NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PUBLIC-PRIVATE-DEFENSE PARTNERING IN CRITICAL INFRASTRUCTURE PROTECTION

by

Gregory M. Jaksec

March 2006

Thesis Advisor:	Ted Lewis
Second Reader:	Rudy Darken

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** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Public-Private-Defense Partnering In Critical Infrastructure Protection			**5. FUNDING NUMBERS**
6. AUTHOR Lieutenant Colonel Gregory M. Jaksec			
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

The problem confronting The Department of Homeland Security (DHS), the Department of Defense (DoD), and America's private sector is how to collectively protect the nation's critical infrastructure. The challenge for the DHS is in motivating partnerships across the public, private, and DoD domains, each with different organizational and cultural objectives governed under a federalist system. The relevance of this problem lies in the vulnerability of America's economic and military foundations to terrorist attacks or a catastrophic natural disaster. Research conducted of the regulated energy and water industries indicates federal standards can be effectively established across the public-private domains. The establishment of federal tax and insurance incentives, limiting corporate liability, and developing industry standards may motivate increased security and circumvent excessive federal mandates.

The conduct of partnering is scrutinized via personal interviews to determine if the recommendation to build security partnerships with federal guidance is sufficient to secure critical infrastructure. The implementation of a dual-purpose strategy is recommended to further enhance the efficiency of security partnerships. This thesis suggests the DHS must develop an innovative CIP policy and utilize the National Infrastructure Protection Plan (NIPP) as the vehicle to integrate and synchronize the actions of all security partners.

14. SUBJECT TERMS Critical Infrastructure, Cross Domain Partnership, Defense (Industrial Base), Department of Defense, Department of Homeland Security, Dual Purpose Strategy, Federal Mandate, Homeland Security Presidential Directive-7, Incentives (Tax), Insurance, Interdependency, Public-Private Partnership, National Infrastructure Protection Plan (NIPP), Regionalization, Security (Partnership), Security (Standards)			**15. NUMBER OF PAGES** 61
			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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PUBLIC-PRIVATE-DEFENSE PARTNERING IN CRITICAL INFRASTRUCTURE PROTECTION

Gregory M. Jaksec
Lieutenant Colonel, United States Army
B.A., Robert Morris College, 1989

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
March 2006

Author: Gregory M. Jaksec

Approved by: Ted Lewis
Thesis Advisor

Rudy Darken
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The problem confronting The Department of Homeland Security (DHS), the Department of Defense (DoD), and America's private sector is how to collectively protect the nation's critical infrastructure. The challenge for the DHS is in motivating partnerships across the public, private, and DoD domains, each with different organizational and cultural objectives that are governed under a federalist system. The relevance of this problem lies in the vulnerability of America's economic and military foundations to terrorist attacks or a catastrophic natural disaster. Research conducted of the regulated energy and water industries indicates federal standards can be effectively established across the public-private domains. The establishment of federal tax and insurance incentives, limiting corporate liability, and developing industry standards may motivate increased security and circumvent excessive federal mandates.

The conduct of public-private partnering is scrutinized via personal interviews with industry and DoD representatives to determine if the recommendation to build security partnerships with federal guidance is sufficient to secure critical infrastructure. The implementation of a dual-purpose strategy is recommended to further enhance the efficiency of security partnerships.

This thesis suggests the DHS must develop an innovative CIP policy and utilize the National Infrastructure Protection Plan (NIPP) as the vehicle to integrate and synchronize the actions of all security partners. Research conducted on the influence of tax incentives and insurance indicates that offering financially-based incentive packages is the most efficient and expeditious means to promote cross domain partnering.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

If an award could be presented to an individual, or individuals, who applied the preponderance of effort toward the completion of this thesis, then my wife Cindy, son Greg, and daughter Rachel, would be gold medalists. Their endless patience and support throughout this entire academic excursion represented my center of gravity.

As I wandered the halls during each in-residence phase, I always made the effort to invoke some form of banter with the likes of Dr. Paul Stockton, Dr. Chris Bellavita, or Dr. Ted Lewis in anticipation that the most diminutive piece of their knowledge would spill over on to my intellect…it's a technique. After all, they individually commanded enough knowledge for several people and probably would not miss a little intellect. Their mission to educate the unknowing was accomplished.

The opportunity to serve and learn side-by-side with the domestic warriors who firmly established cohorts 0403 and 0404 in Naval Postgraduate School history was an education in and of itself. What I learned from the breadth of knowledge, personality, and friendship that formed our composite team for that year and a half could fill a laptop.

And, finally, I owe a tremendous debt of gratitude to Colonel (Ret.) Joel Hooks, Colonel Steve Hatter, and Colonel Kristine Clifton of Joint Task Force-Alaska for the opportunity to attend the Naval Postgraduate School and permit me to depart every three months to enjoy this privilege called the Center for Homeland Defense and Security.

THIS PAGE INTENTIONALLY LEFT BLANK

I. OVERVIEW

A. INTRODUCTION

The events of September 11, 2001, made clear that our adversaries aim to destroy our economic agility and weaken our capability to extend national power from domestic DoD facilities to objectives across the globe. How much federal exertion is necessary to protect critical infrastructure? The President of the United States explicitly charged the Secretary of Homeland Security with securing the nation's critical infrastructure and key assets in the subsequent federal legislation that followed 9/11. The significant challenge in this endeavor has been to reach a productive level of cooperation that is amenable to both public and private entities.

The fact that approximately eighty-five percent of the nation's critical infrastructure is owned and operated by private enterprise is documented and is the basis of this dilemma.[1] The DoD is tasked to secure the Defense Industrial Base (DIB) that provides the military establishment with federally owned and contracted services that produce weapon systems, munitions, and research and development. How can the DoD ensure the security of the DIB when the overwhelming majority of the industrial utilities providing power, energy, telecommunications and water to military facilities are privately owned?

B. DEFINING THE PROBLEM

The author argues that the macro-challenge facing the Department of Homeland Security (DHS) is how to assimilate three distinct critical infrastructure (CI) domains collectively owned by the federal government and the private sector under a unified CIP policy. Embracing public-private partnerships (P3) for the enhancement of security represents only two-thirds of the three CIP domains. The other third, DoD, and for that matter the nation in general, has a vested interest in ensuring CI is functional to preserve national security and also provide a stable environment for the DIB to function.

[1] 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), 8.

The strategic guidance established in the *National Security Strategy* and the *Strategy for Homeland Security* emphasizes the importance of partnering and promoting the benefits of information exchange between all levels of government and most importantly the private sector. However, federal regulations such as the *Strategy for Homeland Defense and Civil Support,*[2] *The National Strategy For The Physical Protection of Critical Infrastructure And Key Assets,*[3] and specifically, *Homeland Security Presidential Directive – 7* (HSPD-7),[4] lack the mandate to ensure that civil-military relations transcend periodic information sharing and promote genuine collaboration that strives to reach common objectives.

Federal directives do not offer the engagement strategy for how federal agencies can guide the private sector in a consolidated effort to improve the DoD's critical infrastructure interdependencies. Federal incentive could be the catalyst that energizes meaningful private sector engagement. Unfortunately, little incentive for critical infrastructure partnering exists at this time. The leadership at the local, state, federal, and private levels each has different and sometimes conflicting interpretations of how their respective organizations can reach their objectives.

Current DHS policy lacks clarity in the division of labor between federal agencies and the private sector and has failed to unify the CI effort. The question of whether or not critical infrastructure protection (CIP) strategy should be defined in terms of sectors or regions creates considerable and legitimate debate. Domestic security is dependent on our ability to maintain economic continuity and ensure our ability to assure strategic and domestic military objectives remain readily available. Common ground is not easily identifiable in this debate.

How do we secure the DoD's critical infrastructure when the forces of free enterprise stand between private business and federal regulation? The DoD's ability to posture forces and maintain readiness remains largely dependent on commercial utilities

---

2 U.S. Department of Homeland Security, The National Strategy For The Homeland Defense and Civil Support (Washington D.C: Government Printing Office, March 2005).

3 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).

4 U.S. Department of Homeland Security, Critical Infrastructure Identification, Prioritization, and Protection: HSPD-7 (Washington D.C: Government Printing Office, December 2003).

and the industrial support provided by private enterprise. The strategic agility of our military is dependent on the DIB, a conglomerate of mutually dependant military and civilian industrial facilities, programs, and services.

1. The Relevance of This Problem

The absence of federal guidance that presents a detailed public-private-DoD engagement plan increases the vulnerability of the nation's CI to terrorist attacks and natural disasters. The failure of the DHS to promote a comprehensive approach to securing defense, public, and private critical infrastructure can result in decentralized partnering efforts that are not nationally synchronized. The emphasis on s*ector specific* analysis in the 'draft" NIPP neglects the assessment of cross-domain interdependencies by not implementing a regional perspective. Information-sharing constraints between the public, private, and DoD domains are preventing collaboration that promotes meaningful partnerships.

2. Thesis

The nation's critical infrastructure (CI) policy remains deficient four years after the attacks of September 11, 2001. The primary reason for this is a deficiency in partnering among public, private, and DoD organizations. The author argues that the gap between the federal government and private enterprise is the primary hindrance to genuine partnering. Public, private, and DoD organizations need to:

- Promote cross-domain partnering for CIP;
- Consider federal regulation of CI security standards to ensure the interdependencies between the federal government and the private sector that facilitate national security and economic production remain secure;
- Perform regional analysis in accordance with the "draft" *National Infrastructure Protection Plan*;
- Consider tax incentives as fiscal motivation for corporate America to invest in security and common standards.

