NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RISK MANAGEMENT AS STRATEGIC CHANGE IN NATIONAL HOMELAND SECURITY POLICY

by

John P. Paczkowski

September 2007

Thesis Advisor: Robert Bach
Second Reader: Thomas Mackin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2007	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Risk Management as Strategic Change in National Homeland Security Policy	
6. AUTHOR(S) John P. Paczkowski	
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	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

Secretary Michael Chertoff has said that the core principle that animates the Department of Homeland Security (DHS) is risk management. Risk management is a process of choosing trade-offs between available resources and the cost of minimizing the risk of unwanted consequences through an ongoing cycle of objective setting, risk assessment, alternatives evaluation, and implementation, in a way that buys down risk over time. The statements of national leaders, federal legislation, and the Department of Homeland Security's own strategy documents have set risk management as homeland security policy. Nonetheless, DHS has been challenged to implement a coordinated and integrated risk management program to include compatible risk assessment methodologies among its component agencies. The National Infrastructure Protection Plan (NIPP), released in 2006, for the first time sets out a vision for a national risk management framework. That vision now extends the application of risk management to the nation's critical infrastructure owners and operators. This paper explores the challenges involved in implementing the risk management framework under the NIPP, examines how implementation has been managed as strategic change through the lens of change management theory, and offers recommendations for improvement. It is hoped this paper will motivate further study into homeland security strategic change.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Risk Management, Risk Analysis, Risk Assessment, Strategic Change, Strategic Leadership, Organizational Change, Open Systems Theory, Complexity, Wicked Problems	197
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

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

RISK MANAGEMENT AS STRATEGIC CHANGE IN NATIONAL HOMELAND SECURITY POLICY

John P. Paczkowski
Civilian, Port Authority of New York and New Jersey
B.S., New Jersey Institute of Technology, 1975
M.S., New Jersey Institute of Technology, 1983
M.A., Columbia University, 1994

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
September 2007

Author: John P. Paczkowski

Approved by: Robert Bach
Thesis Advisor

Thomas Mackin
Second Reader

Dr. Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Secretary Michael Chertoff has said that the core principle that animates the Department of Homeland Security (DHS) is risk management. Risk management is a process of choosing trade-offs between available resources and the cost of minimizing the risk of unwanted consequences through an ongoing cycle of objective setting, risk assessment, alternatives evaluation, and implementation in a way that buys down risk over time. The statements of national leaders, federal legislation, and the Department of Homeland Security's own strategy documents have set risk management as homeland security policy. Nonetheless, DHS has been challenged to implement a coordinated and integrated risk management program to include compatible risk assessment methodologies among its component agencies. The National Infrastructure Protection Plan (NIPP), released in 2006, for the first time sets out a vision for a national risk management framework. That vision now extends the application of risk management to the nation's critical infrastructure owners and operators. This paper explores the challenges involved in implementing the risk management framework under the NIPP, examines how implementation has been managed as strategic change through the lens of change management theory, and offers recommendations for improvement. It is hoped this paper will motivate further study into homeland security strategic change.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMSC	Area Maritime Security Committee
ASME	American Society of Mechanical Engineers
CIP	Critical Infrastructure Protection
CI/KR	Critical Infrastructure / Key Resources
CIPAC	Critical Infrastructure Partnership Advisory Council
CIP/DSS	Critical Infrastructure Protection Decision Support System
CREATE	Center for Risk and Economic Analysis of Terrorism Events
CRS	Congressional Research Service
CS&C	Office of Cyber Security and Communications
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EO	Executive Order
EPA	Environmental Protection Agency
EP	Exceedance Probability Curve
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FMSC	Federal Maritime Security Coordinator
FSLC	Federal Senior Leadership Council
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSA	Homeland Security Advisor
HSAC	Homeland Security Advisory Council
HSDEC	Homeland Security and Defense Education Consortium
HSGP	Homeland Security Grant Program
HSI	Homeland Security Institute
HSPD	Homeland Security Presidential Directive
GAO	Government Accountability Office
GCC	Government Coordinating Council
G&T	Grants and Training
IAIP	Information Analysis and Infrastructure Protection
IGP	Office of Intergovernmental Programs
IP	Infrastructure Protection
ISAC	Information Sharing and Analysis Centers
ITI	Innovative Technologies Institute
KM	Knowledge Management
LANL	Los Alamos National Laboratory

MAST	Maritime Assessment and Strategy Toolkit
MBVA	Model-Based Vulnerability Analysis
MSRAM	Maritime Security Risk Assessment Methodology
NADB	National Asset Database
NGA	National Governors Association
NIAC	National Infrastructure Advisory Council
NIE	National Intelligence Estimate
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NPPD	National Protection and Programs Directorate
NRP	National Response Plan
NSF	National Science Foundation
NYPD	New York City Police Department
ODP	Office for Domestic Preparedness
OECD	Organization for Economic Cooperation and Development
OHS	Office of Homeland Security
OIA	Office of Intelligence and Analysis
OIG	Office of Inspector General
OIP	Office of Infrastructure Protection
ORISE	Oak Ridge Institute for Science and Education
PCCIP	President's Commission on Critical Infrastructure Protection
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PSRAT	Port Security Risk Assessment Tool
RAM	Risk Assessment Methodologies
RAMCAP	Risk Analysis and Management for Critical Asset Protection
R&D	Research and Development
RMA	Office of Risk Management and Analysis
RMAT	Risk Management Assessment Tool
RTSWG	Regional Transit Security Working Group
S&T	Science and Technology Directorate
SARMA	Security Analysis and Risk Management Association
SBI	Southern Border Initiative
SBRM	Systems-Based Risk Management Process
SCC	Sector Coordinating Council
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SNJTK	Special Needs Jurisdiction Tool Kit
SNL	Sandia National Laboratories
SRA	Society for Risk Analysis
SSA	Sector-Specific Agency

SSP	Sector-Specific Plan
TMSARM	TSA Maritime Self-Assessment Risk Module
TPC	Technical Political Cultural Framework
TRAM	Transit Risk Assessment Module
TRAVEL	Transportation Risk Assessment and Vulnerability Evaluation
TSA	Transportation Security Administration
UAWG	Urban Area Security Initiative Urban Area Working Group
USCG	United States Coast Guard
USN	U.S. Navy
VISAT	Vulnerability Identification Self-Assessment Tool
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This work is dedicated to my friends and colleagues at the Port Authority of New York and New Jersey who perished at the World Trade Center on September 11, 2001. It is also dedicated to the heroism of the thirty-seven Port Authority Police Officers who freely sacrificed their lives on that day so that others might live. Their dedication to the highest ideals of excellence in public service has been a guiding light and inspiration. I will never forget them, and I will never forget that day. May I always live up to their memory.

My undying thanks go to my wife, Connie, who has been my coach, editor, and biggest fan throughout the course of this work and the entire master's program. I could not have done it without her by my side. Thanks also to my Thesis Advisor Robert Bach and Second Reader Thomas Mackin. Their sage advice and support kept me going until the job was done. Finally, thanks to my teammates at the Port Authority's Office of Emergency Management for carrying my load. I know of no finer group of professionals.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

According to Director of National Intelligence John McConnell, the U.S. homeland faces a persistent and evolving terrorist threat over the next three years, especially from al-Qa'ida, which continues to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, dramatic destruction, and significant economic aftershocks.[1] Comptroller General of the United States David Walker, on the other hand, has asserted that our nation's fiscal policy is on an unsustainable course in that we face a large and growing deficit that will gradually erode our economy, our standard of living, and ultimately our national security.[2] Moreover, ongoing wars in Iraq and Afghanistan add significantly to nation's current security and fiscal challenges.

With these issues as backdrop, federal homeland security spending continues to rise, with the president's 2007 Budget for the Department of Homeland Security (DHS) well over $42.7 billion. Though this number is substantial, DHS Secretary Michael Chertoff acknowledges that actual funding requirements may be ten to fifteen times greater than the resources currently available.[3] Given that there are not enough resources to address all homeland security needs, risk management and the priority allocation of resources against the greatest threats are central tenets of Homeland Security Presidential Directive–7 (HSPD-7) for critical infrastructure protection and the National Infrastructure Protection Plan (NIPP).

---

[1] Office of the Director of National Intelligence, *National Intelligence Estimate — The Terrorist Threat to the US Homeland* (Washington, DC: Office of the Director of National Intelligence, July 2007), 6-7.

[2] Government Accountability Office, *Homeland Security — Applying Risk Management Principles to Guide Federal Investments* (Washington, DC: Government Accountability Office, February 7, 2007), 12.

[3] U.S. Department of Homeland Security, *Keynote Address by Secretary of Homeland Security Michael Chertoff to the 2006 Grants & Training National Conference* (Washington, DC, November 28, 2006), http://www.dhs.gov/xnews/speeches/sp_1164738645429.shtm [Accessed April 12, 2007].

Unfortunately, DHS efforts to implement homeland security risk management policy and practices over the last several years have been challenged by the absence of a common theoretical framework and well-established professional discipline, a diversity of incompatible approaches advanced independently by its component agencies, and recurring changes in organizational structure and senior leadership. Despite its importance to the nation, there is not a long-term, overarching strategy for the development and coordination of risk management initiatives across DHS. With the issuance of the NIPP in 2006, the problem has become even more acute and now extends more broadly to the larger homeland security community.

The NIPP establishes an unprecedented public/private sector partnership and creates a vision for a risk management framework to guide decision-making and resource allocation for the protection of the nation's Critical Infrastructure and Key Resources (CI/KR). Though the plan clearly delegates responsibility for advancing risk management programs within each of the seventeen CI/KR sectors, it does not provide much else in support of that vision. Problems that have plagued internal DHS risk management efforts persist and are now multiplied across the seventeen industry sectors. There is still no common theoretical framework, no set of professional standards, no commonly accepted risk assessment best practices, and no risk management implementation structure. More significantly, perhaps, there is no long-term, overarching strategy to guide the implementation of the NIPP risk management framework as a significant strategic change in national homeland security policy.

Development and initial implementation of the NIPP has been a remarkable achievement in public-private sector homeland security collaboration. However, if the implementation of the risk management framework as the cornerstone of the NIPP is not effectively managed as strategic change, the goals of the NIPP may not be fully realized. At best this might mean less than cost-effective application of limited homeland security resources. At worst, it could mean that significant homeland security risks go unaddressed, with the potential for catastrophic consequences.

B. RESEARCH QUESTION

How has the implementation of the National Infrastructure Protection Plan (NIPP) risk management framework been handled as strategic change in homeland security policy? How might change management theory and practice be applied to assess the implementation of that policy? What lessons can be learned from this assessment that, if applied, may help ensure successful implementation and sustainability of the NIPP risk management framework over the long-term?

C. PRACTICAL SIGNIFICANCE OF THE PROBLEM

If a major U.S. corporation fails at strategic change and falls victim to the marketplace, there may be momentary consequences, but the economy rights itself and augers on. If there is failure in the implementation of change in homeland security, vulnerabilities go unaddressed, precious resources are squandered or misapplied, and the likelihood of a major catastrophe, for which the nation is unprepared, only increases as the nature of the threat changes and adapts faster than our ability to respond. The human, economic, and political consequences of such a failure could be enormous.

Managing risk is the cornerstone of everything that is homeland security. Successful implementation of risk management policy will be largely determined by how well DHS manages strategic change overall. Risk management policy implementation has thus far been problematic, and current efforts to advance the NIPP risk management framework only makes the situation that much more challenging. If DHS is to get risk management policy right, it must candidly assess its approach to managing strategic change and adjust accordingly. The stakes are just too high to do otherwise.

This thesis will add to the body of knowledge about the implementation of risk management for critical infrastructure protection and the various challenges involved in advancing strategic change in homeland security policy. It assesses implementation of the National Infrastructure Protection Plan (NIPP) risk management framework through the lens of change management theory, and makes recommendations for improvement in

DHS change management strategies to increase the chances of success. The lessons learned here may also be applied to other homeland security policy change initiatives.

The target consumers for this thesis research are the Secretary and senior leadership of DHS, the heads of DHS agencies with risk management responsibilities, and other government policy-makers, to include members of Congress with oversight responsibility for homeland security. This thesis is also intended to be of value to the community of research institutions, consultants and practitioners who are currently engaged in a wide variety of risk-management initiatives, not only within DHS but also across state and local government, academia, and the private sector.

D. ORIENTATION TO THE RESEARCH

Chapter II provides essential background on risk management and how it has evolved as homeland security policy, along with a review of basic definitions and concepts. It describes the fundamental risk formula that underlies most homeland security risk assessment methodologies in use, and the basic risk management cycle. The challenges associated with implementing homeland security risk management programs are also discussed, to include the uncertain nature of the threat. The need for new methods for assessing the risk of low probability / high consequence events are described, along with recognition of the interdependence of homeland security risk management efforts with the political and public policy processes. Related to the implementation of public policy are the challenges presented by our system of government and the concept of federalism. Chapter II closes with an overview of the agencies and stakeholders with equities in homeland security risk management policy and programs, and the complex web of relationships and dependencies that make up the risk management landscape.

Chapter III outlines current critical infrastructure protection and risk management efforts of the Department of Homeland Security (DHS). National critical infrastructure protection policy is reviewed, with special emphasis on the National Infrastructure Protection Plan (NIPP). Three critical elements of the NIPP, the Sector Partnership Model, Sector-Specific Plans, and the risk management framework are discussed in detail. The risk assessment and risk management efforts of DHS are summarized, to

include national-level and asset-based risk assessment, and the various risk assessment methodologies in use by DHS component agencies. The chapter ends with a summary of commentary on DHS risk management efforts by the GAO and other stakeholders, and a review of changing roles and responsibilities for risk management within the Department.

As this research centers on an evaluation of risk management implementation as strategic change in homeland security policy, Chapter IV provides a primer on change management, public policy, and complexity theories, as these may apply to such an evaluation. General concepts for managing strategic change are presented along with change management models that might assist homeland security leaders in planning for and managing major strategic change initiatives. The likely causes of failure in strategic change efforts are reviewed, and step-by-step guidelines for successful change management are discussed. As risk management represents public policy for homeland security, concepts for managing strategic change in a public policy context are also reviewed, culminating in a discussion of implementation efforts that have the potential for high ambiguity and high conflict, as is the case with homeland security risk management policy. Rounding out this chapter is an overview of organizations as open systems, followed by discussions of complexity and organizational networks.

Chapter V brings the research all together by integrating strategic change, public policy, and complexity theories into a hybrid template for evaluating the implementation of the NIPP risk management framework as strategic change in public policy. A set of questions are adapted from the literature and then applied to assess potential gaps in implementation efforts to date. Chapter VI summarizes the findings of this analysis and offers recommendations to DSH policymakers and planners for improvement.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. OVERVIEW OF RISK MANAGEMENT CONCEPTS

1. Society and Risk Assessment

The notion of risk has been with us ever since the dawn of man. It is rooted in our subconscious reasoning and behavior, and has been essential to our evolution and survival as a species. Carlo Jaeger et al., describe risk not only as the analytical lens through which we anticipate consequences, but also as a new consciousness and a new way for society to view the world and assess the tremendous uncertainties of our future, from nuclear holocaust to global climate change. Most significantly, these authors place risk at the center of rapidly growing and complex social and technological transformation, referring to it as the "imprimatur of our age."[4] According to Martin Shubnick, over the last half century there has been an explosive growth in the social and technical sciences and with it, commensurate growth in the way risk is analyzed. Once restricted to use by technically sophisticated experts and decision makers, risk analysis has gradually made its way into social and political discourse as government leaders and the public wrestle with ever more complex issues of public policy. This is especially true in programmatic and spending decisions related to national preparedness and homeland security. As the notion of risk as a criterion for public policy decision-making continues to expand, the way risk is evaluated, communicated, and used will require ever greater focus. [5]

A 2002 National Science Foundation (NSF) workshop on risk concluded that recent economic and technological advances have not only improved our quality of life, but have also produced new, more wide-ranging threats. This is especially true given what the report cites as increased interconnectedness of our physical, economic, social,

---

[4] Carlo Jaeger et al., *Risk, Uncertainty, and Rational Action* (London: Earthscan Publications Ltd., 2001), 13-15.

[5] Martin Shubnick, ed., *Risk, Organizations, and Society* (Boston: Kluwer Academic Publishers, 1991), 7-10.

and communications infrastructures, and the susceptibility to cascading effects where an impact in one part of a system can reverberate and amplify across the entire system. [6] It is thus not surprising that the federal government is increasingly applying consideration of risk in its evaluation of domestic hazards and security threats, and especially to the uncertainties and consequences associated with global terrorism and potential terrorist use of weapons of mass destruction (WMD). The NSF workshop report also stated that given the events of September 11, 2001, the public's perception of the vulnerabilities associated with this growing complexity and system interdependency has increased sharply. Not only is there greater consideration of risk internal to the government, but the continuing shadow of global terrorism, general fear and societal concern over government's ability to protect the safety and security of its citizens has brought the concept of risk ever further into the public consciousness. The statements of homeland security leaders, passionate political debate among members of Congress, and large-scale disasters like the Northeast Blackout of 2003, as well as hurricanes Katrina and Rita in 2005, have further stimulated this consciousness.

