive actions to improve nearby chemical facility security. This approach involves enacting ordinances mandating chemical facility managers to improve their preparedness for attacks. For example, in 2002, officials in Contra Costa County, California, instituted a requirement forcing

⁸⁰ Dana Shea, "Legislative Approaches to Chemical Facility Security", *CRS Report for Congress* (Washington D.C.: Congressional Research Service, August 16, 2005), 2.

⁸¹ *Ibid.*

operators of chemical facilities within its borders to consider incorporating inherently safer technologies into their operations.⁸² These safeguards could include the use of less lethal or volatile chemicals and altering refinery processes to make them less dangerous.

In 2005, the City of Baltimore, Maryland, passed a landmark ordinance, believed to be the first of its kind in the nation. It requires chemical manufacturers to follow a set of safety and security regulations devised by local fire and police commissioners.⁸³ Penalties such as withholding or suspension of facility operating permits can be assessed for non-compliance.⁸⁴ This ordinance was developed with the cooperation and support of the Maryland Chemistry and Industrial Technology Alliance (MIDCITA), which is the state equivalent to the American Chemistry Council.

Both of these local statutes had very positive outcomes. They did require nearby chemical facilities to implement specific protective measures. The ordinances also established a permanent procedure whereby companies and security partners could share sensitive information with confidentiality. However, more important than any result are the actual processes. The Contra Costa case represents the first time that a local government pursued statutory action to mandate certain safety and security requirements for chemical facilities. In Baltimore, the city council took the new step one further. It used a collaborative public-private sector partnership to focus on plant protection. Local officials and MIDCITA joined forces to develop preparedness requirements that were in the best interests of all parties. This effort was the first time that a truly participatory approach was taken by government and the private sector to reduce the attractiveness of chemical facilities as targets for terrorists. Ultimately this strategy demonstrates what is possible when business and government work together in good faith toward a common goal. Many observers hail these ordinances as a model for what other local agencies should do to protect citizens and improve chemical facility preparedness within their communities without negatively impacting the industry.

⁸² Stephenson, "Voluntary Initiatives Are Under Way," 15.

⁸³ Ibid., 16.

⁸⁴ Ibid.

In spite of the successes of the ordinances, they do have one significant downside. The new mandates only apply to those sites located within the boundaries of the local governing bodies that passed them. Facilities just outside the jurisdiction are not impacted. This shortcoming is a major weakness of the local approach because if a facility experiences a catastrophic chemical release, its consequences could extend over several miles. Deadly airborne agents will not simply stop at city-limit signs. Neighboring towns and counties are going to be affected. Other levels of government recognized this drawback and pursued alternative courses of action.

2. State

A third approach used by two states was to pass laws to strengthen security efforts at chemical facilities within their borders. Maryland was the first to enact statewide chemical security legislation in the U.S. by passing the Hazardous Material Security Act (HMSA). It requires prioritization of facilities, the development and implementation of security measures commensurate with risks, training, drills and guidance, communications with employees, communities and government agencies, internal audits and third party verification. The Maryland law is also consistent with Baltimore's local ordinance regarding chemical security passed just one year earlier. Facilities covered by the HMSA must report to the Maryland Department of the Environment and the Maryland State Police.⁸⁵

In addition, New York officials passed the Anti-Terrorism Preparedness Act of 2004.⁸⁶ It mandates that New York's Office of Homeland Security review the vulnerability of chemical facilities and suggest necessary improvements. The same office must identify which chemical plants are covered by the new law, but it exempts facilities holding fuel for sale and facilities that are water suppliers because they are already governed by another office.

The benefits of the state approach are similar to those achieved by the local method. Basically, chemical facilities owners/operators are forced to institute prescribed security measures, but on a statewide scale. As a result, plants became more fortified. However, there are disadvantages. First, as in the local approach, the mandated laws only

⁸⁵ Shea, "Legislative Approaches," 4.

⁸⁶ Ibid.

apply to facilities located within Maryland and New York. Plants in neighboring states are unaffected. Consequently, a toxic release at a site in an adjacent state can still threaten the lives of those in New York or Maryland. For this approach to be truly effective, all other states will need to enact similar chemical facility preparedness legislation. But in states where there is not sufficient support for these kinds of laws, passage is unlikely. A second problem exists with the way in which the statewide mandates were crafted. Their development involved little input from industry officials. This process was not nearly as participatory as the local approach in which collaborative efforts were the norm. Consequently, the chemical security laws passed by the states are more rigid than their local ordinance counterparts and there is less buy-in from the private sector. Combined, these two factors have a tendency to reduce voluntary compliance.

3. Federal

The last approach to review involves federal efforts designed to improve facility protection at certain high-risk sites. Examining the effectiveness of these “other” cases may provide specific lessons-learned for how to better protect the country’s chemical facilities.

In 2002, Congress passed the Maritime Transportation Security Act (MTSA). Under the act, the U.S. Coast Guard (USCG) must conduct risk assessments of all vessels and facilities on or near the water; develop national and area maritime transportation security plans; and approve port, facility and vessel security plans.⁸⁷ Afterwards, Coast Guard personnel must forward these plans to the Environmental Protection Agency. The USCG must also visit MTSA sites at least annually to ensure continued compliance. The effect of this effort has been to establish a baseline level of security at 238 chemical facilities located within ports.

Some in Congress believe the MTSA is THE model approach that federal policymakers should apply to all hazardous chemical facilities, not just those near the water.⁸⁸ The MTSA has forced high-risk facilities located within shipping corridors to implement measures (fencing, lighting, video cameras, 24-hour monitoring, etc.) to improve security. But, there are limitations to trying to apply the MTSA to all RMP

⁸⁷ Shea, “Legislative Approaches,” 5.

⁸⁸ Collins, “Chemical Facility Security,” 2.

facilities. As mentioned, the act only affects 238 plants, a relatively small number compared to the 15,000 RMP sites spread throughout the country. This larger universe makes enforcement much more difficult. Who ensures each site's initial compliance and conducts all of the annually required follow-up inspections? How would this task be accomplished since most chemical plants are not located together in shipping ports?

C. ANALOGOUS PROBLEMS

Nuclear power plants have long been recognized as potential targets for acts of terrorism.⁸⁹ A catastrophic release at any one of these facilities may lead to the dispersal of radioactive materials over several square miles. Depending upon the dosage level, human exposure could result in short-term illness and death, as well as long-term deaths by cancer and other diseases. Because of these risks, nuclear power plants are subject to strict regulation and legislation regarding site preparedness. However, after the 9/11 attacks, protection of these facilities became even more of a concern. As a result, additional measures were implemented to further prepare nuclear power plants against acts of terrorism. Reviewing and evaluating these instituted security steps may provide clues as to how to better safeguard chemical facilities, since the two sites have common characteristics. For example, both serve vital economic functions, are usually located near population centers and maintain large inventories of toxic materials. Accordingly, an attack at either a nuclear or chemical facility could have devastating financial and human costs.

1. Nuclear Facilities

All commercial nuclear power plants licensed by the Nuclear Regulatory Commission (NRC) must be protected by a series of physical barriers and a trained security force. Each facility is broken down into three zones: an "owner controlled" buffer region, a "protected area," and a "vital area."⁹⁰ The buffer region has the fewest physical barriers and access requirements followed by a more restrictive protected area. The vital area is the most heavily defended and critical zone. The mandated security force must abide by NRC requirements on pre-hiring background investigations and training.

⁸⁹ Carl Behrens and Mark Holt, "Nuclear Power Plants: Vulnerability to Terrorist Attack," *CRS Report for Congress* (Washington D.C.: Congressional Research Service, August 9, 2005), 1.

⁹⁰ *Ibid.*

Nuclear power plants are also required by the NRC to conduct periodic exercises to test its ability to defend against the “design basis threat” (DBT). The DBT is supposed to “represent the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law.”⁹¹ During these “force on force” tests an opposing team from outside the plant attempts to penetrate its vital area and damage or destroy critical safety systems. It is up to the facility’s security force to repel the adversaries. These exercises are NRC-monitored and must be performed every three years. The exact details of the DBT are not released to the public for security reasons.

Nuclear power plants must also have emergency plans in place. In addition, the NRC mandates that within an approximately 10-mile Emergency Planning Zone (EPZ) around each plant, the operator must maintain warning sirens and regularly conduct evacuation exercises monitored by the NRC and the Federal Emergency Management Agency.⁹² Furthermore, in some states, those living within the EPZ can obtain free non-radioactive iodine pills. These pills prevent the absorption of radioactive iodine in the thyroid which would be a significant component of a release from a nuclear power plant. However, the pills offer no protection against other affects of radiation exposure.

Preparedness mandates for nuclear power plants have had several benefits. First, the required physical barriers, access restrictions and layered defenses have made plants “hardened” and therefore much more difficult to attack. In addition, since each location is protected by an average security force of 75 members, protection is further improved.⁹³ Sites in various other sectors do not implement comparable security measures. However, licensees are required to have only a minimum of five security personnel on-duty at any one time, which some say is too low. Another disadvantage is that security forces from other power plants are used to make up the adversarial team for the periodically required force-on-force exercises. This practice often pits guards against each other who are from the same security company. To many, this situation is seen as a conflict of interest. Not

⁹¹ Behrens and Holt, “Nuclear Power Facilities,” 2.

⁹² Ibid., 3.

⁹³ Ibid., 5.

surprisingly, allegations of falsifying exercise results have arisen. To address this issue, it has been suggested that a federal force be created within the NRC to replace the private guards at nuclear power plants.