3. Literature Review

The preponderance of federal guidance dedicated to enhancing the security of defense programs and infrastructure explicitly details the roles and responsibilities of federal agencies and the programmatic criteria necessary to support and defend the

defense-industrial base. The *National Infrastructure Protection Plan*, *Homeland Security Presidential Directive-7*, *National Strategy for the Protection of Critical Infrastructure and Key Assets*, and *Strategy for Homeland Security* clearly frame the importance of protecting national infrastructure, but neglect the sensitivity of federal agencies engaging private interests. The Congressional Research Service and the Government Accounting Office have produced several studies that describe the federal grants and programs, background of critical infrastructure policy, and public-private partnering. Unfortunately, only a modest amount of research exists that provides analytical recommendations for pursuing federal incentive as a vehicle to induce public-private engagement.

4. Methodology

This thesis will address the ambiguous nature of cross-domain partnerships by identifying the barriers that complicate collaboration and information sharing and propose innovative incentive-based alternatives. Understanding the effectiveness of federal incentive programs designed to secure lines of communications between DHS, DoD, and the private sector is the core objective of this research. The effect of introducing a federal incentive, used as a tool to energize the private sector's desire to collaborate with federal agencies, is analyzed by assessing the following three factors:

- Information gained via email correspondence and personal and telephone interviews regarding the effectiveness of partnering;
- Organization and policy barriers specific to both public and private sectors that impede collaborative energy;
- The federal guidance and DoD regulations that either promote or constrain the development of cross-domain partnerships.
- In this thesis the author evaluates the following strategies:
- Terrorism insurance and limited corporate liability;
- Tax incentives;
- Security standards;

II. PARTNERING

> Innovative partnerships like those being developed in the IPP [Innovative Partnership Program] can have consequences far beyond the research laboratory and the commercial marketplace. They can form the basis of a space economy that can be the engine for carrying humanity out into the solar system and returning benefits to people back here on earth.[5]

A. DEFINING PARTNERING

The concept of "partnering," in itself, is not complicated in terms of promoting unity of effort in securing critical infrastructure. Partnering entails two or more entities collaborating to accomplish a common goal. The conduct of public-private partnering, however, requires an understanding of the mechanisms that drive community relations, comparative advantage, government contracting, free enterprise, and one's own proprietary limitations. These are just a few of the intricacies that homeland security faces in the effort to secure critical infrastructure.

The issues identified in Table 1 reflect the core constraints that inhibit partnering efforts across not only the broad spectrum of public and private industry but the contribution of the DoD as a integral security partner. According to Ms. Nancy Wong, DHS, "The kind of public-private partnering we are talking about represents a major cultural change for all stakeholders. The difference in language, ways of operating, expected mission results, and adaptability between government and private industry are wide, yet largely unrecognized."[6]

The corporate and federal sectors both indicate that engaging public-private partnerships is worth the investment from the organizational perspective. The partnering initiative is firmly imbedded in the business processes that link the DIB with local, state, federal, and private agencies and enable the military to support the objectives of our national strategy. The United States Army Material Command (AMC) publishes the *Partnerships for Success* guide that not only defines partnering, but also clearly explains

[5] Dr. Frank Schowengerdt, Space Exploration: The Role of the Innovative Partnership Program, available at http://ipp.nasa.gov/innovation/innovation115/4-coverstory.html (Accessed on February 10, 2006.)

[6] Email correspondence with Nancy Wong.

the legality, construct, and the process for the conduct of partnering "to enhance government-industry communication, teamwork and conflict."[7] The AMC's emphasis on government-industry partnering serves as an enabler to circumvent a contract dispute before the dispute impedes the contractual process. Since 9/11 the surge of commercial consultants offering products and services to the public has proliferated.

Any agency, public or private, can obtain consultant advice via web instruction, in-person, through seminars or how-to handbooks. The National Council of Public-Private Partnerships (NIPPP), a non-profit corporation located in the District of Columbia, offers a more stringent approach to partnering by abiding by structured by-laws that formally define conduct and admission to the NIPPP.[8] The NIPPP defines partnerships as the following:

> A Public-Private Partnership is a contractual agreement between a public agency (federal, state or local) and a private sector entity. Through this agreement, the skills and assets of each sector (public and private) are shared in delivering a service or facility for the use of the general public. In addition to the sharing of resources, each party shares in the risks and rewards potential in the delivery of the service and/or facility.[9]

The significance of the NIPPP approach is the establishment of formal by-laws and an organizational structure that enables its board of directors to enforce standards. The NIPPP has projected itself as a critical advocate of partnering by establishing a structured organization with criteria for admission and membership expectations. One could easily assume that collaborative ventures based on contract or mandate would far exceed the expectations of volunteerism. Unfortunately, the notion of a membership bound by contract becomes significantly more complicated when attempting to join the engines of free market and nuances of defense critical infrastructure. Table 1 summarizes the constraints inhibiting cross-domain partnering.

Summary of Constraints to Cross Domain Partnering

[7] Kenneth Bousquet and Mark Sagan, Partnering For Success: A Blueprint For Promoting Government Industry Communication and Teamwork Available at http:://www.amc.army.mil/amc/command_counsel (Accessed on November 15, 2005.)

[8] Creating Effective Public-Private Partnering for Buildings and Infrastructure in Today's Economic Environment, available at http://wwwncppp.org/resources/papers/hdrp3whitepaper.pdf (Accessed on December 1, 2005.)

[9] Ibid.

Issue	Agency	Impact
Lack of federal and state incentives	DHS, state	The private sector has little or no financial justification to participate in CIP partnering initiatives.
Federal mandates and/or regulation do not standardize majority of private sector security criteria	Private sector	The majority of the private sector is not legally bound by statutory regulation to adhere to federal standards for securing infrastructure
Interdependencies between private industry and DoD installations	DoD, Private sector, local, state, and federal	DoD, private industry, and local municipalities are bound by services established by historical infrastructure. However, federal regulations do not mandate private security or free market initiatives
"Draft" NIPP is "sector" focused	DoD, Private sector, local, state, and federal	Projected comprehensive federal guidance will not include regional perspective on CIP analysis
"Draft NIPP does not highlight DoD CIP	DoD	Private Sector does not recognize DoD as a potential or beneficial security partner

Table 1. Summary of Partnering Constraints

B. INTERDEPENDENCIES DICTATE PARTNERING

In terms of geographic cohabitation, civilian and military relationships are created by the indiscriminate sharing of utilities and industrial systems whose functionality is dependant on one another's similar or dissimilar product. Military facilities (posts, bases, stations, depots, etc.) commonly build supportive relationships with the civilian populace adjacent to or surrounding the installation. The DoD presence is a catalyst for economic stimulation through employment and expenditure and additionally provides a means to support the local population in times of emergency.

The interdependencies established within a given communities infrastructure exemplify the essence of partnering. Yet the organizational and cultural differences that

separate private-enterprise and federal agencies often inhibit the collaboration that is as equally important as private-private partnering with the business community.

DoD installations are generally a microcosm of their civilian municipalities and provide varying degrees of federally produced or managed services. However, the DoD still requires vital utilities and industrial support from the private agencies that operate beyond the boundary of government property. The same interdependencies that exist within the sector specific agencies (SSA) reflect the relationships between local corporate enterprise and DoD facilities.

The Homeland Security Presidential Directive/HSPD-7 establishes "The Department and the Sector Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanism."[10] Interdependencies demand information sharing and collaboration between civilian and military coordinators, planners, and most importantly leadership to ensure the uninterrupted continuity of resources critical infrastructure provides. The urgency of the civil-military relationship is more pronounced when the nation's strategic military readiness posture is jeopardized by either terrorism or natural disaster. The premise of degraded critical infrastructure by any avenue of disaster undoubtedly invokes federal concern.

C. DOES THE DEPARTMENT OF DEFENSE HAVE AN ENGAGEMENT STRATEGY FOR THE PRIVATE SECTOR?

The DoD assuredly has an engagement strategy for protecting federally owned critical infrastructure within the parameters of federal law enforcement and pertaining to DoD assets. However, several stipulations prohibit the development of security partnerships with the private sector. The interdependencies that entwine private industry with local and regional military installations should serve as justification to promote incentives for cross-domain partnering. This section will briefly review the federal guidance that defines the Defense Critical Infrastructure Program and DoD partnering.

[10] U.S. Department of Homeland Security, Critical Infrastructure Identification, Prioritization, and Protection: HSPD-7 (December 2003).

The essence of Department of Defense Directive (DoDD) 3020.40, more commonly referred to as the Defense Critical infrastructure Program (DCIP), is the clear delineation of the roles and responsibilities for federal agencies in the conduct protecting critical infrastructure.[11] The DoD strategic vision is stated in The Department of Defense Critical Infrastructure Protection Strategy:

> The DoD CIP vision (stated in the present tense) is to assure that the critical infrastructure assets on which DoD depends are always available to mobilize, deploy, command and control, and sustain military operations. Operators have a real-time situational awareness of critical infrastructure assets. Modeling and simulation reliably depicts the unfolding operational environment sufficiently well that accurate predictions of the operational environment occur in sufficient time to permit military operations, in anticipation of adversary action and/or adverse infrastructure events.[12]

Vulnerability assessments for military facilities, and the more comprehensive defense industrial base, are conducted throughout the DoD via mostly regulated processes based on known standards. The most important aspect of DoD critical infrastructure may be the fact that commanders of DoD installations are responsible for the control and security of all DoD critical infrastructures within their area of responsibility. DoDD 2000.12 states:

> Ensure AT (anti-terrorism) policies & programs include specific prescriptive standards to address specific terrorist threat capabilities & geographic settings, particularly regarding infrastructure critical to mission accomplishment and other DoD-owned, leased, or managed mission.[13]

DoDD 2000.12 and other federal directives do not offer an engagement strategy for how federal agencies can collaborate with the private sector and consolidate the effort to improve the DoD's critical infrastructure interdependencies. This shortcoming in federal critical infrastructure policy is a major theme in the endeavor to understand the reality of cross-sector interdependencies in both the private and federal industrial architectures. Ultimately, the federal government's endeavor to secure the critical

---

[11] U.S. Department of Defense, Department of Defense Directive 3020.40 (Washington, D.C.: Defense Critical Infrastructure Program (DCIP), August 19).