As described by Jaeger et al., risk assessment has its underpinnings in investment and insurance practices dating back a couple of centuries. However, these authors state that the broader and more systematic application of risk is a product of modern times, with the rapid growth in science and technology, and the vulnerabilities and dangers that tend to accompany such advances.[7] Modern risk assessment has developed over the last thirty years, beginning with design and safety studies in the nuclear power industry and various aerospace and military applications. By the 1970s its use had expanded to the setting of federal safety regulations for the chemical industry and establishing environmental standards for air and water quality, as well as the mitigation of toxic hazards (i.e., clean-up of environmentally contaminated sites). Its application to engineered systems soon followed, to include civil infrastructure. Today, risk assessment is successfully applied in a wide variety of areas spanning medicine, business finance, environmental conservation, industrial safety, the social sciences, and more recently,

---

[6] National Science Foundation, *Integrated Research in Risk Analysis and Decision Making in a Democratic Society* (Arlington, VA: National Science Foundation, July 2002), 16.

[7] Carlo Jaeger et al., *Risk, Uncertainty, and Rational Action*, 13-15.

natural disasters.[8] According to Yacov Haimes, what we now know as risk assessment, and the theories, quantitative tools, and methods employed by risk analysts, have steadily evolved over the years and are an amalgamation of contributions from a diverse range of professional disciplines to include statisticians, mathematicians, health scientists, systems analysts, and engineers. At the same time, he points out that social, behavioral, and organizational scientists have also contributed greatly to informing our understanding of the human dimensions of risk. This includes risk perception, risk communication, and strategies for building trust, resolving conflict, and dealing with organizational and institutional barriers to the application of risk in public policy and decision-making. [9]

A large and diverse community of risk analysts has been developing and applying systems-based risk methodologies for decades, and has had considerable success in identifying risks and assisting in the search for cost-effective solutions to mitigate them. In that time, risk assessment tools and approaches to risk management have become very sophisticated. Nonetheless, such tools remain largely inadequate in coping with the low-probability / high-consequence threats posed by the growing specter of global terrorism. The application of risk assessment to terrorism is a relatively new phenomenon and is posing both new opportunities and challenges.[10] As discussion of risk becomes an increasing part of our public consideration of homeland security policy and investment, and as involvement in the application risk assessment practices extends well beyond the Department of Homeland Security to state and local government and the private sector, we will need to consider new ways to involve a larger group of stakeholders in the evolution of these practices and in risk-based policy and decision-making. Building social trust, networking, and collaboration will be equally important considerations in the implementation of risk assessment policies and practices as risk theory and analytics.

---

[8] Rae Zimmerman and Vicki Bier, "Risk Assessment of Extreme Events" (paper presented at the conference Risk Management Strategies in an Uncertain World, Palisades, New York, April 12-13, 2002), 1.

[9] Yacov Haimes, "Roadmap for Modeling Risks of Terrorism to the Homeland," *Journal of Infrastructure Systems* (June 2002): 35-41.

[10] Philip Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, "The Challenge of Protecting Critical Infrastructure" (working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, October 2005), 7.

2. Risk Assessment as Homeland Security Policy

A call for terrorism risk assessment predates September 11, 2001, when, in May 1998, President Clinton issued *Presidential Decision Directive–63 (PDD-63) on Critical Infrastructure Protection.* That directive required the National Coordinator and the National Infrastructure Assurance Council to:

> …propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems… [and to]…offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards. [11]

In what was probably the first call for terrorism risk management before 9/11, Lieutenant Commander Thomas Rancich, USN, delivered a blistering commentary in *Proceedings* on the U.S. Navy's counterterrorism preparedness following the terrorist attack on the *USS Cole* in October of 2000. Rancich, recognizing that acts of terrorism are low-probability / high-impact events, recommended that the Navy establish a risk management program that would, in his words, "identify the most likely and highest impact possibilities and then detail actions taken / risks mitigated and actions not taken / risks not mitigated, along with a logical rationale for each" based on consideration of threat, probability, and political and fiscal restrictions [12]

In its landmark report, the 9/11 Commission recommended that "homeland security assistance should be based on an assessment of risks and vulnerabilities." In addition, the Commission recommended that the federal government should require each state "to provide an analysis based on the same criteria and to justify the distribution of funds in that state." [13] More importantly, the *Homeland Security Act of 2002* (Public Law 107-296), as the federal legislation that authorized the formation of the U.S.

---

[11] William Clinton, *Presidential Decision Directive-63 (PDD-63) – Critical Infrastructure Protection* (Washington, DC: The White House, 1998), 18.

[12] Thomas Rancich, "Combating Terrorism," *Proceedings of the United States Naval Institute* 126, no. 11 (September-October, 2000): 25-32.

[13] The 9/11 Commission, *The 9/11 Commission Report: Final Report of The National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton & Co, 2004), 396.

Department of Homeland Security (DHS), charged it with conducting critical infrastructure vulnerability and risk assessments as a core part of its mission. Specifically, the law requires DHS to:

> Conduct vulnerability and risk assessments of key resources and critical infrastructure to determine the risks posed by particular types of terrorist attacks, the probability of success of such attacks, and the feasibility and efficacy of various countermeasures.
>
> Integrate information, analyses, and vulnerability assessments by DHS or others to identify priorities for protective measures by DHS itself, other Federal, state and local government agencies and authorities, the private sector, and other entities.
>
> Develop a comprehensive national plan for securing the key resources and critical infrastructure (i.e., power, information technology, telecommunications, etc.) of the United States and the physical and technological assets that support such systems.
>
> Recommend measures necessary to protect key resources and critical infrastructure in coordination with other Federal agencies and in cooperation with State and local government agencies and authorities, the private sector, and others. [14]

In February 2003, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* reinforced the responsibility of DHS and other federal departments for pursuing risk-based approaches to critical infrastructure protection.

> The roles of the Federal lead departments and agencies are to assist state and local governments and private-sector partners in their efforts to: Identify and promote effective sector-specific, risk-management policies and protection practices and methodologies… [15]

Almost a year later, *Homeland Security Presidential Directive–7* (HSPD-7) directed the DHS secretary take the federal lead to establish uniform policies, approaches,

---

[14] *Homeland Security Act of 2002*, Public Law 107-296, 107th Congress, 2nd Session, (November 25, 2002), 2146.

[15] George Bush, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 17.

guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors, along with metrics and criteria for related programs and activities.[16]

On publishing the *Homeland Security Strategic Plan*, the DHS secretary outlined his intent to comply with the president's direction in HSPD-7 by issuing his own guidance to the department along these lines. Two key objectives in the plan state that DHS will "conduct and sustain a complete, current and accurate assessment of our Nation's infrastructure sectors and assets…" using risk-based analytic tools, and "…expand the Nation's community risk management capabilities and reduce the Nation's vulnerability to acts of terrorism and other disasters through effective vulnerability assessments and risk management programs." The plan describes risk management as a departmental priority in that "risks must be well understood, and risk management approaches developed, before solutions can be implemented. Managing risk is a continuous process that requires constant vigilance."[17]

According to Christine Wormuth, "assessing homeland security risks, which can stem from both terrorism and natural disasters, is an enormously complex undertaking, but is also a critical task if the Federal government seeks to marshal its finite resources effectively." [18] Since the formation of DHS, considerable resources have been expended in the development and application of risk assessment methodologies to the threat of terrorism by a variety of its own agencies, other federal departments, state and local governments and authorities, academia, and the private sector. However, these initiatives have yet to fully coalesce into the sort of coordinated national effort, under DHS auspices, called for in Public Law 107-296 or the department's own strategic planning documents for homeland security and critical infrastructure protection. Nonetheless, the importance of such an effort continues to be underscored by noted experts in the field, as

---

[16] George Bush, *Homeland Security Presidential Directive 7 (HSPD-7) - Critical Infrastructure Identification, Prioritization, and Protection*, 1.

[17] U.S. Department of Homeland Security, *Securing Our Homeland, U. S. Department of Homeland Security Strategic Plan* (Washington, DC: U.S. Department of Homeland Security, 2004), 10-54.

[18] Christine Wormuth,"*Homeland Security Risk Assessments: Key Issues and Challenges,"* Testimony before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives, (Washington, DC: November 17, 2005), 2.

expressed at various academic and professional conferences, in numerous studies on the matter, and in official testimony before various congressional committees.

In 2005, Wormuth offered that a national risk assessment could strengthen homeland security policy development and resource allocation in three important ways: 1) guiding homeland security planning as the basis for developing common interagency strategies to address specific homeland security challenges; 2) driving the resource allocation process by using risk assessments to not only set priorities for DHS but to also harmonize homeland security resource and policy decisions across the entire interagency, thus maximizing unity of effort; and 3) evaluating potential policy and programmatic options to direct where DHS and other agencies should invest marginal dollars in order to get greatest security return for the dollars invested.[19]

In her advice to Congress, Wormuth suggested that, despite formidable challenges, the development of robust homeland security risk assessments to guide planning and policy development are "absolutely worth the time and effort." Even if based on imperfect information, risk assessment, she said, provides an ability to examine the complexities of terrorism risk in a structured way. By focusing attention on the specific judgments made in the risk assessment process, issues can be "unpacked" to help decision makers better understand those issues and assess for themselves where differences of opinion among experts may lie before making policy decisions that could have profound implications for the security of the entire nation. [20]

Beyond the realm of federal policy-makers, Howard Kunreuther sees a broader set of challenges and the need for a wider community of involvement in the implementation of homeland security risk assessment policies and programs. Though successful implementation of risk assessment practices depends greatly on the development and use of new analytical tools, it also requires the formulation of a wide range of other supporting strategies to include methods for risk communication, economic incentives,

---

[19] Wormuth, "*Homeland Security Risk Assessments*, 4.

[20] Wormuth, "*Homeland Security Risk Assessments*, 3.

standards, and regulations for managing the risks identified. [21] Given the complexity involved, the yet underdeveloped and untested nature of emerging risk assessment methodologies, and the highly interdependent character of critical infrastructure and the responsibility for its security, new inter-governmental and public-private-academic partnerships are needed across a wide range of stakeholders.

3. Basic Definitions and Concepts

One of the most significant challenges in addressing the concept of risk in any context is the absence of a commonly accepted lexicon and set of professional practices, particularly as relate to the relatively new field of homeland security risk. As outlined by Robert Ross, there are many definitions of risk, each having utility within the context each was developed.[22] Though Ross cites 17 different definitions, he acknowledges that the list is far from exhaustive. For a contemporary definition, we can turn to Bilal Ayyub who defines risk as "the potential of losses and rewards resulting from exposure to a hazard or a result of a risk event." [23] Jaeger et al., define risk somewhat differently, as "a situation or event in which something of human value (including humans themselves) has been put at stake and where the outcome is uncertain." [24] Common throughout most of the definitions of risk are the notions of one or more threats, hazards, or unwanted events; a degree of perceived uncertainty about the probability or likelihood of the risk occurring; and a sense for the consequences in terms of cost or severity of loss. Despite the lack of a commonly accepted lexicon for risk, the following terms and definitions are used throughout this paper and are offered for sake of consistency: [25]

---

[21] Howard Kunreuther, "Risk Analysis" (working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, 2004): 9.

[22] Robert Ross, "Risk and Decision-Making in Homeland Security" (paper presented at the SRA 2006 Annual Meeting - Risk Analysis in a Dynamic World: Making a Difference, Baltimore, Maryland December 3-6, 2006), 4.

[23] Bilal Ayyub, *Risk Analysis in Engineering and Economics* (Boca Raton: Chapman & Hall/CRC, 2003), 35-36.

[24] Carlo Jaeger et al., *Risk, Uncertainty, and Rational Action*, 17-19.

[25] Vincent DeGiorgio, "Understanding Your Risk: The Risk Assessment Process, ArupRisk Consulting, June 26, 2002, http://www.nepss.org/presentations/Risk_26June02.ppt [Accessed July 31, 2007].

Risk Analysis – The development of a quantitative estimate of risk based on technical evaluation and mathematical techniques for combining estimates of incident likelihood and consequences.

Risk Assessment – The process by which results of a risk analysis are used to make decisions, either through relative ranking of risks and risk reduction strategies or through comparison with risk targets.

Risk Management – The ongoing process of planning, organizing, leading and controlling people, assets, and activities to minimize the potential consequences and/or probability of risks identified and appraised through risk assessment.

In outlining the analytical process, Haimes uses the terms "risk assessment" and "risk management" in a way that better conforms to the definitions of "risk analysis" and "risk assessment" used above. With this modification then, in conducting risk analysis as a prelude to assessment, the analyst works to answer the following three questions: 1) what can go wrong? 2) what is the likelihood that it will go wrong? and 3) what are the consequences if it does go wrong? Answers to these questions, he says, help identify, quantify, and evaluate risks and their potential impacts. Risk assessment as a prelude to risk management builds on this analysis, according to Haimes, by seeking answers to a second set of three questions: 1) what can be done and what options are available? 2) what are the trade-offs in terms of costs, benefits, and risks? and 3) what are the impacts of current management decisions on future options?[26] As security analyst B.D. Jenkins points out, "security measures cannot assure 100% protection against all threats." Though intelligence, risk, and security experts can evaluate potential threats, vulnerabilities, and consequences, only policy-makers and managers can make informed judgments on risk tolerance, priorities, and resource allocation as part of an ongoing risk management program to mitigate those risks. Given limited resources, this process works to strike a cost-effective balance between the impact of risks and the cost of solutions to manage them. [27] The risk analysis, assessment, and management process is iterative, and performance is measured against actual or relative risk reduction, with the resulting data used to inform each iteration and drive needed changes in the strategies employed.

---

[26] Yacov Haimes, "Roadmap for Modeling Risks of Terrorism to the Homeland," 35-41.

[27] B. D. Jenkins, "Security Risk Analysis and Management – Risk Analysis Helps Establish a Good Security Posture; Risk Management Keeps It That Way," (Countermeasures, Inc., 1998), 1-2.

Henry Willis et al., of RAND view terrorism risk as having three fundamental components: the threat to a target, the target's vulnerability to the threat, and the consequences should the target be successfully attacked. [28] The threats to a target can be measured as the probability that a specific target will be attacked, in a specific way, during a specified period. The example they cite is the estimated probability that a city's football stadium will be subject to attack with a radiological dispersal device. They define vulnerability as an estimate of the probability or likelihood that damage will occur from a given threat. Damages are expressed as fatalities, injuries, property damage, and/or direct and indirect economic loss. The last of the three components is an estimate of consequences. This is assessed as the type and magnitude of damage resulting from a successful terrorist attack. Risk is a function of all three components: threat, vulnerability, and consequence. Simply put, risk is the product of the vulnerability and consequence of a risky event or threat.

Risk = Threat x Vulnerability x Consequence [29]

According to the NSF, "the last few decades have witnessed an explosion of innovative empirical, theoretical, and analytic methods and tools for analyzing risks and for making decisions under conditions of uncertainty." [30] This is no less true for the relatively recent analytical science of terrorism risk. Nonetheless, this basic formula lies at the heart of most of the methods for analyzing terrorism risk that are now emerging. Despite the claims to the contrary by some developers and consultants, this common formula provides the fundamental basis for realizing the common, compatible, and integrated risk management framework called for by the president, the Congress, and DHS strategy documents to date.

---

[28] Henry Willis, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby. *Estimating Terrorism Risk* (Santa Monica CA: RAND Center for Risk Management Policy, 2005), xvi.

[29] Ibid., 10.

[30] National Science Foundation, *Integrated Research in Risk Analysis and Decision Making in a Democratic Society*, 5.

4. Managing Risk

According to the Government Accountability Office (GAO), the basic risk management process is divided into five phases: (1) setting strategic goals and objectives while determining constraints; (2) assessing the risks; (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and the results achieved (see Figure 1). GAO cautions that the application of risk management to homeland security is new, and the process "will likely evolve as processes mature and lessons are learned."

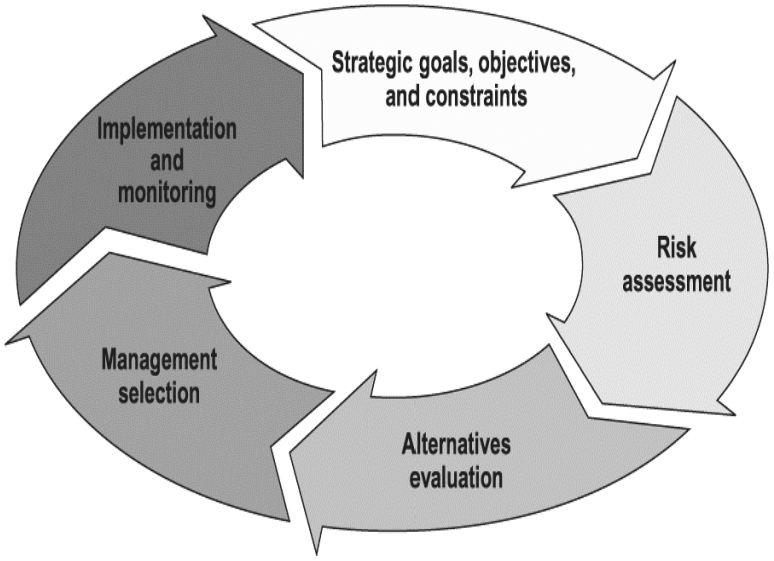

Figure 1. GAO Risk Management Framework. [31]

In proposing an approach to homeland security risk management, researcher Bin Jaing notes that the essence of risk analysis is to outline risk outcomes and probability distributions that frame risk management decisions for policymakers and managers. [32] Citing the work of Preston Smith, he describes a risk map as one of the simplest tools

[31] Government Accountability Office, *Homeland Security - Applying Risk Management Principles to Guide Federal Investments*, 8-9.