Furthermore, in some states security personnel at nuclear power plants are not allowed to be armed. Obviously, this restriction greatly limits the level of defense guards are able wage against a determined adversary. For example, the five required on-duty personnel could all be theoretically neutralized by one terrorist with a firearm. Some have suggested that this state prohibition should be preempted by federal legislation. Also, while background investigations are conducted on security guards, similar history checks are not conducted on all nuclear facility employees, as well as those who import and export nuclear materials at sites. Critics believe that this practice represents a weak link in the chain of security which leaves plants vulnerable. They propose that guards, key employees and hazardous material transporters be investigated. A final problem is cost. It is very expensive to maintain the extensive list of mandatory safeguards.

2. Public Health Security & Bioterrorism Preparedness & Response Act

Another relevant federally enacted law is the Public Health Security and Bioterrorism Preparedness and Response Act (PHSBPRA). It amends the Safe Drinking Water Act (SDWA). The act requires water system facilities (e.g. purification plants) serving more than 3,300 people to conduct vulnerability assessments and to develop emergency response plans.⁹⁴ Some federal financial assistance is provided to affected facilities to help them comply with the new requirements. It is important to note that the amendment did not mandate water systems to mitigate their vulnerabilities.

This act focused on water systems for several reasons. First, government officials were concerned about terrorists contaminating water systems. Second, these facilities store large amounts of chlorine and are frequently located in or near densely populated residential areas. Chlorine is extremely toxic and, if released in significant quantities, it can travel airborne for several miles before dissipating to a non-lethal level. Due to this danger, some facilities near critical locations have voluntarily substituted less lethal substances for chlorine in their operations. For example, a water purification site within

⁹⁴ Shea, "Legislative Approaches," 5.

four miles of the U.S. Capitol now uses bleach in its process instead of chlorine. Bleach is not near as fatal as chlorine, and it dissipates much quicker if airborne. These actions combine to greatly reduce the attractiveness of water purification sites as targets of terrorism.

D. PROPOSED LEGISLATION

Since 9/11, various legislative acts focusing on improving chemical facility preparedness nationwide have been crafted and debated on Capitol Hill. One of the most popular plans is the Chemical Security Act (CSA), authored by Governor Jon S. Corzine of New Jersey.

Broadly speaking, the CSA mandates that the Environmental Protection Agency and the Department of Homeland Security work together to strengthen site preparedness. They are required to develop minimum requirements for the improvement of security and the reduction of potential hazards at chemical plants and other industrial facilities storing large quantities of hazardous materials.⁹⁵ Representatives from the EPA and DHS, as well as state and local agencies are to begin their work by first identifying “high priority” chemical sites within one year of the bill’s enactment. To accomplish this task, the EPA and DHS must start with the 15,000 RMP facilities. By applying criteria like proximity to population centers and other critical infrastructure, the universe of RMP facilities will narrow to eventually produce a list of high priority sites. These identified facilities will be the only ones subject to the act’s requirements. This process is meant to weed out sites located in remote areas, including the vast majority of the agricultural facilities currently subject to the EPA’s RMP requirements.

Next, the CSA requires the EPA, DHS, and state and local agencies to develop regulations to require high-risk chemical facilities to:

- Conduct vulnerability/hazard assessments and

⁹⁵Jon S. Corzine, “Agenda,” May 31, 2005, http://corzine.senate.gov/priorities/chem_sec.html (Accessed May, 31, 2005).

- Develop prevention, preparedness and response plans that incorporate the assessment results, and include actions to reduce vulnerabilities by improving security and using safer technologies.⁹⁶

High priority facilities must perform the first step within one year of the promulgations of regulations, and the second step must be completed six months later. Afterwards, the EPA and DHS will evaluate the assessments and response plans for compliance. If either is inadequate, the EPA must provide notice and offer compliance assistance. If sufficient corrective measures are not eventually instituted by facility personnel, the EPA can issue compliance orders which are subject to notice and hearing requirements.⁹⁷

The Chemical Security Act encourages continued voluntary industry security measures through an “early compliance” provision. It allows high priority facilities to submit assessments and response plans for review any time after the bill becomes law. Assessments and plans received prior to the publication of draft regulations will be evaluated based only on the specific wording of the legislation, and will not be subject to the requirements later established in regulations.⁹⁸ This provision is intended to ensure current voluntary preparedness efforts are not inhibited.

The CSA exempts the information contained in the submitted assessments and response plans from disclosure under the Freedom of Information Act (FOIA) in order to protect it from those who would use it to do harm. The bill does require that certifications of regulation compliance be made publicly available. In this way, citizens will know what facilities are abiding by the CSA while vulnerable information is not unnecessarily exposed.

The Chemical Security Act represents a comprehensive approach to resolving chemical facility vulnerabilities. Basically, the bill requires all high priority sites to identify their chemical hazards, take actions to reduce the possibility of releases, and minimize the consequences of any releases that do occur. These steps would fill in part of

⁹⁶ Jon S. Corzine, “Agenda,” May 31, 2005, http://corzine.senate.gov/priorities/chem_sec.html (Accessed May, 31, 2005).

⁹⁷ Corzine, “Agenda,” http://corzine.senate.gov/priorities/chem_sec.html (Accessed May 30, 2005).

⁹⁸ Ibid.

a large void that currently exists in the nation's chemical safety law. The bill proposes constructive steps toward a national prevention and chemical security program, and gives government additional tools to protect communities in the new era of terrorism.⁹⁹ The CSA also creates a prevention hierarchy for accidental and intentional releases—from prevention as a first resort, to add-on controls, security and buffer zones. Doing so puts prevention as the top priority. This approach addresses the fundamental difference between preventing a chemical facility disaster and trying to control it.¹⁰⁰

Unfortunately, the CSA does not require periodic follow-up inspections of security measures after their initial approval like the MTSA does. This drawback prevents reasonable assurances that instituted measures are working properly and security procedures are being appropriately practiced. Another disadvantage is that the bill is not very inclusive of the private sector. While local, state and federal officials are involved, there is little mention or use of the private sector. This group possesses a wealth of industry knowledge that could be of value. Private sector's buy-in is generally critical for effectiveness, but it will likely be low without sufficient input. Furthermore, the CSA does not address the issue of "insider" threats. For example, how rigorous should background investigations be for employees and contractors? An effective security plan is only as good as its weakest link. Finally, the CSA will only apply to high priority sites. That means thousands of chemical facilities will be left unregulated by DHS. Therefore, it will be business as usual for the bulk of RMP sites.

E. SUMMARY OF APPROACHES

There are those (environmental organizations, activists, emergency responders and many in government) who promote relying heavily on federal mandates to force plant officials to abide by a laundry list of tasks. Most efforts revolve around fortifying sites. Proponents state that this kind of regulation is needed because of the lax security that continues at most chemical facilities, which plant managers refuse to properly address. A history of news reports, undercover investigations and cursory government

⁹⁹ Paul Orum, *Terrorism and Chemical Plant Security – Testimony and Response*, Testimony before the Subcommittee on Superfund, Toxics, Risk and Waste Management, Senate Environment and Public Works Committee, November 14, 2001, http://www.ehw.org/Chemical_Accidents/CHEM_OrumTestimony_2001.htm (Accessed May 31, 2005).

¹⁰⁰ Ibid.

inspections at several key facilities where security was found to be lacking seem to substantiate their claims.¹⁰¹ This camp argues that without mandates, any added protective measures by the industry will only be “window dressing,” and not likely effective. As a model for what stringent requirements can yield, these proponents point to the high level of security at the nation’s nuclear facilities, which they consider safeguarded. They believe the same can be accomplished for the chemical industry.

Relying heavily on government mandates to remedy existing vulnerabilities is unlikely to be as useful a strategy for the chemical sector as it was for the nuclear power industry. Mandates are generally more effective when coupled with adequate oversight and/or a high level of voluntary compliance. Oversight is obviously easier for the country’s 65 or so nuclear plants; however, it would be much more difficult for the nation’s 66,000 chemical facilities.¹⁰² Also, mandating site preparedness measures has been a mainstay of the nuclear industry since its inception. As a result, an expectation and acceptance of oversight is ingrained into the organizational culture of the nuclear industry. Furthermore, the near disaster at Three Mile Island in Pennsylvania has served to raise an already heightened perception of the danger associated with nuclear plants. Therefore, compliance with federal mandates for nuclear sites is relatively high. However, a major chemical facility catastrophe has not happened on U.S. soil in nearly 60 years. Last, the chemical industry has operated with practically no stipulations regarding how facilities should be secured. Both facts make relying solely on government mandates to safeguard sites difficult at best. Something more is needed given the size, scope and history of the problem.

The principle benefit of a mandated approach is that established security standards provide a minimum guarantee regarding preparedness, assuming they are enforced.¹⁰³ But, there are downsides to using “sticks” to get results. First, minimum

¹⁰¹ Carl Prine, “Chemical Sites Still Vulnerable,” *Pittsburgh Tribune-Review*, November 16, 2003, http://www.pittsburghlive.com/x/pittsburghtrib/news/specialreports/potentialfordisaster/s_165518.html (Accessed June 17, 2006).

¹⁰² Behrens and Holt, “Nuclear Power Plants,” 5.