[12] Assistant Secretary of Defense, U.S. Department of Defense, Department of Defense Critical Infrastructure Protection Strategy (April 2003), 1

[13] U.S. Department of Defense. *Directive, 2000.12* (August 18, 2003).

infrastructure that enables domestic and strategic military response is fractured by the proprietary needs of free enterprise and its own administration.

The DoD's ability to secure federally owned critical infrastructure is somewhat straightforward in comparison to how the private sector secures its business assets. By law, the President can deploy federal troops under his Title 10 authority in response to intelligence indications or in response to a terrorist action or natural disaster.[14] Governors also have the ability to activate their state militias or national guard at their discretion under Title 32.[15] The DoD holds a vested interest in ensuring non-DoD CI/KR is secure due to private industry's contribution to the DIB.

The development of federal guidance designed to bridge DoD CIP policy with DHS CIP policy has not transpired between the Assistant Secretary of Defense, Homeland Defense (ASD-HD) and DHS. In essence, partnering has to occur at the federal level to ensure complementary CIP policies are designed that promote interaction between the DoD and private industry that is awarded defense contracts

D. REGIONALIZATION

> The country needs a national homeland security system that mobilizes state and local governments and public safety officials as partners in intelligence, emergency response, and domestic counterterrorism. For more effective coordination between these different levels of government, DHS should create regional field offices, as required by the Homeland Security Act of 2002. [16]

The DHS emphasis on sector specific plans in the initial draft versions of the NIPP is a positive step in understanding sector specific vulnerabilities. However, the identification of sector specific vulnerabilities alone does not contribute to the identification of critical nodes that survive on behalf of cross-sector interdependencies. Concentrating federal CIP guidance on primarily sector specific analysis addresses the

---

[14] U.S. Congress, Armed Forces (1956), Title 10 U.S Code, available at http://uscode.house.gov/download/pls/32T.txt, (Accessed on, October 10, 2005.).

[15] Ibid.

[16] James Jay Carafano, Ph.D., Countdown to 9/11: Five Fixes for Homeland Security by the Fifth Anniversary of the Attacks, available at http://heritage.org/Research/HomelandDefense/wm963.cfm. (Accessed on February 10, 2006.)

initial challenge of promoting collaboration within peer industries but fails to promulgate the necessity to collaborate throughout a region. A comprehensive understanding of a specific region's CIP vulnerabilities requires an analysis of the full range of local or regional industry that forms that infrastructure's critical nodes.

Governors have sovereignty with their borders and are best suited to develop regional CI/KR. Governors can in effect regulate their regions. The significance of state sovereignty is important when recommending the implementation of regional CIP partnerships to identify and prioritize CI/KR. The recommendation to identify states as regions for CIP is driven by the fact that once that service or industry transports products or services across the state line the governor's sovereignty begins to erode and cooperative agreements have to be initiated. A state can function as an autonomous region in terms of industry more effectively than a region that is comprised of two or more states.[17]

An article written by Philip E. Auerswald and Lewis M. Branscomb for the *Journal of Technology* discussed financing the transition from technical innovation to invention in the United States and how private investment in research and development matures. Their research identified trends in the geographical location of technological start-ups and funding sources. Most significant was the role state governments play in establishing regional environments that bridge the development of innovation to invention.[18] Their research provided the following insight:

> State governments facilitate university-industry partnerships, leverage federal academic research funds by providing both general and targeted
>
> grants, build a technically educated workforce through support of public colleges and universities, and ease regulatory burdens to create fertile ground for technology startups.[19]

---

17 Telephone interview with Larry Clark, Public Sector Liaison, George Mason University, December 7, 2005.

18 Philip E. Auerswald and Lewis M. Branscomb, "Valleys of Death and Darwinian Seas: Financing the Invention to Innovation Transition in the United States," Journal of Technology Transfer (August 2003), 227.

19 Philip E. Auerswald and Lewis M. Branscomb, "Valleys of Death and Darwinian Seas: Financing the Invention to Innovation Transition in the United States," Journal of Technology Transfer (August 2003), 227..

Can regional environments within state borders expedite growth more readily than interstate relationships? The Branscomb and Auerswald research indicates public-private partnering could be more readily fostered within state boundaries, based on the community relationships, regulatory commonality, and supportive population bases, than through exercising foreign relations with the neighboring state. The consideration by DHS to supplement sector specific analysis with regional awareness in the CI/KR prioritization process offers an added dimension to the NIPP framework. Consider the following insight by COL Mary Frels, J35, United States NORTHERN COMMMAND:

> DHS must look at CI from a state or geographical perspective as well as sector. Governors are responsible in the civilian sector for the CI in their states. Sectors represent functional interests; e.g. transportation, communications, etc. These are often global. But to a governor or to NC [NORTHERN COMMAND], we need to see the functional parts of CIP in relation to our AOR [area of responsibility]. The other problem with sectors is that they are stovepiped functional areas. At some point we need to understand the impact of sectors on each other and the areas they represent.[20]

The perspective of USNORTHCOM CIP planners is valuable because they have no proprietary motivation and assess CI from the national to the local level. In terms of the development of national CIP policy, prioritizing national CI/KR derived from both regional and sector information is beneficial.

E. DUAL PURPOSE STRATEGY

Dr. Ted Lewis, Naval Postgraduate School, frames the dual purpose concept as a security investment that simultaneously improves productivity.[21] Balancing capital investment in CIP and the deliverables of a security partnership may not be readily identified by all stakeholders, whether private, public, or federal. The determination of what qualifies as acceptable risk, vulnerability, or the prioritization of critical nodes can prove to be a difficult venture when the charter of any given partnership is narrowly defined. The composite make-up of a cross domain partnership may indicate the amount of investment the partnership is able to recommend or the breadth of the CIP programs

[20] Email correspondence: Colonel Mary Frels, U.S. NORTHERN COMMAND.

[21] Dr. Ted G. Lewis, "Critical Infrastructure Protection in Homeland Security: Defending A Networked Nation," (Monterey, CA: Naval Postgraduate School, 2004), 27.

the partnership can even consider. Therefore, a security partnership that restricts its own vision and membership diversity can therefore limit its full potential by inadvertently restricting its investment recommendations.

The question Dr. Lewis asks is, "can an investment in security serve a dual purpose of also improving productivity?"[22] Through securing the critical nodes of any given sector and decreasing the anomalies that drive higher costs, can a cost benefit be derived through lower insurance premiums? The second and third order effects of investing in critical node security can result in network redundancy. Accordingly, network redundancy mitigates risk and improves the efficiencies of that business unit. Thus infrastructure security and sector efficiency are served by a dual purpose strategy.

Apply the same dual purpose concept to partnerships. By expanding the membership of a cross-domain partnership to academia for example, the charter can leverage the benefits of research investment and innovation. NASA's Innovative Partnership Program (IPP) has found success in pursuing its cost-laden vision through leveraging partnerships with universities and private companies. "In order to make those partnerships a reality, tough, potential industrial partners must be convinced that it is in their economic interests to put up their own money to help NASA get back to the Moon and go on to Mars."[23] The term *outreach* is relevant to describing the IPP's vision. The IPP goes as far as proclaiming that the end state of the IPP surpasses a mere partnership and goes as far as establishing a *space economy.*[24]

The Alaska Partnership for Infrastructure Protection (APIP) is a CIP security partnership in our 50th state that applies dual purpose strategies for two distinct applications. The first application is the aggregate assessment and prioritization of CI vulnerabilities by Alaska's public, private, and DoD domains. The partnership moves beyond public-private partnering and leverages Alaska's DoD community as a formidable emergency response resource in the event of an incident of national

---

22 Dr. Ted G. Lewis, "Critical Infrastructure Protection in Homeland Security: Defending A Networked Nation," (Monterey, CA: Naval Postgraduate School, 2004), 27.

23 Dr. Frank Schowengerdt, Space Exploration: The Role of the Innovative Partnership Program, available at http://ipp.nasa.gov/innovation/innovation115/4-coverstory.html. (Accessed on February 10, 2006.)

24 Ibid.

significance. The APIP has effectively bridged the cultural and organizational gap that can obscure the vital relationships of the interdependencies that exist between private and federal infrastructures.

The second application of the APIP's dual purpose strategy is encompassed in Alaska's interagency information management process. The APIP is a contributing member of the Alaskan civil-military agencies that facilitate interagency decision-making. The Anti-Terrorism Advisory Council Alaska (ATACA) serves as an information conduit that contributes intelligence analysis to the decision-making entities such as the Joint Coordination Group (JCG) and the Executive Committee (ExCOM) in the event of terrorist incidents or natural disasters.[25]

The APIP serves as a prime information engine that directly contributes to local and statewide situational awareness. As benefactors to the APIP, the Anchorage Emergency Operations Center and the Alaska Joint Control Group can assess the health of Alaska's critical infrastructure because of the APIP's voice in the interagency committee. Therefore, resources that are needed to ensure uninterrupted operation of critical services are apportioned by Alaska's civilian and military leadership.

The dual purpose strategy can embellish any partnership model for any state or region encompassing a military installation that has not pursued security partnerships. The benefit of leveraging public-private and military cooperation, prioritized vulnerabilities, and gauging security limitations is immeasurable in terms of protecting the CI.