[32] Bin Jiang, "Risk Management and the Office of Homeland Security's Antiterrorism Tasks," *Online Journal of Peace and Conflict Resolution* 4, no. 2 (2002): 30-36.

used by analysts in this regard.[33] A risk map portrays the core elements of the risk equation in a way that facilitates decision-maker understanding of the relative urgency of risks, both individually and in relationship to one another. It is presented here as a basic way to better illustrate for the reader what lies at the core of risk management thinking.

Figure 2 is an adaptation of Smith's risk map, and is an example of an approach used to frame terrorism security risk decision-making at the author's own agency – the Port Authority of New York and New Jersey. It has also been successfully applied at over forty major transportation agencies across the country and elsewhere. The vertical axis represents likelihood as a function of vulnerability, and the horizontal axis represents consequence. Points are plotted on the risk map using a relative scale, derived from the risk arithmetics, for each target (i.e., critical infrastructure) and attack type (threat). This couplet of target and attack type represents an individual risk (i.e., biological attack against an urban transit system). Once all risks are plotted, a curved line of constant risk may be drawn to provide an arbitrary risk threshold. Any risk above that threshold may be identified as a priority for risk management action. [34] Though risks below the line may still be managed, they might not receive priority attention or resources. As indicated in Figure 2, countermeasures may be employed to lessen the likelihood by hardening the target, or the consequence by improving response, or some combination of the two.

[33] Preston Smith, "Managing Risk as Product Development Schedules Shrink," *Research Technology Management* 42, no. 5 (September / October, 1999): 25-32.

[34] Bin Jiang, "Risk Management and the Office of Homeland Security's Antiterrorism Tasks," 31-33.

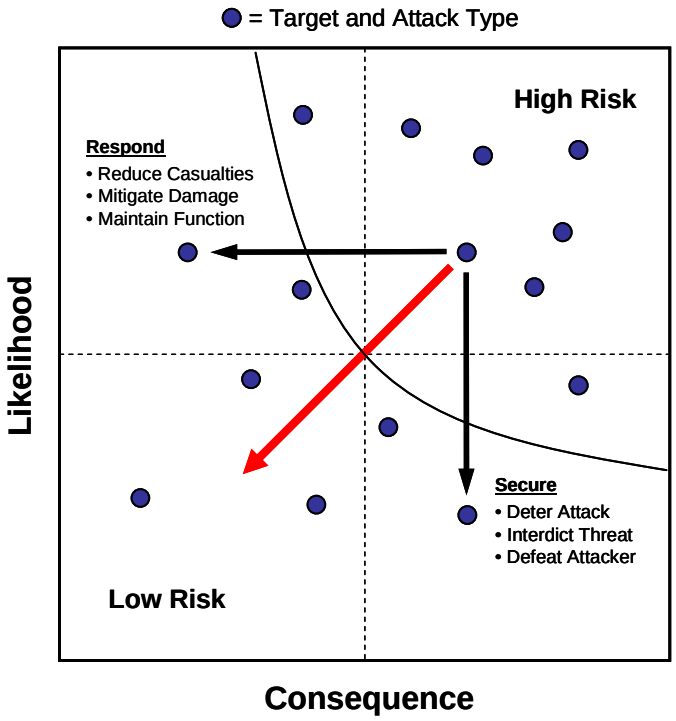

Figure 2. Terrorism Risk Map.

In referencing Smith, Jaing notes that the risk threshold line is set according to the risk tolerance of decision makers and can be moved higher or lower with changes in circumstances, to include changes in threat posture, availability of resources, and the assessed impact of previous risk reduction efforts. Moved lower, more risks receive priority attention with an expected commensurate reduction in the overall risk profile but with a corresponding increase in cost; or, if resources are fixed, a smaller investment available per target. Moved higher, a greater concentration of resources may be applied to a fewer number of risks, but with potentially greater effect. Howard Kunreuther refers to a similar risk mapping approach as an "Exceedance Probability (EP) Curve."[35] Whatever the method of presentation, the ultimate purpose of risk management is to drive down the risk profile of as many of the high priority targets as possible, as far as possible.

[35] Howard Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," *Risk Analysis* 22, no.4 (2002): 655-664.

Strategies are developed and executed based on the decisions made, risk reduction is then measured, and adjustments are implemented given the acceptability of risks identified. [36]

Risk mapping is not the only technique available. Decision-making can be guided by something as simple as a lineal ranking of the priority risks identified or the use of other more sophisticated analytical and modeling tools to more discretely assess how to achieve greatest risk reduction and cost benefit potential. One such technique, particularly well suited to networked systems, is the Model-Based Vulnerability Analysis (MBVA) technique. MBVA provides decision makers with answers to such questions as, how do these targets relate to one another? What specific targets among them are most worth protecting? How much will it cost? Developer Ted Lewis describes it as the only known method that combines asset identification and quantitative analysis to reach a policy decision on how to most cost effectively mitigate risk. [37] Regardless of the techniques used, the process of risk management is never complete. The threats to be guarded against are always changing and adapting, and new vulnerabilities are constantly emerging. It is a never-ending process and likely will remain so for some time to come.

If a national risk management framework is to be implemented to "buy-down" homeland security risk, there must be a broad-based national effort to develop standardized practices, procedures, and analytical tools to permit the integration and assessment of risk across industry sectors and between levels of government. The challenges to doing so will need to be identified and overcome.

B. THE CHALLENGES OF MANAGING SECURITY RISK

1. Nature of the Threat and Infrastructure at Risk

In assessing terrorism risk to private-sector infrastructure, Erwann Michel-Kerjan and Burkhard Pedell state that though catastrophic events are not new, the nature and scale seem to have changed in recent years. In addition to the terrorist attacks of

---

[36] George Baker, "A Vulnerability Assessment Methodology for Critical Infrastructure Sites" (paper presented at R&D Partnerships in Homeland Security, Boston, Massachusetts, April 27-28, 2005), 2.

[37] Ted Lewis, *Critical Infrastructure Protection In Homeland Security: Defending a Networked Nation* (Hoboken, NJ: John Wiley & Sons, Inc., 2006), ix-x.

September 11, 2001, they cite the Northeast Blackout of 2003, the Indian Ocean Tsunami in 2004, and the hurricanes that ravaged the Gulf Coast in 2005, all resulting in an "unprecedented scale of devastation." [38] They point out that the character of terrorism has also changed dramatically, with the emergence of extremist, religious-based terrorist groups and an age of "mega-terrorism." A 2007 National Intelligence Estimate (NIE) concerning the terrorist threat puts the issue much more bluntly: [39]

> The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland.
>
> Al-Qa'ida is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population.
>
> Al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

A report by the NSF indicates that unlike traditional risk analysis, terrorism risk that arises from intentional actions designed to take lives and create social and economic disruption involve "intelligent actors" capable of changing their strategies and tactics to take advantage of perceived weaknesses. [40] Philip Auerswald et al., call this terrorist behavior "adaptive predation." Accordingly, they suggest that the likelihood and consequence of a terrorist attack are not determined by chance, but by a mix of strategies and counterstrategies, developed by various stakeholders (i.e., attackers and defenders), that are constantly changing over time. Such "dynamic uncertainty makes the likelihood of future terrorist events extremely difficult to estimate and increases the difficulty of

---

[38] Erwann Michel-Kerjan and Burkhard Pedell, "How Does the Corporate World Cope with Mega-Terrorism? - Puzzling Evidence from Terrorism Insurance Markets" (working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, January 15, 2007), 4.

[39] Office of the Director of National Intelligence, *National Intelligence Estimate - The Terrorist Threat to the US Homeland*, 6-7.

[40] National Science Foundation, *Integrated Research in Risk Analysis and Decision Making in a Democratic Society*, 19.

measuring the economic efficiency of public policies and private strategies." [41] Detlof von Winterfeldt reinforced this point in testimony before Congress when he suggested that, in contrast to risks from natural hazards and engineered systems that are "neutral" in character, terrorists are adversaries who deliberately seek out vulnerabilities and adjust their actions in response to any defenses that might be erected. The non-random nature of terrorism, he says, greatly complicates risk assessment, and this requires development of new tools for analysis. [42]

As Kunreuther et al., see it, dynamic uncertainty and the changing nature of terrorism risk over time reflects an important difference from natural hazards. [43] One cannot induce an earthquake or a hurricane, for example; these events happen by chance. They also opine that mitigation measures can more easily be implemented to lessen the consequences of natural disasters. When it comes to reducing terrorism risk, it is unknown who the perpetrators are, what motivates them, how they will select their method of attack, or what their target will be. Thus, it is difficult to know what counter-measures to employ, where, and when. Kunreuther suggests that, given the small likelihood of such events happening at any given time, place, or level of consequence, government must otherwise invest significant funds to protect a wide range of potential targets and provide public reassurance. [44] This may not be the most productive or cost effective way to use limited national resources, and in the long term it is not sustainable.

Having been designed for efficiency, convenience, and competitiveness, Yacov Haimes describes the nation's infrastructure as open and accessible, interconnected and vast, and intertwined with society and the global economy. The design and function of that infrastructure is driven largely by the demands of a highly diverse range of owners, operators, and users, and it is controlled and secured by thousands of individuals, private-

---

[41] Philip Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, "The Challenge of Protecting Critical Infrastructure," 8.

[42] Detlof von Winterfeldt, *Information Sharing and Terrorism Risk Assessment Committee on Homeland Security*, Testimony Before the Subcommittee on Intelligence, United States House of Representatives (Washington, DC: November 17, 2005), 1-2.

[43] Howard Kunreuther, Erwann Michel-Kerjan, and Beverly Porter, "Assessing, Managing and Financing Extreme Events: Dealing With Terrorism," (working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, November 20, 2003), 7.

[44] Howard Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," 655-664.

sector companies, and state and local governments.[45] These factors make the nation's infrastructure vulnerable to attack. As the NSF risk workshop report underscores, the very strength of the nation — it is efficient, interdependent, highly integrated, and sophisticated civil and economic infrastructure — is its greatest potential weakness in that there are too many valuable targets and not enough resources to fully protect them all. [46]

Homeland security risk is not just a matter of analyzing terrorist threats. Michel-Kerjan points out that "of the 20 most costly catastrophes between 1970 and 2005 (a thirty-five-year period), ten of them occurred in just the last five years, and nine of these in the United States. Hurricane Katrina alone inflicted nearly $150 billion of economic damage…and…major natural catastrophes worldwide inflicted $230 billion in economic damage in 2005, twice as much as in 2004, the previous record holder."[47] Both terrorist attacks and natural disasters have the potential to cause extreme losses, and there are a few similarities in the measures that can be taken to mitigate consequences as well as how disaster response is managed. However, there are also some significant differences to be taken into account that may impact the approaches used to assess risk. According to Kunreuther et al., these differences include the availability of historical data, the ambiguity of the risks involved, limits on information sharing, the potential to influence the probability of an event, and differences in the impact of mitigation measures. [48] New methods are needed to assess terrorism and all hazards risks in an integrated way.

---

[45] Yacov Haimes, "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures," *Risk Analysis* 26, no. 2 (April 2006): 293-296.

[46] National Science Foundation, *Integrated Research in Risk Analysis and Decision Making in a Democratic Society*, 83.

[47] Erwann Michel-Kerjan "Disasters and Public Policy: Can Market Lessons Help Address Government Failures?" (working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, January 2007), 3.

[48] Howard Kunreuther, Erwann Michel-Kerjan, and Beverly Porter, "Assessing, Managing and Financing Extreme Events: Dealing With Terrorism," 6.

2. Need for New Methods and Common Practices

Regardless of the type of catastrophic risk, to make the hard choices necessary to help policymakers determine where to invest limited resources, George Baker states that there is a need for a "common, repeatable, systematic methodology" to understand vulnerabilities and comparative risks.[49] Following a conference of leading academic experts on risk in 2002, Howard Kunreuther and Arthur Lerner-Lam concluded that although there are well-developed models for low-probability / high-consequence events like natural disasters, there is still considerable uncertainty regarding these risks. Given that uncertainty, they highlighted the challenge of assessing risk concerning threats even more uncertain and ambiguous, like those associated with potential terrorist attacks. [50] At that same conference, Rae Zimmerman and Vicki Bier recognized that current practices are based on flexible, systems-oriented methods capable of being adapted to a variety of risk conditions. However, they agreed that traditional methods are challenged when applied to extreme events like terrorism, and thus require improvement. [51]

In the NSF risk workshop report, Paul Slovic suggested that "some species of trouble — such as terrorism — greatly strain the capacity of quantitative risk analysis." He acknowledged that, at least in 2002, current risk assessment models, if applied to such hazards, were too crude to permit precise and accurate predictions of risk.[52] In that report, Susan Cutter characterized the knowledgebase in this area as fragmented and insufficient to advance an understanding of terrorism or hazards risk assessment, citing the need for new approaches and increased collaboration among the risk, disaster, and hazards research communities.[53] The NSF workshop report, in part, concluded that "unnecessary divisions between risk analysts, decision scientists, and hazards researchers, as well as more traditional disciplinary divisions have impeded scientific progress."

---

[49] George Baker, "A Vulnerability Assessment Methodology for Critical Infrastructure Sites," 2.

[50] Howard Kunreuther and Arthur Lerner-Lam, *Risk Assessment and Risk Management Strategies in an Uncertain World*, 6.

[51] Rae Zimmerman and Vicki Bier, "Risk Assessment of Extreme Events", 18-19.

[52] National Science Foundation, *Integrated Research in Risk Analysis and Decision Making in a Democratic Society*, 72-73.

[53] Ibid., 37-38.

Accordingly, the NSF report called for new inter-disciplinary and multidisciplinary research across the engineering, information science, natural science, and social science domains. [54] The need for an interdisciplinary approach extends to risk-based public policy and decision-making as well. This is an issue that is even more acute in the relatively new arena of homeland security policy and decision-making. Peter Orszag, another participant at the NSF workshop, quoted a senior federal official as saying that an "insufficient stock of off-the-shelf research on homeland security exists to inform policy-making."[55] The 2002 NSF report found that analytic tools and findings produced by those involved in the risk sciences had not been used in policy decision-making as much as they could have been. [56] Clearly, integration and cross-fertilization of perspectives across a range of expert communities is needed to advance new methods for risk assessment of terrorism and other catastrophic events, and should be a priority.

In a 2005 assessment of the state of terrorism risk assessment as applied to homeland security grant programs, Henry Willis et al., of RAND found that there was still no consistent and shared definition of terrorism risk or agreement on the methodologies to be applied to assess that risk, leaving stakeholders with different understandings of the concept and its application. Though they found agreement among many of those stakeholders that DHS grants should reflect the measure of risk to which different jurisdictions are exposed, there was no consensus at that time by which methodology such risk should be determined. In addition, there was, according to their research, no existing framework to guide the selection and combination of risk indicators. Nor did they find much effort directed toward how different risk estimates change with respect to a wide range of different assumptions about terrorist threats and capabilities. In their view, there was also an absence of information about how to measure the effectiveness of investments to reduce terrorism risk. [57] Though much has changed since 2005, the need for a "common, repeatable, systematic methodology" remains.

---

[54] National Science Foundation, *Integrated Research in Risk Analysis*, 19.

[55] Ibid., 61.

[56] *Ibid*., 7.

[57] Henry Willis, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby. *Estimating Terrorism Risk*, vii.

According to GAO research in early 2007, DHS has not yet implemented a comprehensive risk management approach, as required by Homeland Security Presidential Directive 7 (HSPD-7). The agency cautions that, as DHS components mature their individual risk management efforts, "the need for consistency and coherence becomes even greater."[58] In the absence of such guidance, the GAO sees the potential for fragmentation and conflict only increasing. "Efforts to establish guidance to coordinate a risk-based approach…have been hampered by organizational restructuring. The challenges that remain are substantial and will take time, leadership, and attention to resolve."[59] However, these challenges go well beyond DHS itself. The diversity and range of approaches, and the source, sequence, and timing of their development and implementation have resulted in a wide array of conceptual frameworks, incompatible methodologies, conflicting language, and confusion, not only among policy-makers and other stakeholders, but among security risk practitioners, both within and outside DHS.

With specific regard to critical infrastructure protection, a major step forward was taken with the issuing of the National Infrastructure Protection Plan (NIPP) in 2006. For the first time, the NIPP lays out a conceptual risk management framework that describes the general steps in the process and the roles and responsibilities of those involved.[60] The NIPP acknowledges that a variety of different methodologies are already in use by owners and operators of critical infrastructure. However, it does not address the considerable institutional challenges associated with potentially incompatible approaches, but instead establishes only minimum baseline criteria. Though it serves as an overarching plan for critical infrastructure risk management, it does not outline how congruence will be achieved across a nationwide community of risk and security analysts, critical infrastructure owners and operators, and federal, state, and local government agencies. Nor does it describe how nationwide technical and professional standards and practices will be developed and maintained in this new and vital field.

---

[58] William Jenkins, *Homeland Security - Applying Risk Management Principles To Guide Federal Investments*, testimony before the Subcommittee on Homeland Security, Committee on Appropriations, U.S. House of Representatives (Washington, DC, Government Accountability Office, February 7, 2007), 29.

[59] Ibid., 29.

[60] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, (Washington, DC: U.S. Department of Homeland Security, 2006) 29-50.