¹⁰³ Peter Orszag, *Statement before the National Commission on Terrorist Attacks Upon the United States*, November 19, 2003, http://www.9-11commission.gov/hearings/hearing5/witness_orszag.htm (Accessed April 13, 2006).

standards may be set at an inappropriate level.¹⁰⁴ They could be too high for some sites and too low for others. Second, government requirements often prove to be an unnecessarily expensive and inefficient way to achieve a given degree of protection.¹⁰⁵ Significant resources are often needed to ensure compliance. For example, inspections, audits and other bureaucratic “red tape” activities are usually necessary to enforce government requirements. Third, mandates do not generally provide incentives for innovation.¹⁰⁶ In fact, depending on how requirements are written, they may actually impede innovation.¹⁰⁷ Last, mandates usually establish a threshold which becomes the lowest common denominator that companies will meet but are unlikely to exceed.

The disadvantages listed above can all be substantially reduced, although not entirely eliminated, through careful attention to the design of mandates. To improve effectiveness, necessary mandates must focus on outcomes and performance, instead of inputs and activities. Such a results-based approach can provide some measure of encouragement for organizations to be innovative while still attaining a given level of security.

The various mandates discussed herein represent myriad ways in which preparedness measures have been imposed, or proposed, for various types of high-risk facilities. These approaches have their advantages and disadvantages. Distilling the effective parts of each effort is important since, in all likelihood, some mandates will be necessary in the development of a new policy to reduce the attractiveness of chemical facilities as targets for terrorists. However, even properly developed mandates are not enough. Efforts will need to focus on ways to motivate owners/operators of chemical facilities to willingly implement appropriate preparedness measures on their own.

¹⁰⁴ Peter Orszag, *Statement before the National Commission on Terrorist Attacks Upon the United States*, http://www.9-11commission.gov/hearings/hearing5/witness_orszag.htm (Accessed November 19, 2005).

¹⁰⁵ Ibid.

¹⁰⁶ Ibid.

¹⁰⁷ Ibid.

V. INCENTIVES

A. INTRODUCTION

When addressing homeland security issues, the conventional Washington wisdom is to search for an easy solution, often turning to regulating industries into compliance with new federal requirements.¹⁰⁸ However, homeland security requires a multifaceted strategy to prevent, protect against and respond to 21st century threats. Mandates tend to lose utility with the passage of time, since they are generally static versus the evolutionary nature of threats. To stay a step ahead of adversaries, efforts must be more flexible and adaptive. But despite their disadvantages, regulations will likely be a necessary component, not the cornerstone of a holistic approach to chemical facility preparedness. They can be effective to a point, if properly designed and implemented.

In addition to mandates, incentives could be used to reduce the attractiveness of chemical facilities as targets of attack. Developed in cooperation with stakeholders, these powerful instruments can create a strong motivating force to encourage chemical facility officials to voluntarily improve their sites' preparedness. Incentives for owners/operators of chemical plants may take various forms. For example, "On any CEO's wish list of outcomes from a proactive security strategy are lower insurance premiums, reduced legal liability, decreased tax liability, safe-harbor provisions, recognition from the government and its private sector peers, enhanced reputation, and reduced incident response and recovery costs."¹⁰⁹ Some of these carrots are currently in use to a limited extent in the chemical industry. The remaining ones have been successfully utilized in other critical infrastructure sectors to improve their preparedness.

The desired outcomes mentioned above are the intended results of various disconnected initiatives. No overarching strategy connects them. Current sector efforts include industry trade association initiatives, federal outreach programs, grants and tax credits. Also, some insurance incentives and liability protection measures are utilized to

¹⁰⁸ Frank Cilluffo, *Preventing Terrorist Attacks on America's Chemical Plants*, House Committee on Homeland Security, June 15, 2005, http://www.gwu.edu/~dhs/congress/june15_05.htm (Accessed March 5, 2006).

¹⁰⁹ Ibid.

motivate chemical site owners/operators to implement added safeguards. Reviewing these approaches and evaluating their effectiveness may provide direction for how to improve chemical facility preparedness. Illustrations of each are provided below for review.

B. INDUSTRY TRADE ASSOCIATIONS

Strengthening chemical plant protection using incentives such as enhanced industry reputation, reduced incidence response time and costs, lowered liability exposure and decreased recovery costs generally occurs via membership in trade associations. Currently, the most popular and recognized organization is the American Chemistry Council (ACC). Plant officials who agree to join the ACC must adhere to its Responsible Care Code program's self-initiated set of requirements. Among other things, the program calls for companies to assess their vulnerabilities and develop appropriate action/response plans. As a result, preparedness at members' sites is improved. In addition, companies reduce their legal liability exposure and they potentially lower their recovery costs in the event of a disaster. Even so, the Responsible Care Code program has two key shortcomings. First, the initiative's membership includes only a small portion (10%) of the universe of chemical facilities.¹¹⁰ It also lacks fixed metrics and standards for quality control.¹¹¹

While chemical facilities belong to other trade associations, evidence suggests that many sites are still inadequately protected. In fact, according to the Department of Homeland Security, approximately 20% of the overall sector believed to be at high-risk does not subscribe to any voluntary industry security standards.¹¹² In addition, testimony by industry observers and policymakers supports this position. Even representatives from the ACC publicly recognize that voluntary efforts will not sufficiently protect facilities and now seek federal legislation for the industry. Many experts have concluded that the risk of a terrorist attack at a chemical site is insufficient to motivate plant owners/operators to voluntarily join industry safeguard programs.

¹¹⁰ Cilluffo, *Preventing Terrorist Attacks on Chemical Facilities*, http://www.gwu.edu/~dhs/congress/june15_05.htm (Accessed March 5, 2006).

¹¹¹ Ibid.

¹¹² Collins, *Chemical Facility Security*, 2.

Two primary reasons impact why voluntary initiatives alone will likely never lead to the kind of chemical facility preparedness that is necessary. First, most plant managers worry that implementing protective measures will put them at a competitive disadvantage. Second, unique issues associated with industry-driven efforts determine adequate security.

Security is not free, and it is generally not cheap. Significant costs will be borne. If a company does not believe other facilities will or are able to make similar investments, it faces the likelihood of losing market share while displacing the industry's vulnerabilities somewhere else. Furthermore, if terrorists attack chemical sites, the security investing facility will incur the same disruptive consequences of a strike right alongside those companies that did nothing to prevent it. As a result, chemical facility protection suffers from the dilemma frequently referred to as the "tragedy of the commons." An example may help explain this concept.

One day a chemical facility operator decides to implement certain security measures that require an increase in product cost by \$10 per widget. Other competitors, however, decide not to make the same investment. As a result, competitors are able to attract market share away from the security conscious plant because of their lower prices. In addition, terrorists desiring to strike this sector will likely choose to attack the competitors since they are "softer" targets. If the attack is successful, its consequences will not be limited to just the low-cost operations. The impacts will likely be felt by all facilities. For example, insurance costs across the board will probably increase and stiff legislation for the entire sector may be forthcoming. Other disruptive economic repercussions will in all probability ripple through the entire chemical industry.

Even if the "tragedy of the commons" dilemma could be resolved, the industry still faces unique uncertainty when trying to determine an acceptable level of security. Protective measures usually follow the rule of diminishing returns (i.e., greater investments purchase marginally less additional security). Therefore, at some point, a cost-benefit decision has to be made. Determining the costs of protective measures is relatively easy. However, calculating the benefits is much more elusive. To properly accomplish this task, accurate threat information is needed. Typically that kind of

information is tightly controlled by government officials, and it is frequently non-specific. Because of this situation, chemical facility operators are simply left to make their best guess regarding how much protection to invest in. Clearly this situation is less than ideal for determining how limited preparedness funds should be invested.

C. BUFFER ZONE PROTECTION PROGRAM GRANT

A federal initiative aimed at strengthening safeguards at selected chemical facilities is the Department of Homeland Security's (DHS's) Buffer Zone Protection Program (BZPP). Through the BZPP, DHS works with local law enforcement officials and facility owners to improve the security of the area surrounding a site or "outside the fence."¹¹³ This program intends to improve the security of the area, making it more difficult for terrorists to conduct surveillance or to execute an attack. As a result, the implemented security measures create a "buffer zone" to further protect a facility. The added protection also generates other benefits. For example, plant officials lower both their insurance costs and legal liability exposure.

A DHS team of subject matter experts (SMEs) initiates the BZPP process with a technical assistance visit to a high-risk chemical facility. High-risk sites are defined as those that, if attacked, could cause death or serious injury to 50,000 or more people.¹¹⁴ Nationwide, DHS has identified 259 such facilities. Although SMEs are deployed by DHS, they are drawn from government and industry. Members possess extensive experience in areas such as physical security measures, system interdependencies and terrorist attack planning. The team begins their work by evaluating a site's vulnerabilities, as well as the neighboring community's capability to prevent and to respond to an attack. Next, current threat information is shared with company officials and vulnerability reduction measures are suggested. The DHS team then brings together the appropriate local emergency response officials and trains them regarding how to assess buffer zone security and identify measures to mitigate vulnerabilities.¹¹⁵ This process typically lasts one to two days.

¹¹³ John B. Stephenson, "Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed," *GAO Report to Congress* (Washington D.C.: General Accounting Office, January 2006), 25.

¹¹⁴ *Ibid.*, 26.

¹¹⁵ *Ibid.*, 25.

Afterwards, local emergency response officials perform an assessment of the buffer zone and describe desired protective measures to strengthen the area. All of this information is recorded in a Buffer Zone Protection Plan and sent to DHS for review. If DHS approves the plan, federal funding assistance is provided to local emergency response officials to acquire and implement identified protective measures. Generally, the maximum award is \$50,000 per high-risk chemical facility.