[25]The State of Alaska has developed an interagency framework that addresses "all-hazards" prevention, detection, preparedness, response, and mitigation. The APIP, ATACA, and IAG are joint agencies comprised of private, public, and DoD representatives that have established processes for interagency intelligence, information management, and statewide command and control.

III. REGULATION AND STANDARDS

> NCSL [National Conference of State Legislatures] recognizes the significant threat posed by terrorism and the subsequent need for increased homeland security. NCSL believes it is necessary to strike a balance between the need for safety and the rights and freedom of democracy. NCSL further recognizes the demands this challenge places on the federal-state partnership, especially as it relates to the vital role of state and local government in providing a secure homeland and stronger democracy.[26]

A. FEDERAL MANDATES FOR CIP

Can federal mandates energize partnerships? The question reverts to the argument of whether to rely purely on corporate volunteerism or to create an obligation through regulation as an approach to enhance CIP in a unified manner across domains. Generally, the prospect of federal regulation is not well embraced in terms of what is best for free-enterprise. However, this chapter provides evidence that federal regulation is a common instrument that ensures the security of critical industries and the nation's well-being.

The most direct approach available to the federal government in its effort to secure the nation's CI is to mandate federal security measures. The enactment of federal regulation would provide assurance that all sectors are adhering to federally accepted security standards to prevent acts of terrorism and mitigate the effects of natural disasters. The requirement to adhere to federal guidelines would not only establish a common framework for partnering, but would provide the mechanism to bridge the organizational gap inhibiting cross domain partnering as well.

Historically, federal regulation is commonplace throughout American industries such as energy, transportation, and water. So the prospect of regulations governing security would not be considered an extreme act of federal intrusion. Nor would it be welcomed. The desire of all three domains would undoubtedly be for market-based incentives to provide sufficient motivations that drive partnering and collectively increase

[26]Task Force on Protecting Democracy, Recommendations for the Honorable Thomas Ridge, Director of Homeland Security, available at http://www.ncsl.org/programs/press/2001/freedom/pd-fedrec.htm. (Accessed on, February 10, 2006.)

security. However, in the unfortunate event that America suffers another terrorist attack or a natural disaster the deals a severe blow to national CI, the federal government reserves the right to invoke mandates.

The following federal instruments can be considered as solutions for enhancing CI security and concurrently promoting partnering across domains.

1. Invoking government regulation
2. Emphasizing public-private partnerships
3. Requiring insurance
4. Security standards

1. Invoking Government Regulation

The notion of introducing federal regulations to invoke corporate adherence to national CIP standards is not appealing to private enterprise. The task of identifying, assessing, remediating and prioritizing vulnerabilities is generally a matter of process with no concern for proprietary information being accessed by peer competitors via the Freedom of Information Act (FOIA).[27] The construct of the federal bureaucracy and its manifold administrative layers would have to merge with the self-perpetuating mechanics of free enterprise. The private sector would shoulder the preponderance of effort in order to meet the information requirements and protocols necessary to meet the government's requirements.

On Sep 29, 2005 CSPAN3 aired the "House hearings on public safety from 9/11 to Katrina." The hearings at one point focused on the need to expedite communications interoperability that would have enabled the public safety spectrum to support emergency management communications more readily during a disaster like Hurricane Katrina. Senator Chip Pickering, R-MI, offered a compelling question to a panel of

[27] U.S Department of Justice, *Freedom of Information Act of* 1966, available at *http://www.gwu.edu/~nsarchiv/nsa/foia/guide.html.* (Accessed on November 1, 2005.)

telecommunications experts: "Should government wait a year for free enterprise to come up with something or induce a statutory mandate?"[28]

The same ultimatum is relevant in the quest to clearly define how public and private entities should engage in the development of critical infrastructure programs. If a future catastrophic incident degrades defense critical infrastructure to a level that impedes national readiness, volunteerism may ultimately be relegated to just private-private partnering and more stringent federal actions may be implemented to solidify the foundations of public-private partnering.

The federal regulations levied on the energy sector transmission through the Federal Energy Regulatory Commission (FERC) serves as a prominent example of concerns for national security transcending the motivations of free-enterprise "The potential for terrorist attacks on the electric system has pushed secure operation of the grid into the federal policy arena from its traditional position as an industry responsibility."[29] Concurrently, the North American Electric Reliability Council (NERC) established by Presidential Decision Directive-63 (PDD-63) is chartered to oversee the reliability guidelines for the energy industry.[30] The NERC does not have authority to regulate the industry per se but does influence the security guidance for the industry by conducting vulnerability analysis and developing mitigating plans.[31] Even more obtrusive to the private sector is the FERC's legal authority to access industry proprietary information under FERC Order 630.[32]

Similarly, the Environmental Protection Agency (EPA) exercises considerable federal authority in the regulation of hazardous waste management and waste management facilities via the Resource Conservation and Recovery Act (RCRA). The

[28] CSPAN3 aired the "House hearing on public safety communications form 9/11 to Katrina" on September 29, 2005. The panel included Kevin Martin, Chairmen, FCC, David Boyd, SAFECOM, and Vance Hitch, CIO, DoJ. The implication of Senator Pickering's question was that public safety communications were identified as a problem during 9/11 and again during Hurricane Katrina. http://energycommerce.house.gov/108/Hearings/09292005hearing1648/hearing.htm (CSPAN transcript.)

[29] Amy Abel, CRS Report for Congress, Government Activities to Protect the Electric Grid (Washington, D.C.: The Library of Congress, February 4, 2005), 2.

[30] White House, *Protecting America's Critical Infrastructure: PDD-6 (1966).*

[31] Ibid.

[32] Federal Energy Regulatory Commission, "Final Rule," Critical Energy Infrastructure Information. Order No. 630. Docket Nos. RM02-4-000-000 and PL02-1-000-000, February 21, 2003.

EPA delegates much of that authority to the states and distributes much of its budget through grants for improving environmental research.

2. Emphasis on Cross Domain Partnerships (CDP)

What are the criteria for CDP when federal guidance generally only recommends that civil-military partnerships should be developed in order to identify best practices and comprehend each other's vulnerabilities? The melding of federal bureaucracy and free enterprise naturally invokes more negatives than positives. The basic economic principles of return on investment and revenue in comparison to government's calibrated pay scales and bureaucracy can lead to a conflict of interest. The intent of the federal government to identify sector-specific risks cuts deep into the private sector's effort to guard their own vulnerabilities from peer competitors. Thus, the notion of effective CDP really equates to how willing the private sector is to sit down at the table with federal agencies and discuss infrastructure interdependencies and mitigation. Effective civil-military partnering can still be accomplished depending on the relationships that are fostered within every community. Unfortunately, the best practices and metrics of those partnerships will likely not be standardized due to the lack of mandate. As a result, disparate partnerships may proliferate throughout the nation without a common framework to build upon.

3. Requiring Insurance

Can insurance be effectively mandated for the private sector as it is for other aspects of the economy? For instance, "terrorism insurance" is required in order to safeguard lending institutions in the event of catastrophic loss. The McCarren-Ferguson Act of 1945 delegates insurance regulation to the states for regulatory control.[33] The federal government could provide an incentive to states to generate insurance mandates as it did for the REALID ACT.[34] Levying insurance requirements, as some states require for vehicle liability coverage, could standardize building requirements and security

---

[33] United States Congress. *McCarren-Ferguson Act of 1945*. , available at http://www.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_20.html. (Accessed on November 15, 2005.)

[34] The Library of Congress. *Real ID Act of 2005,* available at http://thomas.loc.gov/cgi-bin/bdquery. (Accessed on February 9, 2006.)

standards to increase security (An example of this is TRIA, the Terrorism Risk Insurance Act of 2002.).

The ability of a business to recover financially following a disaster dictates whether or not it will continue in the market place. Insurance is a critical aspect of recovery for the private sector and can also play an important role as an incentive to enhance building security and conversely serve as a prevention agent. Many states require their citizens to maintain some level of automobile liability insurance to protect other drivers from financial distress if injured in an accident. The same standard can be utilized in the promotion of security for physical structures.

The insurance industry can promote compliance to security standards through the manipulation of rates. "A well-functioning insurance market plays a critical role in ensuring social and economic continuity when large-scale disaster occurs. Private insurers paid about 90% of the $23 billion in insured losses that resulted from the four hurricanes that hit Florida in 2004. Two-thirds of the $33 billion in insured losses from the 9/11 attacks were paid by reinsurance companies (mostly European) that operate at a larger level worldwide"[35] The result of the massive payouts after 9/11 resulted in the Terrorism Risk Insurance Act of 2002 (TRIA) which subsidized commercial insurers with federal funding.[36]

The macro affect of TRIA was increased confidence throughout the private sector that insurers would be financially capable of distributing funds in the event of another catastrophic incident. Therefore, the proposed motivation offered by insurance companies is lower premiums to the private sector if they invest in security equipment and systems.

---

[35] Philip Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwan Michel-Kerjan, "The Challenge of Protecting Critical Infrastructure," *Issues in Science and Technology Online*, available at http://www.issues.org/issues/22.1. (Accessed July 2005.)

[36] U.S. Government Accounting Office, Terrorism Insurance, Implementation of the Terrorism Risk Assurance Act of 2002, available at http://www.gao.gov/new.items/d04307.pdf. (Accessed on January 2, 2006.)

4. Security Standards

"Establishing standards" could be perceived as a federal mandate. And although the endeavor to establish a common baseline for security would be difficult, it could be accomplished through critical infrastructure partnerships with the private sector taking the lead for establishing the security criteria.

> Government should be a participant in the standards setting process or take a role in areas that are aimed at protecting the public interest or laying the ground rules for a competitive market. Government should advocate the greater use of voluntary consensus standards and should support that by broader participation by agency personnel in standards development. This aids the government in tackling its mandate to ensure public safety and health.[37]

The establishment of industry-wide security standards can provide the insurance industry with baseline criteria and essentially motivate CIP through premium management.