3. Interdependence with the Public Policy Process

It is difficult enough to build a national risk management framework among like-minded risk and security analysts within DHS, but it is even more challenging to extend it to state and local public safety agencies and private-sector security organizations. An added element of complexity is to involve elected officials, policy-makers, industry executives, and perhaps even the general public into the discussion of risk-based homeland security policies and programs. Risk management must be integral to the policy development and decision-making process if it is to be effective. This occurs across at least fours layers of public policy discourse: a) among DHS, the president, and the Congress; b) within and among individual DHS agencies; c) among DHS and other federal, state and local agencies, and the private-sector; and d) with the American people, both as a body and through their elected representatives. The nature and purpose of that discourse is different at each layer; nonetheless, challenges concerning confidentiality, risk characterization, risk communication, and public trust permeate all four.

During the 2002 NSF risk workshop, Ralph Keeney, in reflecting on the fundamental objectives of risk analysis, posited that the adequacy of risk methodologies is not the relative weak point for achieving those objectives. In his view, "our major weaknesses have to do with effectively applying what we know and effectively communicating the knowledge we have and insights that we can get from applying our knowledge." [61] Paul Slovic points out that "risk assessment is a complex discipline, not fully understood by its practitioners, much less the lay public." [62] Even within more traditional risk assessment applications, there is much debate over terminology and techniques, and this is certainly true of risk assessment for terrorism. According to Slovic, the limitations of analysis and disagreements among risk experts exacerbate the already adversarial climate that often surrounds much discussion of risk. He cautions that risk assessments are constructed from theoretical models that are based on assumptions and subjective judgments, and so communicating risk as a part of the public policy discourse "means finding comprehensible ways of presenting complex technical material

---

[61] National Science Foundation, *Integrated Research in Risk*, 51.

[62] Paul Slovic, "Informing and Educating the Public about Risk," in *The Perception of Risk* (London: Earthscan Publications Ltd, 2000), 182-183.

that is clouded in uncertainty." [63] The remarks of Keeney and Slovic suggest that as much effort should go into developing, applying, and communicating risk information as goes into theory and methodology. This has important implications for risk assessment as public policy, and the nature of the public policy process that supports it.

The Organization for Economic Cooperation and Development (OECD) is dedicated to the sharing of best practices in domestic and international policy. OECD recognizes the critical importance of focusing on the process of effective risk policy formulation, particularly pertaining to natural disasters, terrorism, and the failure of critical infrastructures. From its perspective, government officials must not only assess, appraise, and manage risk in an effort to develop and implement suitable responses, but must also coordinate action among a variety of stakeholders and agencies; reconcile differing perspectives and goals; consider legal and historical context; and inform the public about the nature of risks and tradeoffs. When viewed from this perspective, risk management is more about the process of decision-making and policy development than it is about the technical complexity of risk analysis and assessment practices. [64]

In its guidance on risk management, the Treasury Board of Canada emphasizes the need to effectively integrate risk into the public policy process, taking a consultative precautionary approach to improve predictability, credibility, and consistency of risk-based policy across the government. Internal to the government, risk communication promotes action, continuous learning, innovation, and teamwork. Proactively involving elected officials creates opportunities for the exchange of different perspectives and helps ensure more informed, relevant, and effective policy options. The guidance describes such risk communications as including "issue identification and assessment; analysis of the public environment (including stakeholder interests and concerns); development of

---

[63] Paul Slovic, "Informing and Educating the Public about Risk," in *The Perception of Risk* (London: Earthscan Publications Ltd, 2000), 182-183.

[64] Organization for Economic Cooperation and Development, "Risk and Regulatory Policy", http://www.oecd.org/document/23/0,3343,en_2649_34141_37551127_1_1_1_1,00.html [Accessed July17, 2007].

consultation and communications strategies; message development; working with the media; and monitoring and evaluating the public dialogue." [65] See Figure 3.

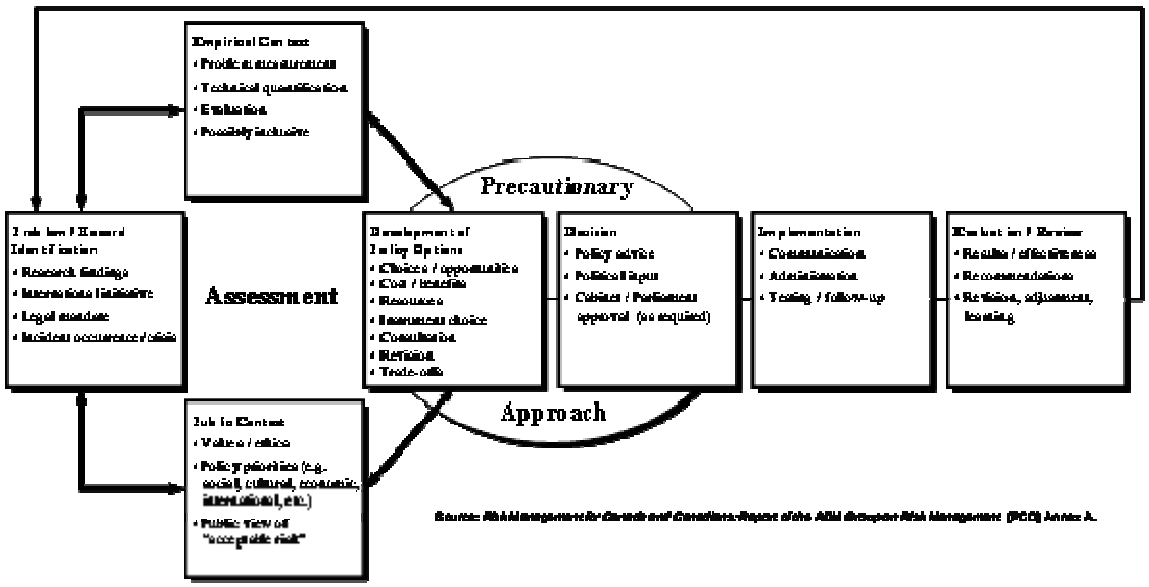

Figure 3. Risk Management in Public Policy: A Decision-Making Process. [66]

Peter Adler and Jeremy Kranowitz see safety and security risks, and especially those perceived as a "possible erosion of civil liberties," as involving the potential for differing perceptions of risk, risk tolerance, and/or social values, possibly causing conflict among different segments of society. They suggest that identifying the types of demands that are faced by different stakeholders is "one of the key first steps to communicating and managing risk and building trust with the public." [67] Facilitating the public policy discourse on homeland security risk will require maintaining a careful balance between need-to-know and need-to-share and acknowledging the imperative to proactively manage the involvement of policy-makers, elected officials, stakeholders, and the public. A national framework for risk management must therefore include a robust public policy

---

[65] Treasury Board of Canada, *Integrated Risk Management Framework* (Ottawa, Canada: Treasury Board of Canada, April 2001), 25-33.

[66] Ibid., 29.

[67] Peter Adler and Jeremy Kranowitz, *A Primer on Perceptions of Risk, Risk Communication and Building Trust* (February 2005), 5.

development and risk communications strategy. The National Research Council defines risk communications as "a continuing discussion among risk assessors, risk managers, and stakeholders from start to finish." [68]

4. Federalism and Distributed Responsibility

In his introduction to the *National Strategy for Homeland Security*, President Bush makes the point that the strategy is national and not just federal in character. The strategy emphasizes that homeland security is a "shared responsibility" stretching across the Congress, federal, state and local government, the private-sector, and the American people. That strategy is based on the nation's tradition of federalism and limited government, and is rooted in the Tenth Amendment to the U.S. Constitution which reserves to the states and to the people "all power not specifically delegated to the Federal government." It is assumed that, given these principles, organizations outside the federal government will, in many cases, need to take a lead role in implementing key elements of the strategy. In the context of this sharing of power and responsibility, the strategy acknowledges that our nation's governance is based on an "overlapping structure" of 87,000 federal, state, and local jurisdictions. Accordingly, a key challenge in implementing homeland security strategy will be to develop "complementary systems that avoid duplication," thus placing a premium on "collaboration and coordination," not only among layers of government, but with business and industry, and other non-governmental organizations as well. [69]

The National Strategy for Homeland Security outlines six critical mission areas: intelligence and warning, border and transportation security, domestic counter-terrorism, defending against catastrophic terrorism, emergency preparedness and response, and protecting critical infrastructure. [70] While the strategy sees the first four as dominantly federal responsibilities, the last two involve significant roles for the private sector and

---

[68] National Research Council, *Scientific Review of the Proposed Risk Assessment Bulletin from the Office of Management and Budget* (Washington, DC: National Academies Press, 2007),109.

[69] U.S. Department of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: U.S. Department of Homeland Security, 2002) iiv-11.

[70] *National Strategy for Homeland Security*, 4.

state and local governments respectively. Though the strategy is clear in its statement that state and local governments have primary responsibility for funding, preparing, and operating capabilities for emergency response, it is less clear concerning state and local responsibility for homeland security prevention activities across the other mission areas, especially the division of responsibility between federal and state governments in dealing with the private sector to address infrastructure protection needs.

With specific regard to critical infrastructure protection, the strategy describes the Department of Homeland Security's responsibility to develop and coordinate implementation of a comprehensive national plan to "provide a methodology for identifying and prioritizing critical assets, systems, and functions, and for sharing protection responsibility with state and local government and the private sector." It also outlines the federal organization mandate for "interacting with particular critical infrastructure sectors," assigning responsibility across major federal departments and agencies. [71] The strategy asserts that the private sector has the "primary and substantial responsibility" to address public safety risks posed by their industries and that such responsibility naturally comes with "sound corporate governance." While the strategy cites the importance of tapping the potential of the private sector to support national homeland security efforts, it also states that government should only fund those activities that are not supplied, or are inadequately supplied in the marketplace, indicating that sufficient economic incentives exist for the private sector to provide itself with the security protection needed. [72]

The *Homeland Security Act of 2002* authorized the creation of DHS and assigned it specific responsibilities related to the protection of the nation's critical infrastructure. This included recommending "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with state and local government agencies and authorities, the private sector, and other entities." [73] In response, DHS issued the NIPP,

---

[71] *National Strategy for Homeland Security*, 31-33.

[72] Ibid., 64.

[73] *Homeland Security Act of 2002*, 2146-2147.

which outlines roles and responsibilities for carrying out critical infrastructure and key resource protection (CI/KR) activities. In addition to its own overarching role to coordinate a national critical infrastructure protection framework, and the assignment of sector-specific responsibilities to various federal agencies, the NIPP assumes roles for non-federal partners as well, creating an extensive network of inter-governmental and public-private sector relationships and interdependencies to carry out the plan. The NIPP assumes that:

> State, local, and tribal governments will develop and implement a CI/KR protection program as a component of their overarching homeland security programs.
>
> Boards, commissions, authorities, councils, and other entities will perform regulatory, advisory, policy, or business oversight functions related to various aspects of CI/KR operations and protection within and across sectors and jurisdictions.
>
> Private sector owners and operators will undertake CI/KR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to the Federal government.
>
> Homeland Security Advisory Councils will provide advice, recommendations, and expertise to the government regarding protection policy and activities.
>
> Academia and research centers will provide CI/KR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs. [74]

A symposium sponsored by The Rockefeller Institute of Government in 2003 focused on the issue of federalism and its implications for the role of state and local governments in homeland security. Participants noted that there is no clear intergovernmental division of labor around most homeland security activities. Though border protection is primarily a federal activity, responding to an incident after it has occurred is a local responsibility. On the other hand, infrastructure protection is more complicated. "Most vital infrastructure is owned by the private sector and regulatory responsibility for some industries is divided between levels of government in frequently complicated ways. In other industries, it is unclear that any public agency has the legal

[74] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 1-2.

authority to set and enforce security standards." [75] Participants concluded that considerable collaboration and cooperation is required; a significant challenge given traditional federal concerns of money, turf, and power. In a 2006 review of homeland security funding programs, Peter Eisinger demonstrated that these concerns are still valid, and cited the complexities involved in finding an effective balance in the loose arrangement of highly decentralized homeland security partnerships under our current system of federalism. [76]

C. A COMPLEX INSTITUTIONAL LANDSCAPE

1. U.S. Department of Homeland Security Agencies

National Protection and Programs Directorate (NPPD) – NPPD is the DHS organization responsible for championing overall risk-reduction efforts to counter both physical and cyber threats. Within NPPD there are three key organizations that have special importance to risk assessment policy implementation. These are the Office of Infrastructure Protection (OIP), Office of Risk Management and Analysis (RMA), and Office of Intergovernmental Programs (IGP). [77] Another important organization is the Homeland Security Threat and Risk Analysis Center (HITRAC), a joint agency of NPPD and the DHS Office of Intelligence and Analysis (OIA).

Office of Infrastructure Protection (OIP) – OIP facilitates the identification, prioritization, coordination, and protection of CI/KR in support of federal, state, local, territorial, and tribal governments, as well as the private sector. It communicates threats, vulnerabilities, incidents, potential protective measures, and best practices to security partners, and is responsible for advancing implementation of the National Infrastructure Protection Plan (NIPP). In accordance with the NIPP, OIP maintains a national CI/KR sector governance and information-sharing framework composed of industry sector

---

[75] The Rockefeller Institute of Government, *The Federalism Challenge - The Challenge for State and Local Government* (Albany, NY: The Rockefeller Institute of Government, June 2003) VI-VII.

[76] Peter Eisinger, "Imperfect Federalism: The Intergovernmental Partnership for Homeland Security," *Public Administration Review* 66, no. 4 (July/August, 2006): 537-545.

[77] U.S. Department of Homeland Security, *Directorate for National Protection Programs,* http://www.dhs.gov/xabout/structure/editorial_0794.shtm [Accessed July 20, 2007].

leaders, CI/KR owners and operators, and other key public and private sector stakeholders. As part of its NIPP implementation efforts, OIP is also advancing risk assessment policies and methodologies to guide CI/KR protection plans and programs. [78]

Office of Risk Management and Analysis (RMA) – RMA leads DHS efforts to establish a common framework for overall management and analysis of homeland security risk. It also serves as the Department's executive agent for national-level risk management analysis standards and metrics. Within its charge is to develop and embed a consistent, standardized approach to risk, and develop a coordinated, collaborative approach to risk management by leveraging and integrating risk expertise across DHS components and external stakeholders. RMA also assesses DHS-level risk performance to ensure that programs are measurably reducing risk across the country. [79]

Office of Intergovernmental Programs (IGP) – IGP's mission is to promote an integrated national approach to homeland security by ensuring, coordinating, and advancing federal communication and interaction with, and acting as an advocate for, state, local, tribal, and territorial governments. It also coordinates and maintains awareness of various bilateral communications occurring regularly throughout DHS and between the Department's agencies and its state, local, tribal, and territorial partners. [80]

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) – HITRAC has a dual reporting relationship and serves both OIP and the Office of Intelligence Analysis (OIA). It bridges the work of the intelligence community via OIA, infrastructure specialists within OIP, and other experts to identify sector-specific vulnerabilities and consequences of attack. It then translates this work into strategic-level risk assessments for use by federal, state, and local authorities, and the private sector. HITRAC receives information about critical infrastructure through Information Sharing and Analysis Centers (ISACs) and through direct contacts with private and public sector

[78] U.S. Department of Homeland Security, *Directorate for National Protection Programs.*

[79] Ibid.

[80] U.S. Department of Homeland Security, *Directorate for National Protection Programs.*

infrastructure owners established by OIP. [81] HITRAC is assuming an increasing role in managing CI/KR risk assessments in support of OIP and its implementation of the NIPP.

Science and Technology Directorate (S&T) – S&T is responsible for identifying, enabling, and transitioning new state-of-the-art technology to DHS components and the public safety agencies of state, local, tribal and territorial governments. Within S&T, two units have specific responsibilities that are germane to the focus of this paper. The Infrastructure / Geophysical Division is responsible for technology projects focusing on critical infrastructure threats and vulnerabilities. The Office of Operations Analysis manages risk analysis projects and oversees the Homeland Security Institute (HSI). HSI is a Federally Funded Research and Development Center (FFRDC), which, among other things, conducts a range of studies to support risk-based decision-making within DHS. [82]

United States Coast Guard USCG – As a part of its homeland security role, the Coast Guard has a special responsibility to protect the flow of commerce, the nation's marine transportation system, and especially its ports, from terrorism. As a part of this responsibility, the Domestic Port Security Evaluation Division conducts a regular program of port-wide security assessments in support of Federal Maritime Security Coordinators (FMSCs). FMSCs (the Coast Guard Captains of the Port) work with state and local agencies and private sector maritime interests to implement risk-based port-wide security programs. To aid these efforts, the Coast Guard has developed a port security risk assessment methodology used to establish risk-based profiles of potential port vulnerabilities, and to guide local port security planning and operations. [83]

Federal Emergency Management Agency (FEMA) – The Risk Analysis and Risk Reduction branches within the Mitigation Directorate of FEMA apply a variety of tools for all-hazards risk assessment and work with other federal, state, and local agencies to

---

[81] Melissa Smislova, *Terrorism Risk Assessment at the Department of Homeland Security,* testimony before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment (November 17, 2005).

[82] U.S. Department of Homeland Security, *Science & Technology – Strategy to Make the Nation Safer* (Washington, DC: U.S. Department of Homeland Security, June 2007), 8-22.

[83] Brady Downs, "The Maritime Security Risk Analysis Model – Applying The Latest Risk Assessment Techniques to Maritime Security," *Proceedings* (Spring 2007): 36-38.

advance all-hazards mitigation programs. The *Post-Katrina Emergency Management Reform Act* transferred key elements of the former Preparedness Directorate to FEMA to include the Office of Grants and Training (G&T). The new Office of Grant Programs administers a range of grants that are increasingly based on the application of risk assessment models and criteria. Before its transfer to FEMA, G&T administered a Technical Assistance Program for Port and Transit Security Risk Assessment, and supported the assessment of roughly forty major transit properties across the country. [84]

Transportation Security Administration (TSA) – TSA is responsible for security of the nation's transportation systems, to include highways, railroads, buses, mass transit, maritime ports, and airports. It does this in partnership with the private sector, and state, local, and regional governments and transportation agencies. Under the NIPP, TSA has a lead role in identifying critical transportation assets and working with transportation security stakeholders to reduce the security risks associated with them. [85] In line with these efforts, TSA is pursuing development of risk assessment tools and techniques for application to threats against both surface transportation systems and air travel.