The BZPP produces several favorable outcomes. First, the program implements additional security steps at participating sites, improving their preparedness. Furthermore, costs of the new safeguards are partially or totally offset by federal funding thus stretching scarce private sector resources. Second, according to DHS officials, the collaborative process helps facilitate relationships between owners/operators and the various response and law enforcement entities in the community.¹¹⁶ As a result, lines of communication have opened up. Third, facility personnel and local officials are advised of relevant threats to their sites and both parties receive valuable training with respect to assessing and addressing vulnerabilities. These advantages are likely to sustain stakeholders' participation for the long-term. Finally, the BZPP is part of a layered approach. It is one of the few initiatives that looks outside the fences of facilities.

There are, however, a few disadvantages of the Buffer Zone Protection Program. For example, it only applies to 259 chemical facilities, a small fraction of the 15,000 RMP facilities that exist. Second, the BZPP primarily focuses on measures to protect the area surrounding a site. Little attention is concentrated on steps to safeguard, or reduce, the attractiveness of a facility's interior where the most damage often can occur. Not all attacks need to be launched from outside the gates of a facility. To illustrate, a terrorist working as a facility employee or security guard would likely not be deterred by a BZPP. Third, the program relies heavily on the voluntary participation of site owners/operators. In fact, without their permission, DHS has no legal right to enter their facilities to conduct the BZPP. Furthermore, DHS personnel can ask but generally not demand BZPP-related records or information from plant officials. Some company executives are hesitant to share sensitive documents with DHS because they are concerned about

¹¹⁶ Stephenson, *Homeland Security*, 25.

information security and protection. Others worry that the BZPP data may expose costly vulnerabilities that facility managers are unable or unwilling to address. As a result, if attacked, this situation could lead to additional liability for the participating facility.

D. INSURANCE MEASURES

In most developed nations, one of the principle tools used by organizations for managing risk is insurance.¹¹⁷ Indeed, insurance is a key mechanism for aiding in recovery after a disaster and ensuring social and economic continuity. It played a pivotal role following the 9/11 attacks. Two-thirds of the \$33 billion in insured losses from the disaster were paid by reinsurance companies that operate at a larger level worldwide.¹¹⁸ A well-functioning insurance market is also critical to preventing or mitigating losses from catastrophes. This protection is most often achieved by offering insurance discounts for the implementation of certain preparedness measures. To illustrate, the insurance industry drove municipalities toward stricter building codes and a focus on fire prevention rather than only responding to fires.¹¹⁹ In exchange, lower fire ratings were provided to cities which reduced their residents' premium costs. Ultimately, fires, fire damages and lives lost in fires all slowly declined.

Currently, several forces require or encourage facility owners/operators to purchase insurance. First, various government agencies mandate sites to carry a minimum level of protection. Usually, periodic inspections or audits are conducted to ensure compliance. Fines are levied and/or operating permits revoked for violations. Second and to a lesser extent, employee groups, shareholders, trade associations, customers and other stakeholders also pressure plant officials to purchase insurance coverage. Each has a vested interest in trying to prevent or minimize the damage a disaster. Collectively, these parties are primarily responsible for why each chemical facility carries its current level of insurance.

For insurance to be an effective tool for managing risk associated with acts of terrorism at chemical facilities, a properly functioning private market is necessary.

¹¹⁷ Philip Auerswald, Lewis Branscomb, Todd La Porte, Erwann Michel-Kerjan, "The Challenge of Protecting Critical Infrastructure," *Issues in Science and Technology Online*, <http://www.issues.org/22.1/auerswald.html> (Accessed April 12, 2006.)

¹¹⁸ Ibid.

¹¹⁹ Cilluffo, *Preventing Attacks on Chemical Facilities*, 9.

Critical to the long-term health of the private market are incentives. They encourage and sustain preparedness-related behaviors. However, many experts agree that under current conditions, private markets by themselves do not generate sufficient incentives for homeland security.¹²⁰ Several conditions support this belief.

- The costs of a terrorist attack will likely extend well beyond the immediate areas and people affected (e.g., negative externalities). Organizations seeking to protect themselves will generally not take these “extra” costs into account and subsequently undertake less investment in safeguards than socially desirable.
- A terrorist attack imposes “contamination effects.” These complications arise when a catastrophic risk faced by one organization is determined in part by the behavior of others, and the behavior of these others affects the incentives of the first firm to reduce its exposure to the risk.
- When trying to prepare for terrorist attacks, a frequently asked question is *How much is enough?* To answer this question, specific threat information is needed but details are often vague. Even if known, the intelligence is generally tightly held by government officials. This situation sets the stage for poor decision-making regarding what safeguards to implement.
- A major terrorist attack is likely to cause losses beyond a firm’s net asset value. These costs are inherently limited by bankruptcy laws. As a result, an organization has little incentive to take total losses into account. Consequently, only measures to prevent losses up to bankruptcy limits will be implemented.
- Some in the private sector now believe that the government will bail them out should a catastrophic terrorist attack occur. They point to the financial assistance provided to the airline industry after 9/11 as one such example.

¹²⁰ Peter R. Orszag, *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentive*, Testimony before the Subcommittee on Cyber-security, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security. House Select Committee on Homeland Security, September 4, 2003, <http://www.brookings.edu/views/testimony/orszag/20030904.pdf> (Accessed June 15, 2006), 2.

This belief creates a “moral hazard” problem—firms expecting to be bailed out by government will undertake fewer safeguards than advisable.

- Under current conditions, imperfections exist in the insurance market. For example, after 9/11 terrorism insurance became extremely expensive. For some, it was not even available. Mostly this shortage was due to the fact that insurance firms were unable to obtain reinsurance coverage. If insurance firms are unable to transfer a portion of their risk, they are unlikely to insure risky assets.¹²¹

For the reasons described above, private markets by themselves fail to provide adequate incentives to support comprehensive homeland security efforts at chemical facilities. In fact, many of the stated shortcomings actually serve to discourage plant owners/operators from purchasing sufficient insurance protection or implementing other appropriate preparedness measures than what is socially desirable. Left alone, the private market is unlikely to overcome these barriers.

According to *The National Strategy For Homeland Security*, “The government should only address those activities that the market does not adequately provide—for example, national defense or border security... For other aspects of homeland security, sufficient incentives exist in the private market to supply protection. In these cases we should rely on the private sector.”¹²² Based on the evidence listed above, it appears that private markets themselves do not produce appropriate incentives for homeland security. Private markets have an important role to play, but government intervention in some form will be necessary to fashion the proper response to the threat of terrorism.¹²³

Insurance can be an extremely powerful tool for strengthening homeland security if properly crafted and supported. Indeed, insurance has the potential to overcome the aforementioned shortcomings. There are at least two ways this can be achieved----with sticks or carrots. For example, legislation can be enacted to force facilities to purchase a given level of insurance. Another possible alternative is a regional insurance

¹²¹ Orszag, *Critical Infrastructure and the Private Sector*, 2-4.

¹²² *National Strategy For Homeland Security*, 64.

¹²³ Orszag, *Statement before the National Commission on Terrorist Attacks Upon the United States*, 4.

requirement.¹²⁴ This would be a geographically established and specific approach that would provide adequate incentives to local facilities to overcome private market inefficiencies. As opposed to applying a “one size fits all” approach characteristic of regulations, elements of an insurance requirement can vary in order to tailor it for geographical areas. For example, regions could craft insurance incentives (e.g., premium discounts for added measures), conduct third-party insurance inspections/audits, establish minimum insurance coverage and deductible levels, provide necessary reinsurance and serve as an insurer of last resort. In addition, a reasonable level of regional indemnification could be provided, similar to the Good Samaritan protection, should agreed upon measures be found wanting following a terrorist attack.¹²⁵ All of these steps could help to modify incentives so that private markets sufficiently encourage chemical facility owners/operators to undertake reasonable preparedness efforts.

An insurance requirement is not a panacea. There are other shortcomings to using this tool. Despite the disadvantages of using insurance to improve chemical facility preparedness, it is plausible that a broader system of anti-terrorism insurance could be developed regionally and thereby play a crucial role in providing incentives to private sector firms to implement adequate security measures.¹²⁶

E. TAX PROVISIONS

Many experts suggest socializing some of the costs related to reducing the attractiveness of chemical facilities as targets of terrorism.¹²⁷ For example, partial government funding for preparedness measures could serve as an incentive to subsidize enhanced preparedness efforts by plant owners/operators.¹²⁸ Currently, the Prevent Act of 2003 accomplishes this function but on a limited basis. The Act allows for a business tax credit of up to twenty percent for the purchase and implementation of security devices and a thirty percent credit for assessments and other expenses incurred while improving

¹²⁴ Orszag, *Statement before the National Commission on Terrorist Attacks Upon the United States*, 6.

¹²⁵ Stephen Flynn, *Ending the Post 9/11 Neglect of America's Chemical Facilities*, Testimony before the Committee on Homeland Security and Governmental Affairs, April 27, 2005, <http://www.iwar.org.uk/homesec/resources/chemical-security/FlynnHSGAtestimony42705final.pdf> (Accessed June 15, 2006), 4.

¹²⁶ Orszag, *Critical Infrastructure and the Private Sector*, 9.

¹²⁷ Farmer, “Homeland Security and the Private Sector,” 27.

¹²⁸ *Ibid.*

security.¹²⁹ These tax breaks create a win-win situation for consumers and manufacturers.¹³⁰ The provisions reduce the financial burden of plant officials to improve their sites' protection while at the same time strengthening homeland security for the public.