The author has already established that the federal government is committed to regulatory control of the energy and water sectors in order to ensure critical services are not interrupted. Given that fact, other equally critical functions should be considered for federally-derived security standards if market-driven forces do not produce sufficient levels of security through incentive. The following areas should be considered for enhanced federal regulation due to the magnitude of catastrophe possible as a result of compromise:

- Chemical and biological plants;
- Cyber-security;
- Large buildings/arenas.[38]

---

[37] Richard Chace, Tax Incentives for Homeland Security Related Expenses (H.R. 3562), available at http://wwwc.house.gov/smbiz/hearings/databasedrivenhearingssystems/displaytestimony. (Accessed December 15, 2005.)

[38] Peter Orszag identified chemical and bio plants, large buildings, and cyber-security as three areas for developing security standards during the Subcommittee on Rural Enterprises Agriculture and Technology, 21 July, 2004.

B. A MORE ASSERTIVE NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP)

The draft NIPP was distributed nationally by the Department of Homeland Security on October 13, 2005 for the nation to review and comment. The final NIPP will inevitably provide the roadmap for how local, state, and federal entities approach and execute CIP programs. Therefore, this plan could serve as the definitive federal CIP guidance that could ultimately bridge the gap between the public, private, and DoD domains. But will it provide a universal framework for building partnerships and present the assertive federal guidance that promulgates the development of an engagement strategy? The engagement strategy can only be successful if it is embraced by all three domains. In order for the NIPP to arrive at *innovation,* several areas of CIP should be considered as parallel initiatives that address the concerns circulating throughout active partnerships. The distribution of the draft NIPP was intended to garner input from all three domains and, for that matter, any entity that has a vested interest in securing CI. The author will summarize what he determines are injections to the final NIPP.

1. The Draft NIPP does not Emphasize the Relationship Between the DoD and Explain the Interdependencies Associated with the Public and Private Industries

Private industry and DoD installations are intimately reliant on one another for infrastructure/industry resources (telecommunications, energy, water), installation support, and community relationships. DoD installations and local private industries are mutually supportive during emergency management, specifically in support of an incidence of national significance (INS) and largely benefit from cooperation. The NIPP can serve as the definitive document that decreases the divide between public-private partnering. The federal mandates in HSPD-7 are in direct conflict with the foundations of free enterprise. Understandably, the divide between the DoD and private industry will never close (despite contractual security requirements embedded in the defense industrial base).

However, emphasizing the important relationship between private industry and DoD installations is critical to not only the fluidity of local, state, and federal emergency management during INS, but the strategic assets that provide for the nation's security. The NIPP can place greater emphasis on the interdependencies associated with the

private sector and DoD installations. The DoD's reliance on local industry for critical infrastructure and the private industry's reliance on federal resources in the conduct of homeland security, and to a greater extend an incidence of national significance, should be addressed in greater detail.

2. The Draft NIPP should Explain the Significance of Integrating State and Local Security Assets to Secure Nationally Identified Critical Infrastructure

The private sector continues to seek tangible local, state, and federal resources to protect commercial infrastructure that is deemed nationally critical. The main effort for private sector security planning is relegated to state Title 32 (National Guard) assets, based on their authority to exercise law enforcement when local and state police are occupied with more proactive actions during periods of heightened security.

Therefore, private industry projects an expectation that state assets should augment commercial facilities that are designated as national infrastructure. The NIPP should address in greater detail what the connotation of "state resources" entails. The expectation of law enforcement augmenting private security (i.e., personnel and technology) should be addressed to include the possible role of state Title 32 assets and/or militias.

3. The Draft NIPP Fails to Explicitly Address the Proprietary Concerns of the Private Sector or Recommend Corporate Best Practices for Information Sharing

The process of identifying critical infrastructure, whether DoD or private, requires acknowledgement and analysis of inter/intra-dependencies by all security partners. The proprietary concerns of a business unit can arguably be the primary obstruction to the conduct of fluid partnering. This aspect of partnering does not apply to federal or DoD entities as comparative advantage is generally not a concern. Proprietary awareness is paramount in the development of sector specific analysis and prioritization under the guise of partnering.

For example, the security partnerships established by the Alaska Partnership for Infrastructure Protection (APIP) inadvertently utilized DoD representatives as "honest

brokers" and found success by mediating the proprietary concerns of the private sector.[39] The NIPP should incorporate language that acknowledges the extent of the sensitivity surrounding the proprietary concerns of private industry and emphasize that common ground has to be identified within the sector to attain legitimate prioritization.

4. The Draft NIPP Fails to Promote the Benefit of Developing Innovative State or Federally Sponsored Incentives to Motivate CIP Partnering

Promoting state CIP programs through direct fiscal incentive could energize the private sector in concert with the Buffer Zone Protection Program (BZPP). The BZPP sidesteps private incentive by funding municipal security initiatives. The ability to offer the private sector fiscal incentive (for example man hours devoted to state CIP, or tax incentives for participating in state CIP or more innovative programs) are more beneficial to obtaining "buy-in" from private industry. The NIPP should emphasize the need for local, state, and federal agencies to develop innovative incentive programs that directly impact the private sector.

This chapter addressed the effects of federal regulation, insurance and establishing security standards as vehicles for promote the protection of national CI. The challenge for DHS is how to arrive at the right mixture of programs that are unobtrusive for free enterprise yet dynamic enough to be accepted by all three domains. Concomitantly, the final NIPP can prove tremendously beneficial as the vehicle to provide the public, private, and DoD domains with explicit knowledge for how to develop cross domain partnerships. Decisive wording in the final NIPP, in concert with innovative federal programs, can serve as the bridge that spans organizational and environmental gaps hindering cross-domain partnering.

[39] The author observed during preliminary meetings with Alaska's telecommunications sector that proprietary concerns were significant enough to inhibit information sharing. Mediation between peer competitors on a "one-on-one" basis alleviated the majority of the anxiety generated when sensitive information that pertained to vulnerabilities or the customer base was required.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INCENTIVE AND TAXATION

A. WHAT INCENTIVE?

The federal government is historically aggressive in regulating the private sector's governance of the energy, water, and transportation industries to ensure critical services are reliable and provide needed support to the nation. It would appear obvious, then, that mandates are inevitable if the federal concern for CIP is elevated to level of drinking water or air quality. Could the specter of federal security mandates inadvertently become the incentive for corporations to pursue partnerships and invest capital in anti-terrorist technologies or the continuity of operation policy?

Some segments of the private sector are not as heavily regulated as the energy or transportation sector; this creates an unbalanced playing field for DHS in synchronizing CIP policy. Conversely, HSPD-7 currently provides all federal agencies with the guidance and mandate to assess and prioritize critical infrastructure and the projected final version of the NIPP will further clarify sector specific roles, responsibilities and processes.

Yet because 80-85% of the nation's CI is owned by private entities, a significant amount of corporate cooperation and information sharing would consequently be expected to ensure all three domains arrive at synchronized best practices.[40] Perhaps the most significant aspect of this dilemma is our federalist system that stipulates the separation of free enterprise and government regulation. That leaves DHS in a quandary over how to develop incentives for partnering and collaboration that in affect simultaneously abide by federal guidance and free enterprise. As Joseph A. Pechman, Senior Fellow of the Brookings Institute, stated:

[40] U.S. Department of Homeland Security, Draft National Infrastructure Protection Plan Base Plan, November 2, 2005.

> To be sure, private firms currently have some incentive to avoid the direct financial losses associated with a terrorist attack on their facilities or operations. In general, however, that incentive is not compelling enough to encourage the appropriate level of security – and should therefore be supplemented with stronger market-based incentives in several sectors.[41]

Various sectors – more specifically the telecommunications sector – acknowledge that a predetermined level of risk is acceptable in terms of degradation of loss of business assets and capital as a result of natural disaster or terrorism.[42] The reluctance to invest heavily in critical infrastructure protection may be a result of corporate efficiency by virtue of organic disaster preparedness plans and redundancies built into their business' infrastructure.

How then does DHS secure America's infrastructure when it cannot legally impose mandates on the majority owners of CI? The current solution of offering DHS grants fails to qualify as a meaningful private incentive.

The fiscal year 2005 Buffer Zone Protection Program (BZPP) was approved by the President on October 18, 2004, when he signed the Fiscal Year 2005 Homeland Security Appropriations Act.[43] This program provides funding for states and municipalities to invest in equipment and assets authorized by the Office of Grants and Training and in conjunction with the Information Analysis and Infrastructure Protection (IAIP) Directorate to secure or enhance security of CI. The objective of the BZPP is to assist municipalities in extending the protected boundary of CI, therefore assisting first responders.[44] The private sector does not receive BZPP funding; municipalities do. And although the BZPP investment can enhance the security of the overall community, it may not justify the corporate investment in time and capital expense put into partnering.

---

[41] Peter R. Orszag, Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentive, Testimony before the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security. House Select Committee on Homeland Security, September 4, 2003.

[42] The March 2005 Interagency and Critical Infrastructure Tabletop exercise (TTX) identified significant redundancy built into the telecomm sector in Alaska, further secured by intra-sector mutual aid agreements to support peer competitors in the event of network degradation.

[43] U.S. Department of Homeland Security, Fiscal Year 2005 Buffer Zone Protection Program Guidelines (Washington, D.C.:2005). http://www.ojp.usdoj.gov/odp/docs/fy05bzpp.pdf

[44] Ibid.