2. Advisory Councils and Information Sharing Centers

Homeland Security Advisory Council (HSAC) – The HSAC is an advisory board that provides independent advice and recommendations to the secretary of Homeland Security to aid in the creation, coordination, implementation, and evaluation of policy and operational capacities. HSAC prepares periodic reports on a range of issues, as requested by the secretary. Membership is composed of senior leaders from state and local government, first responder communities, the private sector, and academia. [86] The HSAC has submitted roughly seventeen major reports to the secretary on a variety of

---

[84] Federal Emergency Management Agency, *Implementation of the Post-Katrina Emergency Management Reform Act*, http://www.dhs.gov/xabout/structure/gc_1169243598416.shtm [Accessed July 20, 2007].

[85] Transportation Security Administration, *Risk Management*, http://www.tsa.gov/approach/risk/index.shtm [Accessed July 10, 2007].

[86] U.S. Department of Homeland Security, *Homeland Security Advisory Council Charter* (February 20, 2007), 1.

homeland security issues. Among these is a January 2006 report on infrastructure protection, which included a range of recommendations related to risk assessment policy and practice. [87]

National Infrastructure Advisory Council (NIAC) – The NIAC provides the president, through the DHS secretary, with advice on issues related to the security of the nation's critical infrastructure and associated information systems, as requested by the president. The NIAC also advances efforts to enhance public / private sector cooperation in infrastructure security, and develop ways to encourage private industry to perform risk assessments of critical systems. The NIAC is composed of members appointed by the president from private industry, academia, and state and local governments.[88] The NIAC has submitted roughly thirteen major reports to the president related to infrastructure protection. Two of these deal specifically with risk assessment and risk management. [89]

Critical Infrastructure Partnership Advisory Council (CIPAC) – Under the NIPP Sector Partnership Model, the CIPAC facilitates coordination between federal infrastructure protection programs and the efforts of the private sector, as well as those of state, local, territorial, and tribal governments. [90] CIPAC membership includes CI/KR owner/operators and designated trade organizations that participate as members of Sector Coordinating Councils (SCCs) for each CI/KR sector. It also includes representatives from federal, state, local, and tribal governments as members of Government Coordinating Councils (GCCs) for each sector. There are coordinating councils for sixteen CI/KR sectors, and within those councils there are over 380 individual owner/operators and other industry interests represented. In addition, another 130 entities represent governmental agencies or interests across the councils. [91] Accordingly, the

---

[87] U.S. Department of Homeland Security, *Homeland Security Advisory Council*, http://www.dhs.gov/xinfoshare/committees/editorial_0331.shtm [Accessed July 20, 2007].

[88] U.S. Department of Homeland Security, *National Infrastructure Advisory Council* (July 3, 2007), 1.

[89] U.S. Department of Homeland Security, *National Infrastructure Advisory Council*, http://www.dhs.gov/xprevprot/committees/editorial_0353.shtm [Accessed July 20, 2007].

[90] U.S. Department of Homeland Security, *Charter for the Critical Infrastructure Partnership Advisory Council* (March 20, 2006), 1.

[91] U.S. Department of Homeland Security, *Council Members, Critical Infrastructure Partnership Advisory Council*, http://www.dhs.gov/xprevprot/committees/editorial_0848.shtm [Accessed July 20, 2007].

CIPAC sector partnership consists of over five hundred individual member entities representing a substantial cross-section of public and private sector CI/KR security stakeholders. It is a far-reaching collaborative network that is largely self-managed, diverse in character, and national in scope. The Partnership Model is described in greater detail in Chapter III.

Partnership for Critical Infrastructure Security (PCIS) – PCIS is a non-profit organization formed in 1999 to address cross-sector critical infrastructure protection and interdependency issues of concern to critical infrastructure owners and operators. A key element of the CIPAC, PCIS strives to build collaborative relationships and advance a non-regulatory approach to CI/KR security and resiliency. Membership consists of the leadership of sixteen of the seventeen sector coordinating councils. In 2006, PCIS was recognized by DHS as the private sector cross-sector council in the NIPP. [92]

Information Sharing and Analysis Centers (ISACs) – Originally established in 1999, the concept of Information Sharing and Analysis Centers (ISACs) was expanded in the 2003 *National Strategy for Homeland Security*. ISACs are government or industry sponsored collaborations dedicated to the mutual protection of critical infrastructure from cyber and/or physical security threats by, as the name implies, sharing related information and analysis within the industry and with the government. Though sponsorship and organization may vary, ISACs generally provide: a forum for information on threats, risks, vulnerabilities, and security solutions; a 24x7 threat detection and warning system; and a forum for information exchange. [93] Some ISACs have been active in establishing security standards and working with local governments on emergency readiness issues.

3. Research, Academic, and Professional Organizations

Homeland Security Institute (HSI) – HSI is a Federally Funded Research and Development Center (FFRDC) that delivers independent analysis and advice to DHS in

---

[92] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 5.

[93] Robert Radvanovsky, *Critical Infrastructure – Homeland Security and Emergency Preparedness* (Boca Raton, FL: CRC Press, 2006), 199-201.

support of policy development, decision-making, analysis of alternative approaches, and the evaluation of new ideas. HSI is operated under contract by Analytic Services Inc., with oversight from DHS Science and Technology (S&T). [94] Threat and risk analysis are listed as among its core capabilities. Since 2004, HSI has completed over twenty major projects, three of which specifically deal with risk assessment and/or risk management. In addition, HSI developed and is now employing a risk-based decision model to guide S&T research and development investment decisions. According to HSI, the model is currently being considered for DHS-wide application. [95] Though it has conducted risk-related projects, its research agenda does not seem to be guided by the need to support implementation of a national risk management framework as outlined in the NIPP.

Center for Risk and Economic Analysis of Terrorism Events (CREATE) – CREATE was the first university-based center of excellence chartered and funded by the DHS Science and Technology Directorate. The Center is focused on improving the nation's security through the development of models and tools for the evaluation of the risks, costs, and consequences of terrorism. [96] Based at the University of Southern California, it has partnerships with New York University and the University of Wisconsin at Madison. Its advisory board includes 65 members from government and 8 members from the scientific community. CREATE's agenda involves research, education, and outreach to inform and support risk-based decision-making. [97] Like HSI, its agenda does not seem to include work related to implementation of the NIPP risk framework.

Critical Infrastructure Protection Program, George Mason University (GMU) – This program pursues basic and applied research related to a full range of issues attendant to critical infrastructure and key resource protection. The GMU Critical Infrastructure Protection (CIP) program provides direct assistance to the DHS Office of Infrastructure

---

[94] Homeland Security Institute, *Homeland Security Institute*, http://www.homelandsecurity.org /Default.aspx [Accessed August 24, 2007].

[95] George Thompson, "Risk Management for Resource Allocation" (briefing presented at the U.S. Department of Homeland Security 2007 S&T Stakeholders Conference, Washington, DC, May 23, 2007).

[96] Detlof von Winterfeldt, *Information Sharing and Terrorism Risk Assessment Committee on Homeland Security*, Testimony Before the Subcommittee on Intelligence, United States House of Representatives (Washington, DC: November 17, 2005).

[97] University of Southern California, *About CREATE*, http://www.usc.edu/dept/create/ [Accessed August 19, 2007].

Protection (OIP), the Partnership for Critical Infrastructure Security (PCIS), and private industry in support of NIPP implementation. It has also advanced work in support of state and local government CI/KR protection efforts to include the National Capital Region Critical Infrastructure Vulnerability Assessment Project on behalf of the Commonwealth of Virginia, the State of Maryland, and the District of Columbia. [98]

National Infrastructure Simulation and Analysis Center (NISAC) – A joint initiative of Sandia National Laboratories (SNL) and the Los Alamos National Laboratory (LANL), NISAC provides modeling and simulation capabilities to support the analysis of critical infrastructure complexities, interdependencies, and vulnerabilities. [99] Sponsored by OIP, the purpose of the Center is to aid decision-making in the areas of preparedness, consequence and risk analysis, policy analysis, investment and mitigation planning, and education and training. SNL developed and offers a suite of security Risk Assessment Methodologies (RAM) for a range of applications.[100] However, RAM methodologies do not seem to figure prominently in the NIPP risk framework.

Wharton Risk Management and Decision Processes Center – Over its twenty-year history, the Center has advanced basic and applied research related to the management of low-probability / high-consequence events involving safety, health, and the environment, in both private and public sector applications. The Center's portfolio includes work in the areas of critical infrastructure protection, mitigating the risks of large-scale natural disasters, and terrorism risk financing. In particular, its research focuses on decision-making to cope with technological and natural hazards and the effectiveness of related strategies, such as incentive systems, insurance, regulation, and the communication of risk information. The Center lists DHS as one of its principal government partners. [101]

---

[98] George Mason University, *Critical Infrastructure Protection Program,* http://cipp.gmu.edu/mission/ [Accessed July 10, 2007]

[99] Sandia National Laboratories, *National Infrastructure Simulation and Analysis Center*, http://www.sandia.gov/mission/homeland/programs/critical/nisac.html [Accessed August 24, 2007].

[100] Sandia National Laboratories, *Security Risk Assessment Methodologies*, http://www.sandia.gov/ram/ [Accessed August 24, 2007].

[101] Wharton School of the University of Pennsylvania, *Risk Management and Decision Processes Center*, http://opim.wharton.upenn.edu/risk/index.html [Accessed August 24, 2007].

Center for Risk Management of Engineering Systems – Located at the University of Virginia, the Center develops theories, methodologies, and technologies to assist in the assessment and management of risk. Among the areas of expertise listed by the Center are critical infrastructure protection and infrastructure interdependencies. Its research agenda has included a variety of projects for the modeling and risk assessment of critical infrastructure at the request of industry, state government, Department of Defense (DoD), and DHS sponsors. [102]

American Society of Mechanical Engineers (ASME) – In May 2002, the ASME issued a position paper that affirmed the organization's stance on the role of risk analysis in society; essentially, that "risk analysis is a technically sound and socially responsible method to facilitate decision-making by government, industry, and the general public." A key tenet of the policy is that "consistent methods of risk analysis should be applied throughout government and the private sector." [103] In line with this position, in 2004, the ASME Innovative Technologies Institute LLC partnered with DHS in developing the Risk Analysis and Management for Critical Assets Protection (RAMCAP) methodology. RAMCAP™ is cited in the NIPP as a principal approach to analyzing CI/KR risks.

The Society for Risk Analysis (SRA) – SRA describes itself as a multi-disciplinary, interdisciplinary, scholarly, international society that provides an open forum for all those who are interested in risk analysis, risk assessment, risk characterization, risk communication, and risk management. The range of SRA activities is wide and spans risks of concern to individuals, to both public and private sector organizations, and to society in general. [104] It encourages the exchange of ideas through its publications and conferences, and its members include those advancing the state of knowledge and practice in risk assessment of large-scale natural disasters and terrorism.

---

[102] University of Virginia, *Center for Risk Management of Engineering Systems*, http://www.sys.virginia.edu/risk/ [Accessed August 24, 2007].

[103] American Society of Mechanical Engineers, *Statement on the Role of Risk Analysis in Decision-making*, http://www.asme.org/NewsPublicPolicy/GovRelations/PositionStatements/Statement_Role_Risk_Analysis.cfm [Accessed August 24, 2007].

[104] The Society for Risk Analysis, http://www.sra.org/index.php [Accessed August 24, 2007].

Security Analysis and Risk Management Association (SARMA) – SARMA is a non-profit professional trade association serving those responsible for analyzing and managing security risks to systems, structures, operations and information systems from man-made threats. SARMA's purpose is to facilitate the development, standardization, and professionalization of the security analysis and risk management discipline by providing leadership, education, and certification for security analysis and risk management professionals. [105] Its membership includes individuals with risk management experience in intelligence, defense, homeland security, and the private sector.

4. State and Local Government, and the U.S. Congress

State Homeland Security Advisors Council (HSAC) – The National Governors Association (NGA) formed the HSAC in June 2006 to provide a forum where homeland security advisors could discuss issues, share information and expertise, and keep their individual governors informed on matters related to the implementation of national homeland security policies impacting their state or territory. [106] As the chief homeland security official for their state or territory, homeland security advisors form an influential constituency. A 2006 NGA survey of HSAC members found that "concern continues over the lack of state input into federal policy… [and] homeland security directors are nearly unanimous in their recommendation that the federal government coordinate with states prior to adopting and implementing policies." [107]

According to the NGA survey, states do not feel they have adequate representation in the DHS policy-making process, and several homeland security directors noted that DHS consults with a limited number of handpicked state officials and then claims to produce policy based on broad state input. The survey found that state advisors believe DHS often lacks transparency, and cites as a good example of this the

---

[105] Security Analysis and Risk Management Association, http://www.sarma.org/about/ [Accessed August 24, 2007].

[106] National Governors Association, "Governors Homeland Security Advisors Council," http://www.nga.org/portal/site/nga/menuitem.1f41d49be2d3d33eacdcbeeb501010a0/?vgnextoid=93b1ff821d16e010VgnVCM1000001a01010aRCRD [Accessed April 12, 2007].

[107] National Governors Association, *2006 State Homeland Security Directors Survey* (Washington, DC: National Governors Association Center for Best Practices, 2006), 1-6.

new risk-based funding formula and how states have little idea of how DHS defines risk. Also cited were the duplicative efforts of multiple federal agencies performing CI/KR protection roles; specifically, in the identification and listing of critical infrastructure and in performing vulnerability assessments. "Not only is this information not being shared with states, but it also appears… [that] various Federal agencies are not sharing their information on critical infrastructure with one another." [108] Problems in risk assessment and information sharing would seem of particular concern because almost all of the state advisors indicated they were pursuing their own infrastructure protection planning efforts with public and private sector CI/KR owner and operators, and half were working in a similar way with surrounding regions.

County, City, and Municipal Government – There are approximately 87,500 units of local government in the U.S., to include special districts and authorities. Of that number, about 3,000 are county governments, and another 36,000 are municipal governments. [109] As a great deal of homeland security is local in nature, each of these entities has a role to play in mitigating risk and protecting the nation's critical infrastructures and key resources. An article by Kiki Caruson and Susan MacManus puts this challenge in a more on-the-ground perspective. They suggest that, while the federal and state governments have dominant roles to play in making and implementing homeland security policy, local governments have to carry out that policy at a grass-roots level. [110] Caruson and MacManus point out that counties and cities have borne a considerable portion of the burden of financing and managing homeland security initiatives. Local law enforcement and emergency first responders are most often directly involved in working with the private sector in their communities to coordinate critical infrastructure security and emergency response efforts.

State and local working groups mandated by DHS grant guidance – As required by DHS, states and urban/port regions have implemented a variety of inter-governmental

---

[108] *State Homeland Security Directors.*

[109] U.S. Census Bureau, *Statistical Abstract of the United States 2007* (Washington, DC: Government Printing Office, 2007), 264.

[110] Kiki Caruson and Susan MacManus, "Homeland Security Preparedness: Federal and State Mandates and Local Government," *Spectrum: The Journal of State Government* (Spring 2005): 25-28.

working groups to pursue planning for homeland security, and more specifically for CI/KR protection. In addition to any frameworks the states have established for overall homeland security planning, other working groups may also be in effect: an Urban Area Security Initiative Urban Area Working Group (UAWG); a Regional Transit Security Working Group (RTSWG); and possibly a port security planning working group under the Area Maritime Security Committee (AMSC). In accordance with the NIPP risk management framework, states must implement a state-wide CI/KR protection program, and integrate it with planning by these other mandated working groups. [111] Since CI/KR planning must be risk-based, and DHS grant programs are largely guided by the application of risk-based formulas, these working groups, and their member agencies, have a significant stake in DHS CI/KR risk management policy.

The United States Congress – As the peoples' representatives, Congress has a significant role in shaping homeland security policy through the formulation of legislation and control over funding. Since the creation of DHS, congressional legislation has increasingly used the language of risk to guide the evolution of DHS programs and to drive for greater effectiveness and accountability in the Department's efforts to secure the nation. It has been particularly focused on the application of risk assessment in the protection of critical infrastructure and the strengthening of state and local preparedness. Consistent with the 9/11 Commission's recommendation that funding assistance to the states be based on risk and vulnerability, members of Congress have been especially vocal about the importance of taking a risk management approach to homeland security, to include the risk-based allocation of funding to the states and urban areas.

According to a recent Congressional Research Service (CRS) report, a successive stream of bills have gradually attempted to reform perceived problems with homeland security grant programs, each time moving further away from guaranteed allotments to a greater percentage of funding allocated on the basis of risk. As the CRS report points out, "To varying detail, each legislative initiative suggested definitions or approaches to

[111] U.S. Department of Homeland Security, *FY 2007 Homeland Security Grant Program -Program Guidance* (Washington, DC: U.S. Department of Homeland Security, January 2007), 4-5.

evaluate risk with regard to homeland security." [112] What the CRS report stops just short of saying is that given the nature of congressional politics, a positive intention may not always come out in the form of well fashioned policy. With each new definition or approach to risk assessment mandated by congressional fiat, DHS must respond, whether it makes sense to or not. Due to what CRS calls the "lack of a coherent, long-term, overarching risk strategy," DHS has no plan of its own to guide the more reasoned evolution of risk policy and practice.[113] This is true, not only across the Department, but across the entire homeland security community; however, such a plan is necessary to implement the national risk management framework called for in the NIPP. In the absence of a plan, Congress will provide guidance, well reasoned or not. The best option is to get Congressional backing for a structured plan presented in advance, rather than wait for the next wave of guidance.