The Prevent Act is primarily directed at “add on” technology to increase security. Its focus is on offsetting the costs of purchasing biometric equipment, closed-circuit television and other defensive-related items to fortify locations. Unfortunately, more robust preparedness measures that would reduce the attractiveness of sites for acts of terrorism are not eligible for the tax credit. Some in chemical sector promote the idea of using tax incentives, like the Prevent Act, to reward facility owners/operators who adopt less dangerous processes for making, handling and storing the most lethal chemicals.¹³¹ Other suggestions include using tax credits to improve warning and mitigation systems. In addition, subsidizing joint training, tabletop exercises and simulations are possible considerations.

Government funding of preparedness measures could affect the behavior of chemical facility operators/owners and, if properly designed, provide some protection against terrorist threats.¹³² This form of government intervention, however, brings with it four dangers:

- They can encourage unnecessarily expensive investments in security measures (e.g., “gold plating”).
- This approach may initiate heated political and lobbying attempts that could undermine its intended purpose.

¹²⁹ 108th Congress 1st Session. H.R. 3562, To amend the Internal Revenue Code of 1986 to allow businesses a credit for security devices, assessments, and other security related expenses. (November 20, 2003), <http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.3562.IH> (Accessed June 15, 2006).

¹³⁰ Richard Chace, Tax Incentives for Homeland Security Related Expenses, Testimony before the Subcommittee on Rural Enterprises, Agriculture, and Technology. House Select Committee on Homeland Security, July 21, 2004, <http://wwwc.house.gov/smbiz/hearings/databaseDrivenHearingsSystem/displayTestimony.asp?hearingIdDateFormat=040721&testimonyId=223> (Accessed April 13, 2006).

¹³¹ Flynn, *Ending the Post 9/11 Security Neglect*, 5.

¹³² Orszag, *Critical Infrastructure and the Private Sector*, 9.

- Tax breaks could provide benefits to facilities that possibly would have implemented the measures even in the absence of the subsidy.
- Funding provided from general revenue is effectively paid for by the entire population which some say is unfair and not feasible.¹³³

If tax incentives are used to improve the preparedness of chemical facilities from acts of terrorism, it will likely take a concerted effort to develop and implement an effective system that overcomes the listed dangers. Public-private partnerships will be critical in that effort. Stakeholders with expertise in various areas, working in a transparent environment towards a common goal, could craft a tax incentive policy to reduce their region's attractiveness of chemical facilities as targets of terrorism.

F. MISCELLANEOUS PROGRAMS

Another potentially powerful incentive to improve chemical facility preparedness is the SAFETY Act. This provision currently provides a liability "safe-harbor" for sellers and consumers of certified anti-terror products and services. This certification is awarded by DHS only after conducting a rigorous evaluation process. To qualify, test results must demonstrate that technologies and services are both valid and effective with respect to strengthening homeland security. By purchasing SAFETY Act certified items and services, buyers receive immunity from lawsuits while they enhance their security. Many believe the SAFETY Act is particularly relevant for the chemical sector, as it provides an incentive to facility owners to invest in their own security.¹³⁴

However, like the Prevent Act, the SAFETY Act primarily focuses on encouraging security upgrades. Some have suggested that it could be extended to other products and services that would better prepare chemical sites against acts of terrorism. Extending the SAFETY Act is something Secretary Chertoff has repeatedly committed to doing.¹³⁵ To this end, collaborative preparedness efforts can help. Stakeholders could serve as a filter for DHS to identify and test various products and services that would reduce the attractiveness of chemical facilities within their geographical region.

¹³³ Orszag, *Critical Infrastructure and the Private Sector*, 9.

¹³⁴ Cilluffo, *Preventing Attacks on Chemical Facilities*, 8.

¹³⁵ Ibid.

Currently, federal outreach programs are used on a limited basis as an incentive to motivate chemical plant owners/operators to improve their sites' preparedness for attack. A site visit by DHS usually initiates this effort. To prioritize sites, DHS has separated nation's 15,000 RMP facilities into four tiers using its own metrics. In the top two tiers there are 272 high-risk facilities.¹³⁶ For now, outreach programs focus on these plants.

While on-scene at high-risk locations, federal representatives use their expertise and threat knowledge to perform site assessments. Afterwards, they suggest to plant managers measures to reduce their vulnerabilities. Currently, these "inside-the-fence" assessments have been performed at 38 of the highest consequence facilities.¹³⁷ It is the intent of DHS that through the outreach process, its recommendations are eventually acted upon, thus improving chemical facility security.

Federal outreach programs could serve as one component in a broader system of incentives to promote chemical facility preparedness. To achieve this outcome, some changes are needed to the current process. First, inspectors will need to visit facilities more quickly. DHS only plans to assess 50 plants in FY 2006.¹³⁸ Even if this objective is reached, just 86 facilities will have been visited in the five years following 9/11. At that rate, it will take almost three more years to finish inspecting every top two tier plant, seeing all 15,000 RMP sites is not even a likely possibility. Second, facilities should be visited more often than just once. As threats evolve, so must preparedness measures. This necessitates periodically revisiting plants and meeting with personnel to ensure they are aware of relevant terrorist threats and their sites are adequately protected. However, under the current process, only one "lifetime" assessment is conducted.

Using public-private partnerships can address both shortcomings mentioned above. For example, federal personnel can train stakeholders how to properly perform site assessments. Armed with this new knowledge, partnering members can then visit facilities within their regions to encourage owners/operators to improve their preparedness. In essence, partners will serve as an extension of DHS, allowing sites to be

¹³⁶ Dana Shea, "Legislative Approaches," 6.

¹³⁷ Ibid., 7.

¹³⁸ Ibid.

visited more often and at a faster pace. This “train the trainer” approach should also help build strong local relationships and communication.

A yet-to-be-used incentive within the chemical industry involves publicly recognizing facility operators’/owners’ homeland security efforts. In other words, openly commend those plant officials that attain a given level of preparedness. This approach could encourage managers to improve their sites’ safeguards. In exchange, their reputation is enhanced, liability exposure reduced and insurance costs decreased.

Recently, the DHS Homeland Security Advisory Council and the Council on Competitiveness called for a homeland security award for private industry akin to the prestigious Malcolm Baldrige National Quality Award.¹³⁹ Something similar could be achieved specifically for the chemical sector. To properly develop and implement this effort, public-private partnerships can be used. They could design a public recognition system that sufficiently rewards good performance by plant managers. In this way, industry will recognize the accomplishments of its own. This incentive would be just one more tool available to stakeholders to improve the preparedness of chemical facilities.

G. SUMMARY OF APPROACHES

Even though some improvements in safeguards at chemical facilities have occurred, it does not appear that current voluntary efforts by themselves will lead to the kind of protection that is needed. Simply put, current free market forces alone are insufficient for strengthening homeland security. Something more is needed, however, the approaches described above can be useful. They will serve as templates for future chemical facility preparedness efforts by public-private partnerships. Evaluating both their advantages and disadvantages is beneficial. This process provides valuable clues on how to craft and sustain a model incentive system. In all likelihood incentives will play a key role in a new approach to safeguarding chemical facilities.

¹³⁹ Cilluffo, *Preventing Terrorist Attacks*, 9.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. POSITION

This thesis presents two intertwined arguments. First, regional public-private partnerships can more effectively improve chemical facility preparedness than focusing on individual plant owner/operator efforts. Second, an approach using a mixture of mandates and incentives is better than relying on current corporate volunteerism or imposing specific legislative preparedness requirements for the industry. It is further argued that allowing regional stakeholders to develop, implement and sustain both mandates and incentives are optimal methods to ensure participant collaboration, policy flexibility and effective results. In essence, community governance of preparedness efforts in each region will lead to the best possible combination of outcomes. These claims are based on a study of industry characteristics and current voluntary preparedness programs, as well as a comparative analysis of mandated approaches used by federal, state and local governments. A review of how regulatory standards and enticements have been applied to other analogous problematic areas of federal responsibility provides further support.

According to the findings of this thesis, it seems apparent that a different approach to reduce the attractiveness of chemical facilities as targets for terrorists is needed. Based on the strengths and weaknesses of the various methods and cases reviewed, a new policy utilizing a mixture of region-specific mandates (sticks) and incentives (carrots) may be more effective. The new proposal will need to engage key stakeholders through the use of public-private partnerships (PPPs). This method will encompass much more than just occasional meetings and luncheons. Partners must meaningfully provide their input into creating the proposed policy and actively take part in its implementation and execution. Participants will have to be cross-trained and given important roles and responsibilities in the new approach. Partners will also need to define desired regional outcomes and then identify activities that are likely to lead to them. Furthermore, stakeholders must establish metrics to evaluate the usefulness of the

proposal. Continuous benchmarking is a necessity. This kind of collaborative and results-based system can ensure that the interests of participants are taken into consideration while still yielding effective results.

As in any joint effort, the issue of assigning primary responsibility is likely to arise. Fortunately the available literature addresses this matter. For example, both the Department of Homeland Security and the National Commission on the Terrorist Attacks Upon the United States promote the idea that the private sector should shoulder the bulk of responsibility for reducing the attractiveness of chemical facilities as targets of terrorism. In fact, the *9/11 Commission Report* states this rationale is entirely appropriate since the private sector owns the vast majority of critical infrastructure which includes hazardous chemical facilities.¹⁴⁰ Furthermore, according to the *National Strategy for Homeland Security*, the private sector bears primary responsibility for protecting the public from the risks their facilities pose.¹⁴¹ However, with regard to assigning responsibility to the private sector, a consistent theme arises. The bulk of the literature advocates that the public and private sector should partner together to develop the most cost-effective and comprehensive plan. This sentiment is echoed in the *National Strategy for Homeland Security*.¹⁴² Moreover, HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, promotes partnering by stating the Secretary of DHS “will work closely with other Federal departments and agencies, State and local governments, and the private sector in accomplishing the objectives of this directive.”¹⁴³ The big question is not if the two parties should join forces, but how their collective effort should be structured, what its focus should be, who specifically needs to participate, and what are their roles and responsibilities.