For example, the State of Alaska was awarded $550,000 in BZPP funds for fiscal year 2006.[45] Given the geographical size of Alaska and the criticality of oil and gas production and international commerce, $550,000 is not an extravagant sum of money to cover the cost of technical applications and hardware. The $550,000 is further distributed with a limit of $50,000 per jurisdiction, allowing the state the option to decrease or increase specific sites as long as the state does not exceed the $50,000 limit per site. The administrative requirements are cumbersome and include regulatory requirements to monitor and report the execution of the BZPP.[46]

The question is posed again: what incentive? Although the BZPP contributes varying levels of DHS funding according to prioritized criteria, it does little to promote cross domain partnering. The crux of the problem is incentive. What mechanisms can persuade private enterprise to unreservedly collaborate and share information with their peer competitors, local, state, and federal leadership, and, in some instances, members of the DOD?

B. TAX INCENTIVES

The author makes the assumption that if direct incentive is offered to the private sector to participate in CIP partnering initiatives then America's infrastructure will become more secure. Based on the stake holders' concern for their investment in a particular business unit, market incentives would play a vital role in motivating the private sector. A prime example of how the federal government can influence a specific market is the offering of incentives to the energy markets to develop renewable energy (wind generated) projects in the 1990s.

Federal incentives were provided via a production tax credit established by the Energy Policy Act of 1992 (EPACT).[47] The EPACT offered a 1.5¢ per kilowatt hour of electricity produced. The monetary effects of this credit were significant over the lifespan of the project. "The production tax credit was valued at more than $20,000,000

[45] U.S. Department of Homeland Security, Fiscal Year 2005 Buffer Zone Protection Program Guidelines (Washington, D.C.:2005). http://www.ojp.usdoj.gov/odp/docs/fy05bzpp.pdf

[46] Email correspondence, Wayne Rush, State of Alaska Homeland Security & Veterans Affairs.

[47] Mark Gielecki, Fred Mayes, and Lawrence Prete, Forces Behind Wind Power, available at http://www.eia.doe.gov/cneaf/solar.renewables/rea_issues/incent.html. (Accessed December 20, 2005.)

in 1998."[48] The macro effects of EPACT forced the power industry to adjust as the market debated lower-cost fossil fuels or higher-cost environmentally-friendly renewable power sources motivated by the tax credit. In essence, federal incentive was the catalyst for the restructuring of the electric power industry and the shift toward a new source of energy.[49]

Creative tax incentives are found beyond the realm of industry. The National Park Service has also had success offering tax incentives as a means to promote the preservation and revitalization our nation's historical buildings through the *Historic Preservation Tax Incentives* program. "The program fosters private sector rehabilitation of historic buildings and promotes economic revitalization. It also provides a strong alternative to government ownership and management of historic properties."[50] This tax incentive has encouraged private investment since 1976 and is governed by standards established by the Secretary of Interior.[51]

The impact of 9/11 levied a demand on privately owned businesses to invest in enhanced security technology to protect the business unit. The investment in security technology can quickly drain the capital of small businesses and often includes recurring costs.

Congressman Bill Shuster (R-Penn.), introduced H. R. 3562 (also known as the Prevent Act of 2003). This legislature amended the IRS code to allow 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 to improve security.[52] The introduction of tax credits to improve anti-terrorism measures can lessen the financial burden and enable the purchase of biometric technology, closed circuit television, and barrier equipment to increase the level of security for the private sector.

---

[48] Mark Gielecki, Fred Mayes, and Lawrence Prete, Forces Behind Wind Power, available at http://www.eia.doe.gov/cneaf/solar.renewables/rea_issues/incent.html. (Accessed December 20, 2005.)

[49] Ibid., 2.

[50] U.S. National Park Service, *Historic Preservation Tax Incentives,* available at http://www.cr.nps/hps/tps/tax/. (Accessed on January 4, 2006.)

[51] Ibid.

[52] 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).

C. PETER R. ORSZAG: TESTIMONY BEFORE THE SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT AND THE SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY. SEPTEMBER 4, 2003

Peter R. Oszag, of The Brookings Institution, offered noteworthy testimony in front of the House Select Committee on Homeland Security with regards to the role of incentives for the protection of critical infrastructure. His remarks highlighted the role of market incentives as a tool to reduce security risks, versus the expectations of the private sector to invest voluntarily. The author regards this data as the most relevant data acquired in this research.

Should the security of America's infrastructure, and consequently the security of Americans, be afforded the government's commitment to deregulate private markets? Federal innovation could feasibly be the catalyst that motivates the captains of industry to participate in public-private partnering through financial incentive. The key is to find the right balance, because "Private markets themselves do not generate sufficient incentives for homeland security."[53] Orszag highlights seven reasons why private markets by themselves do not generate sufficient incentive and why governments should intervene:

- National sovereignty cannot be quantified. A significant terrorist attack undermines the nation's sovereignty, just as an invasion of the nation's territory by enemy armed forces would. The cost associated with a reduction in the nation's sovereignty or standing in the world may be difficult to quantify. In other words, the costs of the terrorist attack extend well beyond the immediate areas and people affected; the attack imposes costs on the entire nation.
- Negative externalities. The government could reduce the risk of terrorist attacks by reducing the overall vulnerability of high payoff targets such as chemical or explosive plants that may supply the sources for a terrorist incident in another location.
- Contamination effects. Contamination effects arise when a catastrophic risk by one firm is determined in part by the behavior of others.
- Accurate evaluation of security standards. The cost of accurately evaluating security measures across a broad spectrum of facilities could be cumbersome. Establish standards, codes or minimum guidelines for building security.

[53] Orszag, Critical Infrastructure Protection, 2.

- Corporate and individual financial loss. Corporate and individual financial exposures to the losses from a major terrorist attack are inherently limited by the bankruptcy laws. Since the outcome for the firm's owners would not depend on the severity of the attack, the firm would have little or no incentive to reduce the likelihood of the more severe version of the attack, even if the required preventive steps were relatively inexpensive.
- Expectation of a government bailout. Private firms, expecting the government to bail them out should an attack occur, do not undertake as much security as they would otherwise. If the government cannot credibly convince the private sector that no bailouts will occur after an attack, it may have to intervene before an attack to offset the adverse incentives created by the expectation of a bailout.
- Complete markets. Government involvement may be warranted to fulfill imperfections in the capital and insurance markets.[54]

The nuances of government incentive and intervention can be complicated when the analysis considers all the ramifications for the private sector. In his testimony, Orszag details his advice that the government provide added security for buildings by taking the following actions.

- Impose direct regulation for the inclusion of anti-terrorist building features.
- Require terrorism insurance for every public and private entity.
- Subsidize anti-terrorism efforts through direct government spending or tax-incentive.

Capital investment committed to securing CI is undoubtedly a step in the right direction. The question is, can direct government spending or tax incentives alone promote cross-domain partnering? A solution lies in the return on investment that appeases stakeholders combined with the residual market effects of tax-incentives. In order for stockholders to condone corporate involvement in CIP partnerships, the incentive must be direct and financially motivating. If corporations are reimbursed or funded for man-hours invested in the conduct of partnering, then an acceptable obligation is created between the public and private sector.

[54] Orszag, *Critical Infrastructure Protection*, 2.

The importance of CIP, given the known threat of terrorism, justifies tax-incentive programs that are designed to promote private investment in security hardware, applications, and training. Tax incentives offered as a catalyst to promote CIP can directly compliment partnering initiatives by establishing new market trends in the security industry. The proliferation of security technologies can subsequently be used as leverage to integrate partnerships linked by sector interdependencies, hence motivating peer-to-peer and cross domain partnerships.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This thesis makes two overarching arguments. First, building cross-domain partnerships is better than relying on corporate volunteerism. Second, regional CIP collaboration is better than sector-specific analysis. The author further argues that the best way to achieve collaboration between the private sector, government, and the military is to develop security standards, incentivize insurance policies, and consider tax incentives to motivate investment in CIP programs. These claims are based on in-depth analysis of CIP partnering, regionalization, taxes, insurance, and standards as they have been applied to other related problematic areas of federal responsibility. The author's initial concern represents the root problem of the partnering dilemma: the definition of partnering itself.

A. DEFINE PARTNERING

Several definitions of *partnering* were provided as a starting point for this thesis to emphasize the proliferation of partnering initiatives throughout the nation. Current federal guidance and constitutional law tell us that partnering cannot be mandated by the government to enhance the security of DoD and/or privately owned critical infrastructure. Conversely, the expectation of corporate volunteerism should not be relied on as the bedrock for any policy because volunteerism does not constitute an obligation that ensures long-term bonds or mandates collaboration and information sharing. Each domain offers its own interpretation of partnering that is invariably formed by either geographic alliances or market forces, ultimately suggesting that partnering is an ambiguous endeavor.

Critical infrastructure partnerships, regardless of domain, should be defined by the intra/interdependencies that induce cross sector relationships and span all three domains. The cascading effects of the 2003 northeast region power outage, for example, make the case that interaction within peer communities and across sectors and domains is inevitable by virtue of our existing industrial architectures. The global threat directed

toward America and its critical infrastructure does not warrant the time needed for market trends to dictate CIP strategies. Expeditious and innovative solutions that assist cross-domain engagement should be buttressed by assertive DHS doctrine.

Ironically, the January 2006 NIPP Base Plan does not offer a definition of *partnerships* or *partnering* in its Glossary of Key Terms.[55] Opponents of a DHS-derived definition of partnerships could argue that partnerships are proliferating without the assistance of federal definition, so why project more federal guidance? Consider the excessive amount of energy initially put forth by public, private and DoD leadership in Anchorage AK, to build the Alaska Partnership for Infrastructure Protection. The contribution of a federal CIP partnering definition as a starting point for their charter would have greatly expedited the formulation of that security partnership by establishing the fundamental objectives of CIP. Therefore, as a catalyst for national partnering initiatives, the DHS should advocate the significance of integrating the three domains for CIP, develop a standard definition for cross-domain partnering, and include that definition in the final NIPP.