---

[112] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (Washington, DC: Congressional Research Service, February 2, 2007), 4-5.

[113] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (Washington, DC: Congressional Research Service, February 2, 2007), 25.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INFRASTRUCTURE PROTECTION AND RISK MANAGEMENT

A. CRITICAL INFRASTRUCTURE PROTECTION PROGRAMS

1. National Critical Infrastructure Protection Policy

President Clinton outlined the basic foundations for the Nation's current policy on critical infrastructure and key resource (CI/KR) protection well over a decade ago, when in July 1996, he issued *Executive Order 1301–Critical Infrastructure Protection* (EO 13010). EO 13010 defined critical infrastructures as those "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." [114] Given that the vast majority of the nation's CI/KR assets are owned by the private sector, the order stipulated that it is essential for the government and private sector to work together to protect those assets and assure their continued operation. The order also established the President's Commission on Critical Infrastructure Protection (PCCIP) to assess CI/KR vulnerabilities and threats and to recommend a national policy and implementation strategy for CI/KR protection.

The PCCIP report – *Critical Foundations: Protecting America's Infrastructures* – was issued on October 13, 1997. In addition to outlining the nature and extent of the challenge, the report cited potential vulnerabilities and what it called "shared threats and shared responsibility" in the recognition of governments' interdependence with the private sector. Along these lines, it recommended a "real partnership between infrastructure owners and operators and the government" to include "collaborative public and private organizational arrangements that challenge our conventional way of thinking about government and private sector interaction." [115] Following the PCCIP report, in May of 1998, President Clinton signed *Presidential Decision Directive 63* (PDD-63),

---

[114] William Clinton, "Executive Order 13010 - Critical Infrastructure Protection," *Federal Register* 61, no. 138 (Washington, DC: U.S. Government Printing Office, July 17, 1996), 37347.

[115] The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures – The Report of the President's Commission on Critical Infrastructure Protection* (Washington, DC: The White House, October 13, 1997), 11-66.

establishing a national critical infrastructure protection policy and a government framework to develop and implement infrastructure protection measures. PDD-63 identified industry sectors and designated lead federal agencies to work with each to jointly advance CI/KR protection efforts. To assist the private sector in achieving and maintaining infrastructure security, it directed the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism to "propose and develop ways to encourage private industry to perform periodic risk assessments." [116]

The *USA Patriot Act of 2001* defined critical infrastructure more broadly to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination." [117] The Act reiterated the policy of public-private partnership involving corporate and non-governmental organizations. Two of eight major initiatives in the National Strategy for Homeland Security of July 2002 are to "build and maintain a complete and accurate assessment of America's critical infrastructure and key assets" and "enable effective partnership with state and local governments and the private sector." The strategy reinforced the belief that a close partnership between government and the private sector is essential to national CI/KR protection efforts. Accordingly, the vision for CI/KR protection expressed in the strategy called for the new Department of Homeland Security (DHS) to "forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions." [118] It also stated that DHS would establish a single office to work with state and local governments and the private sector to implement a comprehensive national plan for CI/KR protection. The *Homeland Security Act of 2002*, signed late that year, created DHS and gave it responsibility for

---

[116] William Clinton, *Presidential Decision Directive-63 (PDD-63) – Critical Infrastructure Protection*, 3-18.

[117] *USA Patriot Act of 2001*, Public Law 107-56, 107th Congress, 1st Session, (October 26, 2002), 400-401.

[118] U.S. Department of Homeland Security, *National Strategy for Homeland Security*, 29-35.

leading the national critical infrastructure protection effort. It also required DHS to develop a comprehensive national plan for CI/KR security. [119]

In February 2003, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* set out specific national goals, objectives, and guiding principles for CI/KR protection. Of special note here is what the strategy outlines as the key role of state government. It specified that states should facilitate coordinated planning for CI/KR protection, applying unified criteria for determining criticality and prioritizing protection investments. It also specified the need for DHS to work with state and local governments and the private sector to establish a uniform methodology for determining national-level criticality. [120] The strategy went on to describe a unifying organizational framework through which the public and private sectors could cooperate in national-level efforts to assess CI/KR vulnerabilities and advance protection efforts. Though the strategy references the need to coordinate and consolidate federal and state protection plans, it clearly emphasizes a direct national-level relationship between DHS, lead federal agencies, and the CI/KR industry sectors.[121] Despite broad policy statements concerning collaboration with state and local government, the strategy begins to set the stage for what has emerged as DHS-dominated interaction with the CI/KR sectors. This is concurrent with ongoing CI/KR protection initiatives by state and local agencies. Such a dichotomy in policy has implications for the implementation of the National Infrastructure Protection Plan, and especially the national risk assessment framework.

Homeland Security Presidential Directive 7 (HSPD-7) identified what are now the 17 CI/KR sectors, further defined the overarching leadership and coordination role of DHS, and outlined the responsibilities of other federal departments and agencies with CI/KR sector-specific responsibilities. Consistent with the Homeland Security Act of 2002, HSPD-7 directed the DHS secretary to produce a comprehensive, integrated national plan for CI/KR protection by December 2004. The Plan was to include a strategy to identify, prioritize, and coordinate CI/KR protection and a summary of

---

[119] *Homeland Security Act of 2002,* 2146.

[120] George Bush, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 1-19.

[121] *Homeland Security Act of 200* , 22-24.

activities to define, prioritize, and reduce the vulnerability of CI/KR assets. [122] In response to HSPD-7, the Interim National Infrastructure Protection Plan was published in February 2005. It was issued to provide the framework to guide a coordinated national approach, as called for in the 2003 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. DHS released other drafts of the National Infrastructure Protection Plan for comment in November 2005 and January 2006. [123] The final National Infrastructure Protection Plan (NIPP) was published in June 2006.

The NIPP has been described as a base plan or national blueprint for how DHS, Sector-Specific Agencies (SSAs), and other relevant stakeholders should advance and coordinate CI/KR protection initiatives within and across sectors. The SSAs interact with their respective sectors through a sector partnership model in the form of the Critical Infrastructure Partnership Advisory Council (CIPAC). CIPAC is the organizing structure for coordinating joint government and private sector efforts to implement the NIPP. That structure is composed of a mirror arrangement of industry sector coordinating councils and government coordinating councils for each sector. The NIPP required individual SSAs for each sector to submit Sector-Specific Plans (SSPs) to DHS by the end of December 2006. Following the guidance and basic outline established in the NIPP base plan, SSPs were to set out the means by which the sectors would identify critical assets, assess risks, set priorities, and develop protective measures for that sector. Central to the entire concept of the NIPP, and at the heart of sector planning and implementation efforts, is the NIPP's risk management framework. That framework established basic principles and criteria for assessing CI/KR risks and formulating and managing the implementation of sector-specific security strategies. [124]

---

[122] George Bush, *Homeland Security Presidential Directive 7 (HSPD-7) - Critical Infrastructure Identification, Prioritization, and Protection*, 3-4.

[123] Government Accountability Office, *Critical Infrastructure Protection - Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics* (Washington, DC: Government Accountability Office, October 2006), 2.

[124] U.S. Department of Homeland Security, *National Infrastructure Protection Plan – Executive Summary* (Washington, DC: U.S. Department of Homeland Security, 2006), 1-5.

2. Sector Partnership Model

In proposing collaborative approaches to addressing the complex problems in homeland security, researcher Thomas Stanton presented the Stakeholder Council Model in 2003 as an alternative to top-down federal interaction with state and local government and the private sector. Stanton cites Lester Salamon when he says "the administration of government services is moving from a hierarchical structure to the management of organizational networks." [125] Stanton suggests that to achieve national homeland security aims, the federal government must act through what Salamon has called third-party government, consisting of state and local government and the private sector. The Stakeholder Council Model provides a means for bringing many different stakeholders together to develop solutions to specific federal concerns. He asserts that "the Stakeholder Council Model is based on years of experience with standard-setting groups in many sectors of the economy" including the Electronic Benefits Transfer Council and the delivery of government payments to clients (i.e., food stamps, etc.) by the states. [126]

Stanton describes the traditional federal model as being hierarchical, with the imposition of policy from above, often on the basis of limited consultation with the affected parties. He posits that this is unlikely to be effective in dealing with complex homeland security problems, especially ones that call for management of complex networks. The number of stakeholders, the variety of positions, and the range of differing values makes success difficult through a purely mandatory approach. He acknowledges that state and local governments and the private sector have a better understanding of the critical facts needed to implement national homeland security strategy. The Stakeholder Council Model as proposed by Stanton, while potentially more labor intensive and time-consuming in the deliberative phase, "may allow the development of more effective and comprehensive solutions for the longer term." [127]

---

[125] Lester M. Salamon, "The New Governance and the Tools of Public Action: An Introduction," Chapter 1 in Lester M. Salamon, ed., *Tools of Government: A Guide to the New Governance*, (New York: Oxford University Press, 2002), 11-14.

[126] Thomas Stanton, *Improving Federal Relations with States, Localities, and Private Organizations on Matters of Homeland Security: The Stakeholder Council Model* (March 18, 2003), 1-3.

[127] Ibid., 2-10.

Similar to what Stanton proposed in 2003, the NIPP sector partnership model provides a structure through which different levels of government and the private sector can collaborate in CI/KR protection planning and implementation efforts. CIPAC supports the sector partnership model by "providing a legal framework" for members of the industry sector coordinating councils (SCCs) and government coordinating councils (GCCs) to engage in joint CI/KR protection-related activities. Through this partnership, SSAs liaise with their industry sector and federal, state, and local government counterparts in the development and review of their respective SSPs. Under the CIPAC, SCCs and GCCs are also empowered to advance policy initiatives unique to their individual sectors. Beyond the SSPs themselves, the CIPAC serves as a forum for SCCs and GCCs to engage in ongoing CI/KR protection-related functions such as the implementation of security programs and coordination of incident response and recovery. CIPAC encourages all CI/KR owners and operators to use the SCC for their industry as their primary means for coordinating with government on CI/KR protection issues. [128]

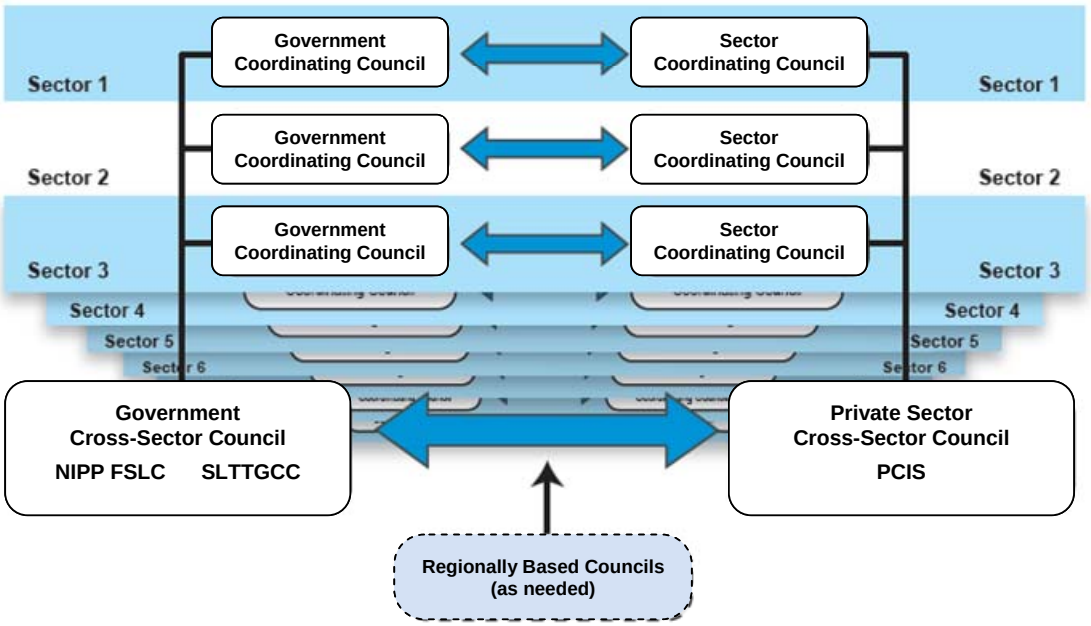

Figure 4. Sector Partnership Model. [129]

[128] U.S. Department of Homeland Security, *National Infrastructure Protection Plan – Sector Partnership Model* (Washington, DC: U.S. Department of Homeland Security, 2006) 1-2.

[129] Ibid., 53.

Membership in SCCs varies by sector, but is intended to be representative of all stakeholders within that sector. GCCs, as government counterparts to each SCC, provide interagency and cross-jurisdictional coordination, and are comprised of members from across various levels of government as appropriate to each sector. Providing "cross-sector" coordination are the Private Sector Cross-Sector Council (the previously established Partnership for Critical Infrastructure Security or PCIS), and the Government Cross-Sector Council. PCIS provides senior-level, strategic coordination with DHS and the SSAs. The Government Cross-Sector Council is made up of two sub-councils: the Federal Senior Leadership Council (FSLC), and the State, Local, and Tribal Government Coordinating Council (SLTGCC). The FSLC provides coordination between and among federal agencies. The SLTGCC provides a structure to coordinate across state and local jurisdictions. In addition, the NIPP partnership model makes provisions for Regional Coordinating Councils to enable CI/KR protection coordination within and across geographical areas and sectors. [130]

As described in Chapter II, the CIPAC sector partnership consists of over 500 individual member entities representing a substantial cross-section of public and private sector CI/KR security stakeholders. It is a far-reaching collaborative network-of-networks that is largely self-managed, diverse in character, and national in scope (see Figure 4).

3. Sector-Specific Plans

The NIPP required that Sector-Specific Agencies (SSAs), as designated in HSPD-7, develop Sector-Specific Plans (SSPs) to "provide details on how the CI/KR mission will be coordinated, developed, and implemented within the 17 CI/KR sectors." SSPs were to be developed in collaboration with SCCs and other security partners and submitted to DHS within 180 days of final approval of the NIPP (December 2006). Developed according to the basic requirements outlined in the NIPP, SSPs are tailored to the individual needs of the CI/KR sector for which they are written. Basic requirements for SSPs include definition of sector security partners, authorities, regulatory basis, roles

[130] *National Infrastructure Protection Plan*, 1-2.

and responsibilities, and interdependencies; procedures for sector interaction, information sharing, coordination, and partnership; goals and objectives for CI/KR protection; and a sector-specific approach to implementing the risk management framework. [131]

Sector-Specific Agency	Critical Infrastructure/Key Resource Sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Health Care
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Waste Water Treatment Systems
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard	Transportation Systems
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

Figure 5. Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors. [132]

[131] U.S. Department of Homeland Security, *National Infrastructure Protection Plan – Sector-Specific Plans* (Washington, DC: U.S. Department of Homeland Security, 2006) 1-2.

[132] Ibid., 2.

SSAs are responsible for leading and coordinating the development of SSPs in conjunction with the SCCs, GCCs and other security partners. SSPs are to be updated as threats change and protective programs are implemented. As a common risk management framework develops and becomes institutionalized, it will permit the assessment of performance in implementing CI/KR protection programs. SSAs, in coordination with the GCCs and SCCs, are responsible for revising SSPs to reflect this performance and any other changes in overall security posture. Having responsibility for national coordination for CI/KR protection, DHS monitors NIPP and SSP implementation and tracks progress toward achieving NIPP goals and objectives. [133] On May 21, 2007, the DHS secretary announced the completion of the 17 SSPs. In making this announcement, Secretary Chertoff stated… "This is the first time in the history of the country that the government and the private sector have ever come together on such a large scale to develop a joint plan. And if you think about the literally millions of businesses and the millions of types of economic activity that occur every day, you'll begin to realize what a truly remarkable exercise this has been…" [134]

A July 2007 review of the SSPs by the GAO found that nine SSPs generally met NIPP requirements and DHS supplemental guidance. Most included the required elements of the NIPP risk management framework, but eight did not address incentives the sectors would use to encourage risk assessments by CI/KR owners. GAO also found that some plans were more developed and comprehensive than others, largely depending on the maturity of those sectors and how they defined their assets and functions. According to GAO, given the differences in the plans to date, it is unclear to what extent DHS will be able to identify gaps and critical interdependencies across the sectors as part of any national roll-up. Perhaps most significant among GAO findings was that representatives of the GCCs and SCCs had differing views regarding the value of sector-specific plans and DHS review of those plans. The report said that… "while 10 of the 32 council representatives we interviewed reported that they saw the plans as

---

[133] *National Infrastructure Protection Plan – Sector-Specific Plans*, 1-2.

[134] U.S. Department of Homeland Security, "DHS Completes Key Framework for Critical Infrastructure Protection" (May 21, 2007), http://www.dhs.gov/xnews/releases/pr_1179773665704.shtm [Accessed May 27, 2007].

useful…representatives of eight councils disagreed because they believed the plans either did not represent a partnership among the necessary key stakeholders, especially the private sector, or were not valuable because the sector had already done so much work on its own and had progressed beyond the plan." [135] As of this writing, the SSPs are still under review by DHS.