In building the new partnerships, key stakeholders need to first be identified. Ideally, Department of Homeland Security personnel should formally initiate this task for several reasons. First, this office adds a measure of instant credibility to the proposed

¹⁴⁰ *The 9/11 Commission Report*, 398.

¹⁴¹ *National Strategy For Homeland Security*, 33.

¹⁴² *Ibid.*

¹⁴³ U.S. Department of Homeland Security, *Critical Infrastructure Identification, Prioritization, and Protection: HSPD-7* (Washington D.C.: Government Printing Office, December 2003), <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html> (Accessed June 17, 2006).

policy, increasing the likelihood that others will voluntarily participate. For the most part, DHS has a good reputation within the chemical industry, as opposed to the adversarial relationship between the private sector and the EPA. Second, DHS has an extensive knowledge base of the chemical sector. Third, the *National Strategy for Homeland Security* states that the Secretary of Homeland Security is responsible for coordinating and integrating federal, state, local and private sector efforts.¹⁴⁴ Last, the Department of Homeland Security is the lead federal agency for the chemical industry. Accordingly, it seems intuitive that DHS should take a leadership role in reaching out to major participants of the proposed policy.

After the inclusion of the Department of Homeland Security, other principal parties likely to be involved in the suggested policy include emergency responders, environmentalists, insurance personnel, government employees, political leaders, industry association members, sector experts, key officials and citizens. These groups have the power, expertise, resources and networks necessary for the success of the proposed approach. Therefore, obtaining their active support is critical.

The actual framework for how to incorporate representatives from each principal party into the proposed nationwide policy should be broken down into regions. For example, within a geographical area, DHS will map out the chemical facilities using information from the Environmental Protection Agency's current Risk Management Plans and other source data. These selected sites, including their vulnerable zones, are then clustered together to form various regions. Next, Local Emergency Planning Committees (LEPCs), as well as representatives from the principal parties listed above who have jurisdictions or interests within a given region, will be drawn together by DHS officials to form a Regional Defense Unit (RDU). These members have general knowledge of the industry, are aware of the risks that chemical facilities pose, possess credibility and political clout within their communities and have a vested interest in making chemical facilities less attractive targets for terrorists.

Representatives from the chemical industry will also be invited to join the RDU. These individuals have specific expertise, actual information about facilities/operations

¹⁴⁴ *National Strategy For Homeland Security*, 33.

and practicing knowledge of the industry that will be crucial to the success of the proposed policy. In all likelihood, industry representatives will accept the invitation because they have a strong reason to participate. The incentive is to ensure their facilities' and industry's interests are represented, while RDU mandates (sticks) and incentives (carrots), as explained below, are being promulgated. Industry representatives should recognize this opportunity and accept the invitation. However, if they choose not to participate, the consequences of doing so will vary depending on the exact requirements ultimately developed by the RDU. For example, RDU members may decide that non-participants have to carry higher levels of insurance protection, not be eligible for tax breaks, have to pay higher fees, incur increased transaction costs, be inspected more often, have operating permits suspended or revoked, encounter slower government processing, etc.

Industry officials could try to pursue legal action to prevent the RDU's efforts. Although this avenue is a possibility, it is unlikely for two reasons. First, litigation will publicize the sector's overall lax security as documented earlier. This deterrent, coupled with the fact that a catastrophic release at any one of thousands of chemical facilities would threaten large numbers of Americans, makes legal action less palatable for industry. Furthermore, news agencies would probably use the conflict to demonize the chemical sector. As a result, more severe action could be imposed on chemical facilities than what would have been produced had industry officials simply participated. Second, other local, county and state governments have initiated stronger actions (e.g., mandates) than suggested in the new policy, and no legal repercussions have occurred.

Next, every RDU will perform a variety of tasks, such as categorizing regional facilities by risk, conducting appropriate vulnerability assessments, describing minimum-security measures/standards, identifying adequate warning and mitigation systems, developing necessary requirements, etc. In addition, a major portion of the RDU's efforts involves creating and structuring incentives to encourage additional preparedness efforts by facility owners/operators. To illustrate, what mix, if any, should there be regarding tax cuts, credits and abatements? Also, what about government-sponsored insurance, grants, and low interest loans? Can operating permit processes be expedited, costs reduced, number of inspections lowered and so on for compliant facilities? Another key area for

RDU members will be developing necessary preparedness-related mandates. For example, what are the minimum standards and safeguards needed to ensure adequate preparedness? These questions will need to be addressed by each RDU and evaluated from the viewpoint of promoting effective results, not merely causing activities to take place or “boxes to be checked.” Much of this work is likely to be long and tedious, but a properly balanced “carrot and stick” approach will be critical for the ultimate success of the new regional policy.

To keep processes transparent and to reduce the chances that the RDU is co-opted, periodic reports and public presentations must be made to governing bodies within the region. Also, a citizen oversight/accountability committee will be established to ensure efforts stay above board and on target. Another step involves creating an ombudsmen group to support the RDU by conducting research, providing technical assistance, identifying issues of interest, operating a “whistle blower” hotline and so forth. Lastly, a mediation body should be included to help resolve conflicts that may arise and to minimize potential litigation.

In order to fund this policy, a tax or fee can be charged to facilities located in the geographical area of the RDU. The amount charged could be based on the classification of the site. For example, a plant may be charged a specific rate for storing, consuming, transporting or manufacturing certain hazardous chemicals. The amount could be established at a relatively low rate and be continuous, or set somewhat higher and stopped once sufficient operating capital for the new policy is amassed. Structuring costs in this fashion may encourage facilities to reduce their attractiveness as targets (e.g. store less volatile substances on-site, substitute hazardous chemicals with safer ones, reduce high-risk processes, etc.). Establishing a taxing entity within the RDU region represents another alternative. This option could involve setting up a general sales tax district or statewide tax whereby the revenue is used exclusively to secure nearby critical infrastructure such as chemical facilities. The RDU, with approval of DHS, can be responsible for determining how the collected funds are spent. Under this approach all that would be needed is a public referendum.

The suggested policy has several advantages. First, it initiates a comprehensive and cost-effective process for making chemical facilities less attractive as targets of terrorism. To date, this scenario has not occurred, and it appears unlikely, unless a catastrophic event at a plant occurs. Second, the strategy establishes an ongoing structure that facilitates the active participation of key members of the private and public sector towards a common goal. It does this through a mixed approach of mandates (sticks) and incentives (carrots). Currently, no other similar method is available. Third, the new policy focuses on addressing key issues that most observers agree need to be resolved. Many of these problems have existed within the chemical sector for years. Fourth, the proposal is a networked and layered approach to the problem of chemical facility “insecurity.” Because of the multi-disciplinary makeup of the RDU, measures will not be considered in a vacuum but in concert with other dynamics. This holistic view is possible when key members of all parties gather together and strive towards one common mission. With stakeholders working side by side, results should be produced quicker, saving valuable resources. Furthermore, innovation is more likely to occur in this atmosphere. Buy-in and industry adherence with the new jointly developed policies should be higher than with a strictly mandated approach. For example, strong public-private collaboration was used in drafting the FFIEC regulatory handbook, which is broadly recognized by the banking industry for its value.¹⁴⁵ However, the EPA’s Underground Storage Tank (UST) program, which regulates leak detection and prevention in tanks, was developed with little external input. To no surprise, more than 60% of states cannot inspect facilities in adherence with EPA’s UST guidelines due to understaffing.¹⁴⁶ Considering the scarcity of resources for enforcement, regulations that lack sector buy-in are generally less effective.

The suggested policy also establishes permanent structures that will allow for continuous evaluation and improvement, what the Japanese call “kaizen”. It will not dissolve, as government committees or commissions often do, after their initial work is completed. As a result of sustaining the new approach, it can be adapted to meet new

¹⁴⁵ National Infrastructure Advisory Council, *Best Practices For Government To Enhance The Security Of National Critical Infrastructures*, Final Report And Recommendations By The Council, April 13, 2004, 14.

¹⁴⁶ Ibid.

threats. This characteristic is beneficial because as threats constantly emerge and evolve, so must the proposal. Another advantage of the proposal is the design of the self-funding mechanism, requiring appropriate parties to incur the costs. Last, since stakeholders are working more closely together, coordination, cooperation and collaboration should be high. In summary, the suggested policy is likely to produce more cost-effective and comprehensive results than voluntary or mandated alternatives will yield.

Just as there are many advantages to the suggested policy, there are some disadvantages. For example, it does create another layer of “bureaucracy,” and this process could become mired in “turf battles.” In addition, operating costs will likely increase which may have unforeseen rippling effects. The suggested strategy also infringes on the free market enterprise by imposing government intervention. Historically the results have not been efficient or effective when this has happened. Another problem is that developing, implementing and sustaining the new proposal will consume participants’ time, and quite a bit of it. There will be meetings, training, research, reporting, planning and so forth. Obviously, accomplishing this “new” work may cause efforts in other areas to suffer. Finally, suggested incentives could become abused, either by illegal means or through a lobbying process and therefore undermine the suggested policy’s effectiveness.

The proposal’s primary constraint is that while it is well suited for metropolitan areas where high-risk facilities are usually clustered together, it may not be as practical when sites are isolated or geographically dispersed. Also, the approach may run into political difficulties, especially when a region crosses several jurisdictional boundaries (cities, counties or states). This situation could make consensus building more difficult for DHS.