B. SECURITY STANDARDS

The most expeditious, yet controversial, method to promote security partnerships could be federal regulation of security standards. Standards are both market-driven and mandated by the government, bottom-driven and top-fed. The energy, oil, and water industries have a long history of federal regulation enforcing sector-wide compliance for security and operations. The DHS's Protective Security Division (PSD) is working in conjunction with the Electric Power Research Institutes (EPRI) to develop an International Standards Institute (ISO) compliant high-voltage recovery transformer that can be readily transported.[56] The author's discussions with Alaska's corporate and public telecomm sector, and research in the area of federal mandates, indicate additional regulation would be unwelcome. Redundant communications architectures within the

---

[55] U.S. Department of Homeland Security, National Infrastructure Protection Plan, Base Plan, Revised Draft NIPP Ver.2 (Washington, D.C.: January, 2006), 7.

[56] Amy Abel, CRS Report for Congress: Government Activities to Protect the Electric Grid (Washington, D.C.: The Library of Congress, February 4, 2005), 5.

Alaska's telecomm sector and mutual aid agreements amongst carriers mitigate the effects of a single point of failure.

The Department of Defense's reliance on military doctrine as the foundation for its operational efficiency exemplifies the importance of deriving common standards to support organizational objectives. Universal standards and common language serve as enablers in large organizations. Correspondingly, DHS mandated security standards developed in conjunction with industry sectors would provide security partnerships with the ability to assess industry-wide data across sectors, regions, and the DHS.

As a result of DHS, and more specifically industry, not establishing common security standards, contrasting security and disaster recovery programs are dispersed throughout the sectors. The result of the latitude and ambiguity left to the interpretation of discreet CIP partnerships may ultimately dictate the speed with which federal standards are considered if market forces do not develop security standards before the next catastrophic incident.

C. PROPOSED SOLUTIONS

The DHS has to arrive at a consensual incentive package that directly appeases the private sector's stakeholders and genuinely promotes partnering throughout the public, private, and DoD domains. The research included in this thesis makes three recommendations that can promote security partnerships and subsequently increase the security of national CI.

1. Provide assertive language in the NIPP that emphasizes public-private-DoD partnerships.
2. Promote regionalization to understand cross-sector and cross-domain interdependencies.
3. Provide innovative CIP incentive packages that include:
    - Security standards;
    - Insurance; and
    - Tax incentives.

1. The NIPP

The final NIPP is the definitive DHS vehicle to emphasize the importance of the private sector collaborating and sharing information with its contiguous DoD community. The array of deployable resources projected by the DoD and its management of the defense-industrial base is critical to the security of this nation, as is privatized infrastructure. The NIPP can serve as the conduit to bridge the challenges and limitations that encompass public-private-DoD partnering. The term "partnering" must be defined with concise guidance and incentive within the NIPP to invoke genuine teamwork to prioritize infrastructure in order to direct local, state, and federal resources to secure what is critical to the nation's security. The motives and nuances of private sector partnering with DoD deserve special recognition in the final NIPP.

2. Regionalization

Geographic regionalization is the preferred solution to maximize the overall effectiveness of security partnerships. The sovereignty of the state governor and the commerce boundaries within a given state establish the optimal security environment for identifying and prioritizing CI vulnerabilities and critical nodes. The sector-specific guidance and framework defined in the NIPP Base Plan serves as the basis for planning and analysis, but remains sector-centric. A comprehensive analysis of what a state region produces and supports is relevant to understanding the foreseeable risks that can be mitigated once interdependencies are understood. To highlight the efficiency of regionalization, consider this justification, offered by International Association of Business Communications.

> The unwieldy eight districts nationwide are being consolidated into three larger regions that will be able to provide a plethora of services that might not have been available in the past. The consolidation also opens the door for sharing best practices among different chapter leaders that will prove to make all chapters stronger. The result is a better value for all local chapter members.[57]

The Alaska Partnership for Infrastructure Protection (APIP) model offers additional proof that cross-domain partnerships incorporating a regional perspective

[57] Camille Downing, Regional Leadership Opportunities, Opportunities Abound In New IABC Heritage Region. Available at http://www.isbcpittsburgh.com/leadership/index.jsp. (Accessed January 14, 2006.)

collectively reinforce prevention, preparedness and recovery policy on a statewide scale. Understanding the sector-specific nuances of peer relationships is critical to the formulation the security partnerships. However, in the case of the APIP, progress was further advanced by assessing the state's sector-specific vulnerabilities with regional vulnerabilities. The APIP's ultimate objective was met by producing a statewide prioritized listing of CIP vulnerabilities; this could not have been achieved by focusing purely on sector-specific vulnerabilities.

3. Incentive Packages

Financial incentives can individually, or as an amalgam, produce sufficient motivation for the private sector to engage in partnerships and invest in security. The relationship between federally-mandated security standards and insurance is complimentary. Participation in CIP security partnerships can be motivated by offering reduced disaster or terrorism insurance premiums for entities that engage in CIP initiatives. The Terrorism Risk Insurance Act (TRIA) of 2002 was extended to 2007 under legislation introduced by Senator Christopher Dodd and approved on November 18, 2005.[58] Many modifications were built into the TRIA-Extension Act of 2005 that offers risk mitigation for the private sector through the manipulation of premiums.[59] If a business unit complies with security standards or joins a security partnership, and subsequently reduces corporate liability, then an obligation to remain a security partner begins to solidify.

Research provided in this thesis suggests that tax incentives are monetary catalysts that can affectively promote the migration of policy and attitudes. Peter Oszag refers to this amalgamation as a "*mixed system*" of incentives and suggests that just one approach is insufficient. "A mixed system has the advantage of being flexible, a key virtue in an arena where new threats will be "discovered" on an ongoing basis."[60] The strength of tax incentives can be summarized in the U.S. Department of Interior's Historic Preservation Tax Incentive Program. Since 1976, The Historic Preservation Tax

[58] Baird Webel, CRS Report for Congress: Terrorism Risk Insurance Legislation: Issue Summary and Side-by-Side (Washington, D.C.: Library of Congress, updated, January 11, 2005).

[59] Ibid, 7.

[60] Peter R. Orszag, "Tax Incentives for Homeland Security Related Expenses" (H.R. 3562), available at http://wwwc.house.gov/smbiz/hearings/databasedrivenhearingssystems/displaytestimony. (Accessed December 15, 2005.)

Incentive Program has rehabilitated more than 32,000 historic properties, stimulated over thirty-three billion dollars in private investment, rehabilitated more than 185,000 housing units, and created over 140,000 housing units.[61] In this case, tax incentives have profoundly motivated investment and provided a catalyst for the federal government to promote the specific national objective of revitalizing historical structures.

Tax incentives may promote expenditure on equipment or systems that are inherently designed to deter vandalism, as opposed to technical solutions designed to deter or prevent terrorism. The definition of anti-terrorism equipment may require refinement to avoid what could be viewed as wasteful spending. At the national level, tax reform and spending on homeland security programs remain a delicate topic and would certainly draw debate as the taxpayers are the ultimate bill payers. The easing of taxes on the private sector for security enhancement could easily beg the question: Why? We have not been attacked since 9/11. The levying of a security tax on consumers of specific resources that are produced by CI can inadvertently disrupt free enterprise. A corporation's competitive advantage in a specific market can be affected if the population does not share the same concern for security as the federal government – particularly if that market area is not categorized as a national priority.

A solution is rooted in both financial enticement and impending federal regulation. The federal government and the private sector need to successfully navigate the forces of free enterprise in order to find common ground that appeases stakeholders who do not find securing critical infrastructure worthy of capital investment. Initially, this approach translates to public-private engagement with the objective of identifying what incentives are meaningful to corporate leadership and stakeholder alike. The federal government must research the offering of fiscal incentives to offset the minimal man-hours that will be devoted to collaboration. The government's goal is to invoke a more substantive private approach to collaboration with federal agencies through fiscal incentive. And although historical research and studies on what incentives effectively promote cross-domain partnerships is limited, the question of what actually is an incentive continues to be asked in public, private, and DoD forums. Therefore, the

[61] U.S. National Park Service, *Historic Preservation Tax Incentives,* available at http://www.cr.nps/hps/tps/tax/. (Accessed on January 4, 2006.)

federal government should, in conjunction with the states, consider the aforementioned incentives as mechanisms to promote CIP partnering.

D. THE CONTRIBUTION TO CRITICAL INFRASTRUCTURE PROTECTION

This thesis' contributes to the existing body of critical infrastructure protection knowledge by examining the premise that the Department of Defense is a peer security partner with the public and private sectors. The conclusion refutes the commonly accepted belief that the concept of public-private partnering represents the overarching framework to protect the nation's infrastructure, with only the collaboration of free enterprise and public utilities.

The author's fundamental objective, to emphasize the critical relationships that military installations share with communities throughout the United States, was highlighted by proposing that these are cross-domain partnerships. Cross-domain partnerships, as described in this thesis, encompass the public, private, and DoD synchronized initiatives to secure private and federally owned and operated critical infrastructure. These extended partnerships have historically relied on each other by virtue of the resources and community support needed when acts of terrorism or natural disasters debilitate a region and overwhelm local emergency management.

Concomitantly, this thesis projects that assertive, if not aggressive, federal critical infrastructure guidance can promulgate an innovative framework for security partnerships, as opposed to the current guidance that merely recommends that sectors conduct partnering. The DHS must function as the leader and facilitator of a nationally synchronized CIP initiative by implementing a National Infrastructure Protection Plan that promotes cross domain partnering.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abel, Amy. CRS Report for Congress. *Government Activities to Protect the Electric Grid*. Washington, D.C.: The Library of Congress, February 4, 2005.