4. Risk Management Framework

In the keynote address to the DHS 2006 Grants & Training National Conference, DHS Secretary Michael Chertoff stated that "we all have to work together to protect our communities and our country, and we have to do it not by mandates from the top down but by networking from the bottom up…We have to have a common approach, a coordinated approach, across all of the phases of what we have to do to create homeland security." The secretary then emphasized a point he has made numerous times since taking office…"the core principle that animates what we do at DHS…is risk management." [136] Indeed, in every public appearance and in most of his testimony before Congress, the DHS secretary has reiterated his strategic intent to implement risk-based decision-making to guide homeland security at all levels of government, consistent with the guidance he has received from both the president and the Congress. Nowhere is the application of risk management more fundamental than in the protection of the nation's critical infrastructure. Accordingly, the cornerstone of the NIPP is a risk management framework that sets out broad guidance for a process of continuous assessment and improvement in the security of the nation's CI/KR assets.

The NIPP risk management framework includes the basic steps of risk management: setting security goals; the identification of critical CI/KR assets; risk assessment; priority setting; implementation of protective measures; and the ongoing measurement of program effectiveness and the reprogramming of results as the cycle repeats itself. The risk management cycle described in the NIPP is similar to the

---

[135] Government Accountability Office, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve* (Washington, DC: Government Accountability Office, July 10, 2007), 3-6.

[136] U.S. Department of Homeland Security, *Keynote Address by Secretary of Homeland Security Michael Chertoff to the 2006 Grants & Training National Conference*.

framework outlined by the GAO for application to homeland security decision-making, as described in Chapter II. The process is intended to drive cooperative CI/KR risk-reduction and risk management efforts by DHS, the SSAs, SCCs, and other security partners that share responsibility for CI/KR protection. According to the NIPP, the risk management framework can be applied at an asset, system, network, or functional level, depending on the individual CI/KR sector. In some cases it may be applied bottom-up, asset-by-asset, or top-down, taking a broader business-wide or continuity approach. [137]

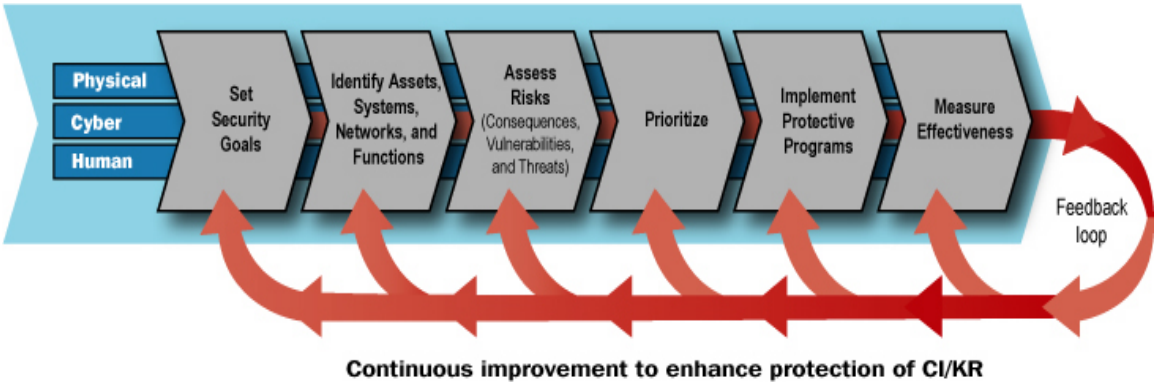

Figure 6. NIPP Risk Management Framework. [138]

The NIPP assigns SSAs the responsibility for leading sector-specific risk management programs and for ensuring that the tailored, sector-specific application of the risk management framework is addressed in their respective SSPs. The NIPP describes DHS responsibility as supporting the efforts of the SSAs by providing guidance, tools, and analytical support. DHS is also responsible for integrating the results of sector-specific risk management efforts for cross-sector, national-level risk analysis and management activities. According to the NIPP, state governments are responsible for establishing security partnerships, facilitating coordinated information sharing, and enabling planning and preparedness for CI/KR protection within their jurisdictions. The NIPP suggests that state efforts essentially mirror those of DHS and the SSAs to include developing a unified

[137] U.S. Department of Homeland Security, *National Infrastructure Protection Plan – Risk Management Framework* (Washington, DC: U.S. Department of Homeland Security, 2006), 1-2.

[138] Ibid., 2.

approach to CI/KR risk management. [139] It further suggests that state and local governments participate in the NIPP sector partnership model and may pursue CI/KR protection initiatives as a regional coordinating council. The NIPP considers such efforts as complementary and enhancing the implementation of the NIPP and the SSPs "by providing unique geographical focus and cross-sector coordination." [140] A NIPP appendix addresses state and local concerns and provides advice on pursuing their own CI/KR protection programs. [141]

Though the NIPP outlines a basic risk management framework, it does not provide a common method or metrics for the most pivotal part of the process – the assessment of risk. The NIPP essentially acknowledges that there are a variety of risk assessment methodologies in use across the various sectors and that these have varied widely in terms of assumptions, comprehensiveness, objectivity, and other dimensions. In the interest of supporting comparative risk analysis at a national level, a set of baseline criteria are set forth for methodologies that may be employed under the NIPP framework. There are seven baseline criteria to establish whether a methodology is both credible enough to stand up to objective evaluation, and comparable with other standard methods used. [142] There is no indication in the NIPP as to how the baseline criteria will be applied, what existing methodologies meet the criteria and are thus recommended for application, and what the process will be for advancing common standards and processes for risk assessments that are robust and compatible enough to support comparisons both within and across sectors as an essential component of the national risk management framework.

Of the SSPs not restricted and available for public review, only the transportation and water sectors had a robust discussion of their approach to risk assessment. The water sector described a suite of assessment tools available to and used extensively by that industry. The transportation sector also outlined tools available for asset-level

---

[139] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 22-29.

[140] Ibid., 76.

[141] Ibid., 167.

[142] Ibid., 149-152.

assessment within individual sub-sectors. However, the transportation SSP also outlined an overall approach to system-wide risk management in what it called the Systems-Based Risk Management Process (SBRM). [143]

B. HOMELAND SECURITY RISK ASSESSMENT PROGRAMS

1. National-Level Risk Assessment

Despite successive statements of strategic intent by the president, the Congress, and two secretaries, the Department of Homeland Security (DHS) continues to face challenges in advancing an integrated national program of risk assessment and risk management. There are a number of practical reasons for this. The concepts surrounding risk assessment for high consequence / low probability events, particularly for acts of terrorism, are new and complex. The Department is large and still evolving. It struggles with amalgamating the established cultures and practices of legacy agencies while having to build entirely new functions and integrate all of these into one unified organization. It is also advancing a wide range of other programs, all national in scope, at the same time it is developing the policies, procedures, and practices necessary to support and sustain those programs. Finally, it exists in a highly charged political climate where it is under constant scrutiny and its senior leaders are, by necessity, often engaged in defending its actions to a sometimes partisan and always impatient Congress as well as state and local elected leaders. Despite progress made by individual DHS agencies in developing and implementing risk assessment initiatives, the Department's evolution of risk management policies and programs overall has often been slow and painful, still in search of an over-arching strategy and departmental and national-level coordination. According to the Congressional Research Service (CRS), one of the central problems for DHS is that risk needs to be defined not only at the macro-level but on the micro-level as well. [144]

---

[143] U.S. Department of Homeland Security, *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan* (Washington, DC, U.S. Department of Homeland Security, May 2007), 15-17.

[144] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, 17.

Evaluation of risk at the macro-level is by geographic region and the nation as a whole. At the micro-level, it is by specific critical assets or groupings of assets. DHS describes its approach to these two types of risk assessment in a 2006 grant program fact sheet. Geographically-based risk considers "…general characteristics of a geographic area, mostly independent of the assets that exist within that area…reported threats, law enforcement activity… suspicious incidents… the area's proximity to international borders… the potential consequences of an attack on that area, including human health, economy, strategic mission, and psychological impacts." On the other hand, asset-based risk "...employs strategic threat estimates from the Intelligence Community of an adversary's intent and capability to attack different types of assets… using different methods of attack… The vulnerability of each asset type to each attack method is analyzed to yield the form of attack most likely to be successful." [145] The evolution of DHS risk assessment can therefore be viewed along these two different lines.

In theory, risk assessment should guide overall homeland security strategy, programs, and investment priorities for both the federal interagency community and the rest of the nation. Unfortunately, much of the national focus on risk assessment has centered on only a part of the total picture – allocations of grant funds to states and high-threat urban areas for preparedness under the Homeland Security Grant Program (HSGP). CRS notes that, since the formation of DHS, many state and local leaders have expressed frustration with the risk assessment process and the Department's method of allocating grant funds. This is in addition to "a perceived lack of transparency regarding the risk assessment process." [146] In the face of this frustration, and corresponding pressure from Congress, DHS has made incremental changes to its risk assessment formula to guide HSGP fund allocation.

In its recent review of DHS grant programs and risk assessment methodologies, CRS outlined a basic evolution in the Department's approach to macro-level risk assessment to drive the grant process. As CRS describes it, from 2001, when the

---

[145] U.S. Department of Homeland Security, *Homeland Security Grant Program – Risk Analysis – Fact Sheet* (Washington, DC: U.S. Department of Homeland Security, n.d.), 2.

[146] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, 4.

Department of Justice (DOJ) had primary responsibility for assessing risk, to 2002-2003, when this responsibility was transferred to DHS, risk assessment was at an early stage and developmental in character, with risk generally assessed and measured according to population. From 2003 to 2006, DHS began using a more sophisticated methodology that incorporated probability into its risk calculus, and by 2006 was expressing risk more fully as the product of threat, vulnerability, and consequence. In so doing, it also began to consider risk to both geographic areas and critical assets within those areas. [147] However, from its national perch, DHS had too distant a perspective to assess the actual criticality or vulnerability of individual assets, and came under fire for what was being characterized as "critical infrastructure" in the National Asset Database (NADB).

The NADB should be a fundamental source of asset information for DHS risk assessment efforts. However, an audit by the DHS Office of Inspector General (OIG) in 2006 indicated that "the NADB is not yet comprehensive enough to support the management and resource allocation decision-making envisioned by the National Infrastructure Protection Plan (NIPP). OIP has a substantial amount of work ahead to determine the ultimate disposition of the NADB's contents and each asset's importance to the country." [148] Consequently, for 2007, CRS notes that "due to difficulties associated with differentiating vulnerability values across areas and states, according to DHS it has, in effect, assigned a value of one to vulnerability. As a result, while three variables may formally remain in the formula, in effect only two exist… In addition, significant changes to the underlying elements of each variable were made." [149] The absence of solid and reliable information in the NADB has thus blunted the ability of DHS, on its own, to consider asset vulnerability in performing asset-based risk assessments. This is not surprising given the volume of data and the context in which this data was acquired.

---

[147] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, 7.

[148] U.S. Department of Homeland Security, *Office of the Inspector General – Progress in Developing the National Asset Database* (June 2006), 1.

[149] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, 7.

Though the NADB began with an initial list of almost two thousand assets identified by DHS, it grew to a list of over seventy-seven thousand assets after two data calls to the states in 2003 and 2004. According to the OIG, the database included assets that are "unusual, or out-of-place… and whose criticality is not readily apparent." [150] OIG also noted inconsistencies in the data from state to state. The OIG report cites the remarks of Harold Rogers, then chairman of the House Appropriations, Subcommittee on Homeland Security who said, "Without a comprehensive and current inventory of our Nation's critical infrastructure …the department's efforts to implement the appropriate protective measures… and make the right decisions about grant allocations are severely hampered." [151] Such an inventory cannot be developed without active involvement from state and local officials and the private sector, and clear guidelines applied uniformly across the nation.

Given the sheer number of potential targets, no macro-level national risk assessment can be wholly reliable unless fed by bottom-up micro-level criticality, vulnerability, and risk assessments conducted by state and local governments and critical infrastructure owners and operators. Of course, this assumes buy-in to a uniform and integrated national framework, one informed by the use of compatible risk assessment methodologies by these non-federal partners, as called for in the NIPP. However, as of this writing, no such compatible set of methodologies exist, though various DHS agencies and others have advanced their own approaches to micro-level risk assessment along the way. These approaches have evolved independently from the top-down macro-level methods used to drive the Homeland Security Grant Program.

2. Asset-Based Risk Assessment

In an effort to help DHS officials better understand the range of existing tools available to support risk-based decision-making, the Homeland Security Institute (HSI) reviewed over fifty different risk assessment methods and over thirty different risk

---

[150] U.S. Department of Homeland Security, *Office of the Inspector General – Progress in Developing the National Asset Database*, 9.

[151] Ibid, 16.

assessment frameworks from government, academia, and private industry. These were distilled into twenty-five discrete approaches, each chosen for its use in, or promise to, homeland security. These twenty-five approaches were offered by HSI as basic "primers" to support further development of DHS risk assessment programs. [152] The range of methods and frameworks outlined in the HSI study underscores the complex challenge DHS decision makers have in pursuing a common and integrated approach to risk assessment consistent with the guidance concerning a national risk management framework in the NIPP. That challenge may either be further aided or complicated by risk assessment initiatives advanced by several of its component agencies working within the transportation sector, one of the largest sectors in the NIPP. This includes the Coast Guard and ODP (now Grant Programs) and their respective port and transit risk assessment activities that pre-date the NIPP. Driven by both the strategic guidance from above and the practical need to advance risk-based decision-making in their individual mission areas, various DHS agencies have, on their own and in the absence of an overall department-wide risk strategy, advanced efforts to develop and employ asset-based risk assessment methodologies. Each of these initiatives has been pursued on different timelines, using diverse approaches, for various (sometimes overlapping) customers, and with varying degrees of success.

The U.S. Coast Guard (USCG) was the first federal agency after 9/11 to develop and employ a terrorism risk assessment methodology with its introduction of the Port Security Risk Assessment Tool (PS-RAT) and the National Risk Assessment Tool (N-RAT) in late 2001, well before the formation of DHS and the passage of the Maritime Transportation Security Act of 2002. [153] The Office for Domestic Preparedness (ODP) soon followed in 2002 with its production of the Special Needs Jurisdiction Tool Kit (SNJTK) for transportation infrastructure, which it applied for the first time with the Port Authority of New York and New Jersey, a multimodal regional transportation authority,

---

[152] Homeland Security Institute, *Homeland Security Risk Assessment - Volume I: Setting* (Arlington, VA: Homeland Security Institute, June 16, 2006), 5.

[153] Government Accountability Office, *Homeland Security - Applying Risk Management Principles to Guide Federal Investments*, 23.

and owners and operators of the World Trade Center.[154] Not too far behind was the Transportation Security Administration (TSA). That agency advanced an entirely separate risk assessment regime to include the Transportation Risk Assessment and Vulnerability Evaluation (TRAVEL) Tool for transportation assets, and the Vulnerability Identification Self-Assessment Tool (VISAT) for mass transit. Add to these the TSA Maritime Self-Assessment Risk Module (TMSARM). [155]

After several years of development, The USCG PS-RAT evolved into the Maritime Security Risk Assessment Model (MSRAM). Likewise, ODP's SNJTK evolved into two newer methods, the Transit Risk Assessment Module (TRAM) toolkit and the Maritime Assessment and Strategy Toolkit (MAST). TRAM and MAST are compatible methodologies, and each goes beyond basic risk assessment by enabling the comparison of the risk reduction potential of various countermeasures across different assets. They also allow the evaluation of the relative cost-benefit potential of different classes of countermeasures. ODP has conducted TRAM assessments at over thirty of the nation's major transit properties under a Risk Assessment Technical Assistance program. MAST is now being used to amplify MSRAM results and aid in the transition to a maritime security risk management regime. Thus far, the USCG has conducted MSRAM assessments at over 70 of the nation's ports. MAST assessments (a more involved and lengthy process) have been conducted at some of the nation's largest port regions – Los Angeles and Long Beach, Baltimore, and New York. Both TRAM and MSRAM/MAST assessments continue to be conducted for ports and transit agencies across the country. More recently, TSA has entered into a cooperative agreement with Boeing to develop a Risk Management Assessment Tool (RMAT) for the commercial aviation system. The agreement continues joint TSA / Boeing collaboration to evaluate the costs and benefits of proposed security measures. [156]

---

[154] U.S. Department of Homeland Security, *Special Needs Jurisdiction Tool Kit Case Study* (Washington DC: U.S. Department of Homeland Security, 2003), 3-10.

[155] Transportation Security Administration, *Risk Management – Risk Assessment Tools,* http://www.tsa.gov/approach/risk/assessment_tools.shtm [Accessed May 12, 2007].

[156] Wilson Dizard III, "TSA Rolls Dice On Risk Model," *Government Computer News,* June 4, 2007.

In the New York / New Jersey port region, risk assessments conducted by the Coast Guard, covering all critical infrastructure along the waterfront, have overlapped with ODP-supported risk assessments performed by the Port Authority of New York and New Jersey for its own port, bridge, tunnel, transit, and airport facilities in the same jurisdiction. The assessments have neither been coordinated nor the results integrated. The same facilities have been assessed through different methodologies, by different agencies, with different results, for different purposes.