If implemented, the proposal may have several unintended consequences. For example, in lieu of adhering to the new RDU regulations, some chemical facilities may decide to relocate overseas. This option would be more difficult for refineries because of their huge capital investments, but it could be easier for storage and transportation sites. In addition, industry growth within the identified region may be stifled. Plants may not expand and other multinational corporations could decide not to move their companies to

the U.S. because it may be viewed as “unfriendly” to the industry. Also, complying with the new policy could inadvertently bankrupt some already financially struggling facilities. All of these outcomes would have a negative effect. Another unintended consequence is that RDU members or other participants may become too close of allies to the very industry they are supposed to be overseeing. Last, the proposed approach might digress into a highly politicized process, potentially causing all parties to move further apart instead of bringing them closer together.

If the proposal is adopted, clearly the chemical sector will lose some of its freedoms. The industry will no longer have carte blanche over its operations. Certain measures will have to be undertaken and some oversight will be instituted. Also, the suggested funding mechanism, fees, taxes, etc., for the proposal will likely impact corporate earnings. However, industry officials may be able to reduce some of their costs. For example, newly implemented security steps could be marketed by the chemical sector to demonstrate its “consumer consciousness.” Furthermore, the industry can offset its added preparedness costs of compliance by passing on the increases to customers and/or corporate investors (e.g., reduce dividends). Last, some of the sector’s increased expenditures may be partially or totally reduced by available tax credits, grants, insurance reductions, pooling of resources, etc.

Initially, opponents of the chemical industry likely will be viewed as the winners in the adopted policy. But, in reality the collaboratively developed quasi-mandates implemented as a result of the proposal will not be nearly as rigid as federal legislation long suggested by some industry opponents. As mentioned earlier Governor Corzine, a harsh critic of the chemical industry, has long proposed a laundry list of specific regulations for its facilities (e.g., the Chemical Security Act).¹⁴⁷ However, the steps offered under the new approach are more flexible, comprehensive and participatory than the CSA.

If implemented, the public is the big winner of the suggested regional policy because effective steps will finally be taken to reduce the attractiveness of chemical sites as targets of terrorism. As a result, future attacks should be prevented or deterred and the

¹⁴⁷ Corzine, “Agenda,” http://corzine.senate.gov/priorities/chem_sec.html (Accessed May 30, 2005).

consequences of successful strikes will be substantially mitigated. Both outcomes significantly improve homeland security. As a result, all Americans will benefit.

B. POLICY RECOMMENDATIONS

Federal legislation should be enacted that authorizes the Department of Homeland Security to ensure that chemical facilities are adequately prepared against acts of terrorism. To achieve this goal, the new Act needs to assert that DHS forms regional public-private partnerships (e.g., Regional Defense Units). Eventually these collaborative groups will craft, implement and sustain both mandates and incentives to reduce the attractiveness of chemical facilities as targets of terrorism. In essence, much of the required effort of the new proposal will be, and should be, performed by Regional Defense Units, with guidance from DHS. However, before getting to these tasks, RDU members must perform some related groundwork. For example, once the RDUs are formed, they will conduct a variety of tasks such as:

1. Action Steps

- Identifying meaningful security measures
- Crafting third-party inspections/audits procedures
- Determining a tax/fee structure for the handling of certain hazardous materials
- Identifying potential inherently safer technology alternatives
- Establishing drill, training, and “red team” requirements
- Submitting specified reports and appearing before local governing bodies
- Reviewing facilities’ procedures/plans (safety, personnel, equipment, response, mitigation, etc.) to ensure preparedness adequacy
- Establishing levels of insurance for the handling certain hazardous chemicals
- Assessing facility vulnerabilities, based on recognized methodologies, and ensure steps to address weaknesses are implemented
- Calculating realistic off-site consequences to categorize chemical sites based on risks
- Establishing background check and periodic review procedures for employees

- Creating and implementing employee training to thwart “social engineering” attacks
- Determining eligibility for grants, tax credits, and/or fee reductions to encourage facilities to take extra protective measures
- Providing expedited inspections/audits/reviews for facilities that exceed basic security expectations
- Seeking representation on the region’s FBI’s Joint Terrorism Task Force (JTTF) to ensure follow-up on homeland security matters and to improve communication
- Developing and offering training for RDU members and facility personnel to improve preparedness
- Leading an effort to establish a meaningful ongoing partnership between the private and public sectors
- Collaborating and networking with neighboring RDUs to share lessons learned, best practices, intelligence, etc.

It should be noted that the list above is not exhaustive nor are the tasks provided in order of importance. Once these and other action steps are complete, RDUs will craft and institute regional “carrot and stick” measures to ensure chemical facility owners/operators undertake adequate steps to improve their preparedness.

The new approach can produce several positive outcomes. First, chemical facilities will become harder for terrorists to penetrate. The proposal should also deter attacks since suggested measures will significantly raise the odds that terrorists will not gain access. Second, RDU efforts are likely to reduce the high consequences commonly associated with an attack on the chemical sector. For example, some of the action steps specifically encourage chemical facility operators to store fewer quantities of hazardous materials on-site, use safer technology, improve response and mitigation efforts and shift towards substituting less lethal chemicals. Third, the new policy should pre-empt attacks at chemical facilities by improving terrorism recognition capabilities of law enforcement, chemical facility personnel and the general public. Finally, the suggested approach

encourages industry innovation through incentives to reduce the attractiveness of chemical facilities as targets for terrorists. All of these measures can strengthen the preparedness of the chemical industry.

C. SUMMARY

According to recent government reports, chemical facilities present desirable targets for terrorists.¹⁴⁸ Their attractiveness is due to several factors. First, a catastrophic release of a toxic substance at a key facility could endanger the lives of millions of Americans. Second, in spite of the dangers of such an event, many sites are not adequately prepared. Third, terrorists could strike the chemical sector to send crippling reverberations through the economy or for symbolic purposes. For these reasons, chemical plants are prime terrorist targets. In fact, the seriousness of the chemical facility preparedness was recently highlighted by the former Deputy Homeland Security Advisor, Richard Falkenrath. In July of 2005, he stated before the Committee on Homeland Security and Governmental Affairs:

Of all the various remaining civilian vulnerabilities in America today, one stands alone as uniquely deadly, pervasive, and susceptible to terrorist attack: toxic-inhalation hazard (TIH) industrial chemicals, such as chlorine, ammonia, phosgene, methylbromide, hydrochloric acid and other various acids. The IDLS (immediately dangerous to life standard) for two of the most common industrial TIH chemicals, ammonia and chlorine, is 500 and 10 parts per million, respectively. These are extraordinarily dangerous substances: they are identical to those used as weapons on the Western Front during the First World War.¹⁴⁹

To prevent terrorist attacks and to mitigate the consequences of successful attacks on the chemical industry, efforts need to focus on reducing the attractiveness of its facilities as targets. Achieving this monumental goal requires a comprehensive, cost-effective, and collaborative approach. It also necessitates DHS to demonstrate real leadership and for stakeholders to be actively engaged in preparedness efforts. Consequently, a new proposal should be developed, implemented and sustained by regional public-private partnerships. Through joint efforts (e.g., regional governance) and

¹⁴⁸ Stephenson, "Voluntary Initiatives Are Under Way", 3.

¹⁴⁹ Richard A Falkenrath, *Chemical Facility Security: What Is The Appropriate Federal Role?* Statement before the Committee on Homeland Security and Governmental Affairs, April 27, 2005, 9.

by using a mixture of incentives and government mandates, chemical facilities can become better prepared for attacks. These requirements are all pillars of the proposed approach.

LIST OF REFERENCES

- Ackerman, Gary, and Cheryl Loeb. "Watch Out For America's Own Extremists." *Christian Science Monitor* (October 19, 2001):13-15.
<http://www.csmonitor.com/2001/1019/p11s3-coop.html> [Accessed May 29, 2006].
- American Chemistry Council. *ACC Supports Federal Chemical Security Legislation* (October 2004).
http://www.americanchemistry.com/s_acc/sec_policyissues.asp?CID=329&DID=1156 [Accessed May 27, 2006].
- _____. *Protecting a Nation: Homeland Defense and the Business of Chemistry* (April 2002).
http://americanchemistry.com/s_acc/sec_article.asp?CID=26&DID=1218 [Accessed July 22, 2005].
- Auerswald, Philip, Lewis M. Branscomb, Todd M. La Porte, and Erwann Michel-Kerjan. "The Challenge of Protecting Critical Infrastructure, Issues in Science and Technology Online." *Journal of Technology Transfer* 28, no. 2 and 3 (August 2003): 227-239.
- Behrens, Carl, and Mark Holt. "CRS Report for Congress." *Nuclear Power Plants: Vulnerability to Terrorist Attack*. Washington, D.C.: The Library of Congress, August 9, 2005.
- Bennett, Elizabeth A., Peter Grohmann, and Brad Gentry. "Public-Private Partnerships for the Urban Environment: Options and Issues." PPPUE & Yale University, 1999.
- Brashear, Jerry P. "The Necessity of Regional Public/Private Partnerships for Effective Critical Infrastructure Protection." *The CIP Report* 4, no. 3 (September 2005).
- Bryson, John M. *Strategic Planning For Public And Nonprofit Organizations*. San Francisco: Jossey-Bass Publishing, 2004.
- Chace, Richard. *Tax Incentives for Homeland Security Related Expenses* (H.R. 3562). Washington, D.C.: U.S. House of Representatives, December 15, 2005.