"AIA Urging Federal Incentive for Primary Seat Belt Laws." *Insurance Journal, National News* (April 2005). http://www.insurancejournal.com/news/national/2005/04/13/53731.htm?print=1 (Last accessed December 5, 2005)

Auerswald, Philip, Lewis M. Branscomb, Todd M. La Porte, and Erwan Michel-Kerjan. "The Challenge of Protecting Critical Infrastructure." *Issues in Science and Technology Online*, July 2005. http://www.issues.org/issues/22.1 (Last accessed September 10, 2005)

Auerswald Philip, E., and Lewis M. Branscomb. "Valleys of Death and Darwinian Seas: Financing the Invention to Innovation Transition in the United States." *Journal of Technology Transfer,* 28, no. 2 and 3 (August 2003): 227-239.

Bousquet, Kenneth and Mark Sagan. *Partnering For Success: A Blueprint For Promoting Government Industry Communication and Teamwork."* http://www.amc.army.mil/amc/command_counsel (Last accessed November 5, 2005

Brashear, Jerry P. "The Necessity of Regional Public/Private Partnerships for Effective Critical Infrastructure Protection." *The CIP Report* 4, no. 3 (September 2005)

Carafano, James Jay, Ph.D. *Countdown to 9/11: Five Fixes for Homeland Security by the Fifth Anniversary of the Attacks*. http://heritage.org/Research/HomelandDefense/wm963.cfm (Last accessed February 10, 2006)

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/databasedrivenhearingssystems/displaytestimony (Last accessed December 15, 2005)

Datz, Todd. "Capital Ideas." *CSO Online,* December 5, 2005. http://www.csoonline.com/read/120103/ideas.html (Last accessed December 15, 2005)

Defense Contract Management Agency. *DCMA Guidebook.* Washington, D.C.: Defense Contract Management Agency, October 15, 2005. http://guidebook.dcma.mil/74/instructions.htm (Last accessed September 15, 2005)

Downing, Camille. "Regional Leadership Opportunities, Opportunities Abound in New ABC Heritage Region." *International Association of Business Communicators*, January 14, 2006. http://www.isbcpittsburgh.com/leadership/index.jsp (Accessed January 14, 2006)

Florida Department of Community Affairs. "Welcome to the Florida Wind Insurance Incentive Web Site!" Florida: Florida DCA, February 10, 2006. http://www.dca.state.fl.us/fdem/mitdb/index.cfm (Accessed February 25, 2005)

Gielecki, Mark, Fred Mayes, and Lawrence Prete. *Incentives, Mandates, and Government Programs for Promoting Renewable Energy.* Washington, D.C.: Energy Information Administration, December 20, 2005. http://www.eia.doe.gov/cneaf/solar.renewables/rea_issues/incent.html (Accessed January 10, 2006)

_____. *Forces Behind Wind Power*. Washington, D.C.: Energy Information Administration, December 20, 2005. http://www.eia.doe.gov/cneaf/solar.renewables/rea_issues/incent.html (Accessed January 3, 2006)

Hanson, Julie. "Government Knows Best." *CSO Online*, February 12, 2006. http://www.csoonline.com/read/010104/wonk_who.html (Accessed February 12, 2006)

HDR. *Creating Effective Public-Private Partnering for Buildings and Infrastructure in Today's Economic Environment*. Washington, D.C.: The National Council for Public-Private Partnerships, November 2005. http://www.ncppp.org/resources/papers/hdrp3whitepaper.pdf (Accessed December 15, 2005)

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending A Networked Nation*. Monterey, California: Naval Postgraduate School, 2004.

Lewis, Ted, G. and Rudy Darken. "Potholes and Detour in the Road to Critical Infrastructure Protection Policy." *Homeland Security Affairs* 1, no. 2 (December 2005). www.hsaj.org (Accessed January 3, 2006)

Library of Congress. *Real ID Act of 2005.* Washington, D.C.: Library of Congress, February 9, 2006.

Moteff, John and Paul Parfomak. CRS Report for Congress. *Critical Infrastructure and Key Assets: Definition and Identification*. Washington, D.C.: Library of Congress, October 1, 2004.

Moteff, John. CRS Report for Congress. *Critical Infrastructure Protections: The 9/11 Commission Report and Congressional Response*. Washington, D.C.: Library of Congress, January 11, 2005.

_____. CRS Report for Congress. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Washington, D.C.: Library of Congress, February 4, 2005.

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://wwwc.house.gov/smbiz/hearings/databasedrivenhearingssystems/displaytestimony (Accessed December 15, 2005)

_____. *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentive*. Testimony before the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security. Washington, D.C.: House Select Committee on Homeland Security, September 4, 2003.

Parfomak, Paul W. CRS Report for Congress. *Guarding America: Security Guards and U.S. Critical Infrastructure Protection*. Washington, D.C.: Library of Congress, November 12, 2004.

Policy Monitor. *Critical Infrastructure and Homeland Security*. Washington, D.C.: U.S. Chamber of Commerce, April 2003.

Pommerening, Christine. "Regional Public-Private Partnerships in Perspective." *The CIP Report* 4, no. 3 (September 2005).

Poulsen, Kevin. "U.S. Info-sharing initiative called a flop." *Register,* August 31, 2005. http://www2.theregister.co.uk/2005/02/15/us_infosharing_initiative_flop_claim/ (Accessed October 20, 2005)

Riehl, James R. CRS Report for Congress. *Homeland Security: Federal Assistance Funding and Business Opportunities*. Washington, D.C.: The Library of Congress, December 23, 2004.

Schowengerdt, Dr. Frank. *Space Exploration: The Role of the Innovative PartnershipProgram*. Washington, D.C.: National Aeronautics and Space Administration, February 10, 2006. http://ipp.nasa.gov/innovation/innovation115/4-coverstory.html

Task Force on Protecting Democracy. *Recommendations For The Honorable Thomas Ridge, Director of Homeland Security.* Washington, D.C.: National Conference of State Legislatures, February 10, 2006. http://www.ncsl.org/programs/press/2001/freedom/pd-fedrec.htm (Accessed February 10, 2006)

U.S. Alaskan Command. *Private Sector and Interagency, Critical Infrastructure Protection Tabletop Exercise: Guidebook*. May 2005.

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.

_____. *McCarren-Ferguson Act of 1945*. Washington, D.C., 1945. http://www.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_20.html (Accessed January 3, 2006)

_____. Armed Forces (1956). *Title 10 U.S Code*. http://uscode.house.gov/download/pls/32T.txt. (Accessed October 10, 2005)

_____. National Guard *(1956). Title 32 U.S Code*. http://uscode.house.gov/download/pls/32T.txt. (Accessed October 10, 2005)

U.S. Department of Defense. *Department of Defense Critical Infrastructure Protection Strategy*. Washington, D.C.: Department of Defense, April 2003.

_____. *Department of Defense Directive 2000.12. Department of Defense Antiterrorism (AT) Program.* Washington D.C.: Department of Defense, 2003.

_____. *Department of Defense Directive 3020.40. Defense Critical Infrastructure Program (DCIP*). Washington D.C.: Department of Defense, 2005.

U.S. Environmental Protection Agency. *Corrective Action.* Washington, D.C.: Environmental Protection Agency, January 2006. http://www.epa.gov/cgi-bin/epaprintonly.cgi (Accessed January 20, 2006)

U.S. Government Accounting Office. *Terrorism Insurance, Implementation of the Terrorism Risk Assurance Act of 2002.* Washington, D.C.: Government Accounting Office, 2002. http://www.gao.gov/new.items/d04307.pdf (Accessed January 2, 2006)

U.S. Department of Homeland Security. *Critical Infrastructure Identification Prioritization, and Protection: HSPD-7*. Washington, D.C.: Department of Homeland Security, December 2003.

_____. *Fiscal Year 2005 Buffer Zone Protection Program Guidelines*. Washington, D.C.: Department of Homeland Security, 2005.

_____. *National Infrastructure Protection Plan, Revised Draft NIPP, V2.0*. Washington, D.C.: Department of Homeland Security, January 2006.

_____. *National Strategy for Homeland Security*. Washington, D.C.: Department of Homeland Security, July 2002.

_____. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, D.C.: Department of Homeland Security, February 2003.

_____. *Sector-Specific Plan; Defense Industrial Base*. Washington, D.C.: Department of Homeland Security, November 2004.

U.S. Department of Justice. *Freedom of Information Act.* Washington, D.C.: Department of Justice, 1966.

U.S. National Park Service. *Historic Preservation Tax Incentives.* Washington, D.C.: Department of the Interior, 2006. http://www.cr.nps.gov/hps/tps/tax/ (Accessed January 4, 2006)

Webel, Baird. CRS Report for Congress. *Terrorism Risk Insurance Legislation: Issue Summary and Side-by-Side.* Washington, D.C.: Library of Congress, updated January 11, 2005.

The White House. *Protecting America's Critical Infrastructure: PDD-63*. Washington, D.C.: Critical Infrastructure Assurance Office, May 1998. http://www.fas.org/irp/offdocs/pdd-63.htm (Last accessed August 31, 2005)

Wong, Nancy. *Interview with Nancy Wong, Commissioner, President's Commission On Critical Infrastructure Protection*, July 2002. http://www.homelandsecurity.org/journal/interviews/wong.html (Last accessed September 10, 2005)

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alaskan Command Headquarters
   Attn: ALCOM Chief of Staff
   Elmendorf Air force Base, Alaska

4. Paul Stockton, Director
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

5. Ted Lewis, Academic Associate
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

6. Colonel Mary Frels
   NORTHCOM J34
   United States Northern Command
   Colorado Springs, Colorado

7. Nancy Wong
   Infrastructure Protection
   Department of Homlend Security
   Washington District of Columbia