- <http://wwwc.house.gov/smbiz/hearings/databaseDrivenHearingsSystem/displayTestimony.asp?hearingIdDateFormat=040721&testimonyId=223> [Accessed April 12, 2006].
- Chertoff, Michael. Remarks by Secretary Michael Chertoff U.S. Department of Homeland Security at the Commonwealth Club.
<http://www.dhs.gov/dhspublic/display?content=4700> [Accessed April 10, 2006].
- Cilluffo, Frank J. *Preventing Terrorist Attacks on America's Chemical Plants*. Washington, D.C.: U.S. House of Representatives, June 15, 2005.
http://www.gwu.edu/~dhs/congress/june15_05.htm [Accessed April 5, 2006].
- Collins, Susan M. "Chemical Facility Security: What Is The Appropriate Federal Role?." Washington, D.C.: Senate Committee on Homeland Security and Governmental Affairs, July 27, 2005. <http://hsgac.senate.gov/files/072705SMCopen.pdf> [Accessed June 14, 2006].
- Corzine, Jon S. "Agenda: Fact Sheet on Senator Corzine's Chemical Security Legislation." http://corzine.senate.gov/priorities/chem_sec.html. [Accessed May 31, 2005].
- Davis, Steven. *NFPA 1600*. DavisLogic.Com, 2004.
<http://www.davislogic.com/NFPA1600.htm> [Accessed April 30, 2006].
- Durbin, Martin. "Chemical Facility Security: What Is The Appropriate Federal Role?" Testimony before the Committee on Homeland Security and Governmental Affairs, Washington, D.C.: Government Printing Office, 2005.
- Falkenrath, Richard A. "Chemical Facility Security: What Is The Appropriate Federal Role?" Statement before the Committee on Homeland Security and Governmental Affairs. April 27, 2005.
- Farmer, Richard D. "Homeland Security and the Private Sector." CBO Paper for Congress. Washington, D.C.: The Library of Congress, December, 2004.
- Flynn, Stephen E. *America the Vulnerable*. New York: HarperCollins Publishers, 2004.
- _____. and Jeane Kirkpatrick. *Ending the Post 9/11 Security Neglect of America's Chemical Facilities*, Council on Foreign Relations, April 27, 2005.

- <http://www.iwar.org.uk/homesec/resources/chemical-security/FlynnHSGAtestimony42705final.pdf> [Accessed April 13, 2006].
- Goode, Darren G. "Chertoff wants flexibility in managing chemical plant safety." *GovExec.com: Daily Briefing*, March 2, 2006. <http://www.govexec.com/dailyfed/0306/032106cdpml.htm> [Accessed March 21, 2006].
- Gupta, J. P. "The Bhopal Gas Tragedy: Could it have happened in a developed country?" *Journal of Loss Prevention in the Process Industries*, V.15, Issue 1, (January 2002): 1-4. <http://webdrive.service.emory.edu/users/vdhara/www.BhopalPublications/Environmental%20science/Bhopal%20tragedy-could%20it%20have%20happened%20in%20a%20developed%20country.pdf> [Accessed May 27, 2006].
- Kim, W. C., and Renee Mauborgne. *Blue Ocean Strategy*. Boston: Harvard Business School Press, 2005.
- Knieser, Thomas. *Cato Handbook for the 105th Congress*. Washington, D.C.: The Cato Publishing Institute, 1996.
- Kouri, Jim E. "Preventing Terrorist Attacks at Chemical Facilities." *Men's Daily News Home Page*, May 6, 2005. <http://mensdaily.com/blog/kouri/2005/05/preventing-terrorist-attacks-at.html> [Accessed May 31, 2005].
- Kuepper, Gunnar. *The NFPA 1600 Standard on Emergency/Disaster Management: New Edition Expected in 2004*, IAEM Bulletin (July 2003). http://www.emergency-management.net/pdf/iaem/IAEM_July_Bulletin.pdf [Accessed June 15, 2006].
- Levy, Julian A. "Baltimore Officials Applaud Hazardous Materials Safety Law." MDCITA Press Release, July 19, 2005. <http://www.acusafe.com/newsletter/stories/citapressrelease102802.doc> [Accessed January 20, 2006].
- Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Monterey, CA: Naval Postgraduate School, 2004.

- Mitnick, Kevin D. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing, 2002.
- McGlooin, Kate B. *ACC Sees Maryland Chemical Security Bill as Step in the Right Direction*, ACC Press Release, August 14, 2004. <http://www.accnewsmedia.com> [Accessed November 20, 2005].
- Morgan, Peter. *Capacity Development and Public Private Partnerships*. <http://www.gdrc.org/uem/undp-capacity.html> [Accessed April 12, 2006].
- Moteff, John D. "Critical Infrastructures: Background, Policy, and Implementation." *CRS Report for Congress*. Washington D.C.: Library of Congress, April 18, 2006.
- National Infrastructure Advisory Council. *Final Report and Recommendations By The Council. Best Practices For Government To Enhance The Security Of National Critical Infrastructures*. April 13, 2004.
- O'Hanlon, Michael E. *Protecting the American Homeland: A Preliminary Analysis*. Washington, D.C.: Brookings Institute Press, 2002.
- Orszag, Peter, R. *Tax Incentives for Homeland Security Related Expenses* (H.R. 3562). Washington, D.C.: U.S. House of Representatives, December 15, 2005. <http://www.house.gov/smbiz/hearings/databasedrivenhearingsystems/displaytestimony> [Accessed February 12, 2006].
- _____. *Statement before the National Commission on the Terrorist Attacks Upon the United States*, Washington, D.C: Government Printing Office, November 19, 2003.
- Orum, Paul. *Terrorism and Chemical Plant Security – Testimony and Response*. Washington, D.C.: Environmental Health Watch, November 14, 2001. http://www.ehw.org/Chemical_Accidents/CHEM_OrumTestimony_2001.htm [Accessed May 31, 2005].
- Pandanell, Mark E. *The Texas City Disaster: April 16, 1947*. <http://www.local1259iaff.org/disaster.html> [Accessed June 17, 2005].
- Prine, Carl C. "Chemical sites still vulnerable." *Pittsburgh Tribune-Review*, November 16, 2003.

Rudge, David F. *Ben-Elizer Warns of Bombing Wave*.

<http://www.synapsenow.com/synapse/news/fullstory.cfm?articleid=4576&website=israelfacts.org> [Accessed April 5, 2006].

Schierow, Linda-Jo D. "Chemical Plant Security." *CRS Report for Congress*.

Washington, D.C.: The Library of Congress, February 14, 2005.

Shea, Dana A. "Chemical Facility Security: A Comparison of S. 157 and S. 994." *CRS Report for Congress*. Washington, D.C.: The Library of Congress, August 16, 2005.

_____. "Legislative Approaches to Chemical Facility Security." *CRS Report for Congress*. Washington, D.C.: The Library of Congress, August 16, 2005.

Stephenson, John B. "Federal Action Needed to Address Security Challenges at Chemical Facilities." *GAO Report to Congress*. Washington, D.C.: The Library of Congress, February 23, 2004.

_____. "Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action Is Needed." *GAO Report to Congress*. Washington, D.C.: The Library of Congress, April 27, 2005.

_____. "DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed." *GAO Report to Congress*. Washington, D.C.: The Library of Congress, January 2006.

_____. "Voluntary Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Actions Is Needed." *GAO Report to Congress*. Washington, D.C.: The Library of Congress, April 27, 2005.

_____. "Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown." *GAO Report to Congress*. Washington, D.C.: The Library of Congress, March 2003.

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. New York: W.W. Norton & Company, 2004.

- U.S. Congress. *H.R. 3562, To amend the Internal Revenue Code of 1986 to allow businesses a credit for security devices, assessments, and other security related expenses*. 108th Congress 1st Session, November 20, 2003.
- U.S. Department of Homeland Security. *Critical Infrastructure Identification, Prioritization, and Protection: HSPD-7*. Washington, D.C.: Department of Homeland Security, December 2003.
- _____. *DHS Organization*. Washington, D.C.: Department of Homeland Security http://www.dhs.gov/dhspublic/interapp/editorial_0413.xml [Accessed April 20, 2006].
- _____. *National Infrastructure Protection Plan*. Washington, D.C.: Department of Homeland Security, January 2006.
- _____. *National Strategy for Homeland Security*. Washington, D.C.: Government Printing Office, 2002.
- _____. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, D.C.: Department of Homeland Security, February 2003.
- U.S. Department of Transportation. *U.S. International Trade and Freight Transportation Trends*. Washington, D.C.: Government Printing Office, 2003.
- The White House. *Protecting America's Critical Infrastructure: PPD-63*. Washington, D.C.: Government Printing Office, July 2002. <http://www.fas.org/irp/offdocs/pdd-63.htm> [Accessed June 18, 2006].
- Wilkins, Barry. "C-TPAT On A Roll." *Cargo Security International*, December 2005. http://www.cargosecurity.com/ncsc_dotnet/press/C-TPAT_SpecialPressRelease.pdf [Accessed June 17, 2006].

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Ted Lewis, Academic Associate
Center for Homeland Defense and Security
Naval Postgraduate School
Monterey, California
4. Paul Stockton, Director
Center for Homeland Defense and Security
Naval Postgraduate School
Monterey, California
5. Gary Ackerman, Director of Research
National Consortium for the Study of Terrorism and the Response to Terrorism
College Park, Maryland
6. Nancy Wong
Infrastructure Protection
Department of Homeland Security
Washington District of Columbia
7. Mike Massey, Chief of Police
Pasadena Police Department
Pasadena, Texas