In 2003, through a grant from the Office for Domestic Preparedness (ODP), and under the oversight the Office of Infrastructure Protection (OIP), the American Society of Mechanical Engineers (ASME) Innovative Technologies Institute LLC (ITI) was commissioned to create the Risk Analysis and Management for Critical Asset Protection (RAMCAP™) program. [157] The purpose of the RAMCAP™ initiative was to develop a common framework for evaluating consequences, vulnerability, and risk based on common terminology, common metrics for comparing risks, and a common basis for reporting results across all CI/KR sectors. [158] Though it is the only risk assessment tool identified in the NIPP for use across all sectors, RAMCAP™ has not yet enjoyed wide acceptance, for reasons not readily apparent from the available literature. As noted by Congresswomen Carolyn Maloney in a letter to the DHS Secretary, to date RAMCAP™ has only been adopted for use in three of seventeen CI/KR sectors: chemical manufacturing, nuclear power and energy. Two more are underway – water and wastewater treatment, and dams. [159]

As of this writing, the future application of RAMCAP™ across the remaining twelve CI/KR sectors is uncertain. OIP has recently tasked the Oak Ridge Institute for Science and Education (ORISE) to conduct expert panels to identify and evaluate risk assessment methodologies available for use by the various CI/KR sectors. According to a project fact sheet, deliverables include "a list and brief description of available risk

---

[157] The intellectual property for RAMCAP™ and the RAMCAP™ trademark are owned by ASME-ITI.

[158] ASME Innovative Technologies Institute LLC, *RAMCAP™ Executive Summary* (2005), http://staging.files.asme.org/ASMEITI/RAMCAP/12604.pdf [Accessed December 11, 2006].

[159] Carolyn Maloney, Member of Congress, letter to the Secretary for Homeland Security Michael Chertoff (May 18, 2007).

assessment methodologies and results of an initial evaluation of each method against the NIPP Baseline Criteria and a listing of the methods currently used by the sectors." [160] So the search for CI/KR risk assessment methodologies goes on, despite prior DHS investment in RAMCAP™ and other sector-specific methodologies.

3. Commentary on Homeland Security Risk Assessment

Even before September 11, 2001, the GAO had been advocating the use of risk management practices to set priorities and facilitate decisions on the allocation of federal funds for counter-terrorism activities. Since then, the GAO and the CRS have issued numerous reports to Congress on the progress of DHS risk management efforts. In testimony before Congress in October 2001, the GAO outlined basic risk management principles and strongly urged lawmakers to ensure that the Office of Homeland Security (OHS) embraced this practice.[161] In addressing the challenges associated with critical infrastructure protection a year later, GAO emphasized again the importance of proactively managing security risk. [162] In December 2002, a CRS report provided a primer for Congress on risk assessment as outlined in the National Strategy for Homeland Security. CRS noted that the *Homeland Security Act of 2002* assigned risk analysis activities to the HSI as well as to other components of DHS. CRS suggested options for Congress to include requiring the establishment of guidelines and conditioning grants on state and local completion of risk assessments. [163]

During September 2003, in what would become a nearly annual report on risk management and critical infrastructure protection, CRS noted that DHS responsibility for coordinating critical infrastructure protection had been delegated to Information Analysis and Infrastructure Protection (IAIP). In particular, IAIP was tasked with integrating

---

[160] Oak Ridge Institute for Science and Education, *Expert Panels to Identify and Evaluate Risk Assessment Methods – Fact Sheet* (n.d.).

[161] Government Accountability Office, *Homeland Security - A Risk Management Approach Can Guide Preparedness Efforts* (Washington, DC: Government Accountability Office, October 31, 2001), 2-3.

[162] Government Accountability Office, *Critical Infrastructure Protection - Significant Challenges Need to Be Addressed* (Washington, DC: Government Accountability Office, July 24, 2002), 21.

[163] Congressional Research Service, *State and Local Preparedness for Terrorism: Selected Policy Issues* (Washington, DC: Congressional Research Service, December 19, 2002), 10-11.

threat and vulnerability assessments to identify and manage risk and help set priorities. CRS pointed out that similar activities were being undertaken by other agencies and by the private sector and state and local governments. CRS again suggested that DHS develop a protocol outlining the specific steps to be taken in the risk management process to ensure consistency in carrying out assessments and in making decisions. A February 2005 CRS report essentially cited the same issues and options. [164]

In June of 2003, GAO was asked by Congress to review the state of security efforts across the nation's transportation system. In its report, the agency noted efforts by some transportation operators to apply risk management practices. It also noted the TSA's intent to incorporate risk management into its decision-making and that it was in the process of developing standardized criticality, threat, and vulnerability assessment tools. [165] One year later, in a GAO review of aviation security, it found that although the TSA was conducting airport vulnerability assessments, it would benefit from a more comprehensive risk management approach. [166] In a follow-up review of TSA in February 2005, the GAO found that it still had not implemented a comprehensive risk management program. Throughout the course of GAO's work, "one theme consistently surfaced – the need for TSA to fully utilize and integrate a risk management approach into its decision making processes." [167]

With increasing national concern over rail system security, a GAO report in October 2005 found that, notwithstanding risk assessments of passenger rail systems conducted by the ODP, TSA had only just begun to establish a risk methodology, and that TSA efforts may be unnecessarily duplicating risk management activities already underway at other agencies. Like CRS, GAO noted the overlapping risk assessment

---

[164] Congressional Research Service, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences* (Washington, DC: Congressional Research Service, September 2, 2004), 1-23.

[165] Government Accountability Office, *Transportation Security - Federal Action Needed to Help Address Security Challenges* (Washington, DC: Government Accountability Office, June 2003), 36-38.

[166] Government Accountability Office, *Aviation Security - Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls* (Washington, DC: Government Accountability Office, June 2004), 43.

[167] Government Accountability Office, *Transportation Security - Systematic Planning Needed to Optimize Resources*, (Washington, DC: Government Accountability Office, February 15, 2005), 1-32.

work of ODP, TSA and IAIP, the latter having overarching responsibility for risk management across all CI/KR sectors. GAO also reported that DHS had not yet developed common and consistent risk assessment practices: "Until this framework is complete, it will not be possible for information from different sectors to be reconciled to allow for a meaningful comparison of risk — a goal outlined in DHS's interim NIPP." [168]

In December of 2005, GAO looked beyond the domain of TSA and examined how three other DHS components — the Coast Guard, ODP and IAIP — were carrying out efforts to advance risk management for port security. GAO identified the Coast Guard as being furthest along and that it, and ODP, had a relatively robust methodology in place for assessing risk. As the newest of the three components, IAIP had made the least progress, but clearly had the most complex task — addressing not just ports but all CI/KR sectors. GAO noted that IAIP was still developing its methodology and that the agency had several setbacks in completing the task. Though some progress had been made in conducting risk assessments of individual assets, there was little progress on comparisons and priority setting across ports or other infrastructure sectors — the type of assessments IAIP was set up to do. GAO opined that progress would depend on how these activities were coordinated across agencies, since current approaches are neither consistent nor comparable. GAO went on to suggest that the need for "consistency and coherence" becomes greater as individual risk management efforts mature, since the likelihood only increases that disparate programs will "fragment, clash, and work at cross purposes." [169]

In its March 2006 review of federal response to Hurricane Katrina, GAO extended its call for risk management approaches to large-scale natural disasters. GAO said that "the stand-up and sustaining of capabilities should be based on a risk assessment that would call for examining what vulnerabilities from a potential catastrophic disaster

---

[168] Government Accountability Office, *Passenger Rail Security - Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* (Washington, DC: Government Accountability Office, January 18, 2007), 1-46.

[169] Government Accountability Office, *Risk Management – Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington, DC: Government Accountability Office, December 2005), 88-97.

require attention and how they should be addressed within available resources." [170] In May 2006, GAO reinforced its push for critical infrastructure protection guidance and the need to assess the progress being made, highlighting the importance of risk management in that regard.[171] This was followed by a more in-depth report in September 2006 in which the GAO recommended a comprehensive national framework be established to address the full spectrum of catastrophic disasters by taking an "all-hazards approach" to risk management. GAO envisioned risk management being applied to guide decision-making at the federal, state, and local level. [172]

In a review of homeland security efforts to that point, a January 2007 GAO report found that "while much attention has been focused on mitigating the specific risks of 9/11, other critical assets…are also at risk of terrorist attack." GAO's review showed that while various risk assessment approaches were in use, they were neither consistent nor comparable, and that there was still no common framework "to evaluate risk assessments within sectors or across sectors." [173] GAO cautioned that implementing a national risk management framework would rest heavily on how well DHS coordinates homeland security risk management efforts with other federal departments as well as with state, local, and private-sector partners. DHS acknowledged that it could not yet assess how effective federal investments had been in mitigating risk because they did not have the metrics to do so. GAO also found that "efforts to establish guidance to coordinate a risk-based approach across DHS components have been hampered by organizational restructuring." [174]

---

[170] Government Accountability Office, *Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery*, 4-25.

[171] Government Accountability Office, *Homeland Security: Guidance and Standards are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts* (Washington, DC: Government Accountability Office, May 2006), 1-11.

[172] Government Accountability Office, *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System* (Washington, DC: Government Accountability Office, September 2006), 8-37.

[173] Government Accountability Office, *Homeland Security – Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks* (Washington, DC: Government Accountability Office, January 2007), 91.

[174] Government Accountability Office, *Homeland Security – Applying Risk Management Principles to Guide Federal Investments*, 3-32.

In January 2007, CRS was also pointing out to Congress that DHS had still not implemented a "consistent systematic approach for identifying nationally critical assets, assessing the risks they pose, and using that information to inform cost-effective allocation of resources." Though CRS did note that "the NIPP appears to provide a framework…that outlines…the steps taken in the risk assessment and risk management process…it is not clear how transparent the implementation of the plan will be." [175] In a detailed report on the evolution of DHS risk assessment practices and homeland security grant program allocation formulas, CRS cautioned Congress that…

> The lack of a coherent, long-term, overarching risk strategy…could have negative repercussions for buying down risk. Without a clearly articulated risk methodology…a baseline understanding of the Nation's risk profile may never be achieved and the…process could potentially be vulnerable to budget fluctuations and political influence. This is especially important given the apparent division of risk assessment responsibilities throughout various offices and directorates within the department. [176]

CRS went on to say that, as states and localities continue to provide information to the risk assessment process, the need to develop a national risk assessment strategy at all levels of government becomes even stronger. CRS suggested several procedural and organizational options for Congress to consider, among them to further enhance transparency of risk management policy and processes; develop a risk strategy within DHS and throughout all government agencies; appoint a DHS Risk Assessment Manager; create a Risk Advisory Board; and establish a permanent Risk Assessment Center. These recommendations were similar to those made by the president's own National Infrastructure Advisory Council (NIAC) in October 2005.

NIAC investigated whether private sector risk management experience could provide meaningful guidance on planning and programs for critical infrastructure protection. The three principal findings of the report were that standard methodologies maximize the effectiveness of risk management programs; empowered leadership and a

---

[175] Congressional Research Service, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences* (Washington, DC: Congressional Research Service, January 19, 2007), 25.

[176] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, 25-28.

supportive culture and organization are likewise essential to success; and, independent oversight of risk management enhances overall strategic direction, focus, and accountability. Accordingly, the report recommended standardization of risk management approaches; establishment of a risk management leadership role; and an oversight function to ensure accountability, promote standards, and set resource priorities.[177]

The task of developing and implementing a national risk assessment framework and associated policy and practices in support of the NIPP is immensely challenging and fraught with its own risk. However, the findings of both the GAO and CRS over the years, and the relative success of at least two DHS components in establishing risk assessment programs in their own mission areas, would seem to indicate that implementation may have more to do with organizational and institutional issues rather than matters of mechanics or methodology, as complex as these maybe.

4. Changing Roles and Responsibilities

Roles and responsibilities for leading risk assessment and risk management functions within DHS have evolved a number of times since its formation on March 1, 2003. The *Homeland Security Act of 2002* assigned DHS responsibility for coordinating the protection of the nation's critical infrastructure and key resources (CI/KR). Much of this role was delegated to the newly created Information Analysis and Infrastructure Protection (IA/IP) Directorate. IAIP was charged with carrying out vulnerability and risk assessments, preparing a national plan for CI/KR protection, and recommending specific protection measures as necessary. [178] The *Homeland Security Act of 2002* also directed that the Office for Domestic Preparedness (ODP), transferred into DHS from the Department of Justice (DOJ), be responsible for coordinating federal preparedness efforts

[177] National Infrastructure Advisory Council, *Risk Management Approaches to Protection - Final Report and Recommendations by the Council* (October 2005), 4-19.

[178] *Homeland Security Act of 2002*, 2145-2146.

and working with state, local, and tribal governments and the private sector on all matters related to combating terrorism, to include coordinating risk analysis and risk management activities. [179]

The president's strategic intent with regard to the application of risk assessment and risk management practices by the new DHS was initially outlined within the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, issued in February 2003. The strategy suggested that risk assessment and risk management had to be closely integrated and coordinated, and that industries and institutions would need to be guided by common vocabulary and standards. It also emphasized that close cooperation among all levels of government and the private sector would be essential to a shared vernacular and vision. Accordingly, the strategy called for DHS to work in collaboration with other key stakeholders to develop a "uniform methodology for identifying facilities, systems, and functions with national-level criticality to help establish Federal, state, and local government, and the private-sector protection priorities." [180] In so doing, it charged DHS with coordinating the sharing of risk management best practices between government and the private sector to build a common assessment framework. This responsibility was reiterated in late 2003 with HSPD-7. HSPD-7 directed the DHS secretary to establish "uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria." [181] It also directed SSAs to collaborate with federal departments, state and local government and the private sector to pursue vulnerability assessments and encourage risk management strategies to advance CI/KR protection efforts.

After taking office, Secretary Michael Chertoff initiated a systematic evaluation of the Department's operations, policies and structures. That second stage review was completed in June 2005. In his remarks before Congress, the secretary emphasized that

---

[179] *Homeland Security Act of 2002*, 2192.

[180] George Bush, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 22-24.

[181] George Bush, *Homeland Security Presidential Directive 7 (HSPD-7) - Critical Infrastructure Identification, Prioritization, and Protection*, 3-4.

homeland security priorities needed to be driven by risk and that a new focus on preparedness would be guided by objective measures of risk and performance. Accordingly, the secretary outlined a major reorganization that consolidated all planning, training, exercising, and funding activities into a new Preparedness Directorate, to include the Infrastructure Protection half of the former IAIP. What was the Information Analysis (IA) half of IAIP would become the new Office of Intelligence and Analysis (OIA). [182] With major changes in the alignment of DHS components, missions, and leadership came changes in the continuity and direction of risk management programs as well. But these would not be the only changes. Hurricane Katrina would be the unlikely catalyst for yet another major DHS reorganization the following year.

The *Post-Katrina Emergency Reform Act* was signed into law in October 2006, as part of the *Homeland Security Appropriations Act* of FY 2007. In January 2007, the DHS secretary implemented the requirements of the Act by directing organizational changes that abolished the Preparedness Directorate, just over a year old, and reallocated a number of other key DHS components to FEMA. Those reassigned functions included what was Grants and Training (G&T) under the Preparedness Directorate, formerly ODP when the Department was first created. G&T would become simply Grant Programs under an expanded FEMA, taking along its risk assessment technical assistance initiative. While complying with the Act, the secretary also made other organizational changes, the most significant of which was the creation of the new National Protection and Programs Directorate (NPPD). NPPD is currently made up of the US-VISIT program; the Office of Intergovernmental Programs; the Office of Cyber Security and Communications; the Office of Infrastructure Protection (OIP); and the new Office of Risk Management and Analysis (RMA). [183] Established in April 2007, RMA assumed the lead role for coordinating all DHS risk management efforts from OIP. Another recently created organization with a major role in national risk assessment and management efforts is the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). An overview of

---

[182] Michael Chertoff, "U.S. Department of Homeland Security Second Stage Review" (statement before the United States Senate, Committee on Homeland Security and Government Affairs, Washington, DC, July 14, 2005), 1-14.

[183] Federal Emergency Management Agency, *Implementation of the Post-Katrina Emergency Management Reform Act*.

current risk assessment and risk management roles and responsibilities of these DHS components follows. This information was primarily obtained from recent DHS briefing materials and a report to Congress on the status of DHS risk management efforts.

Office of Risk Management and Analysis (RMA) – RMA is now tasked with leading DHS efforts to establish a common framework to address the overall management and analysis of homeland security risk by coordinating national risk policy, risk analysis and assessment methodologies as well as risk management efforts by synchronizing and leveraging assets across DHS. RMA is to support federal, state, local, and private sector efforts to implement and institutionalize risk-based programs by promoting cross-department and interagency coordination on risk issues, promoting generally accepted risk assessment and management principles, and developing a common vocabulary for risk analysis and risk management. Subordinate functions within RMA include risk doctrine and policy, risk analysis, risk management, and risk performance. DHS executive guidance and direction to RMA is to come from a Risk Steering Committee chaired by the undersecretary for National Protection and Programs and whose membership is drawn from the various components of the Department. [184] Newly established, as of this writing, RMA is still in its formative stages, developing its organization and building its staff.

Office of Infrastructure Protection (OIP) – OIP is in a state of transition with regard to DHS risk assessment and risk management efforts. Initially responsible for taking the lead on risk assessment and management across DHS, its role has been steadily refocused with successive changes in DHS organization to include the creation and then abolition of the Preparedness Directorate, followed by the formation of NPPD and RMA. As has been its mission, OIP has conducted threat and risk analysis across CI/KR sectors, at the sector, geographic, and national levels for federal, state, local, and private sector partners. A major product for senior-level homeland security decision makers is the National CI/KR Protection Annual Report which includes the National CI/KR Risk

[184] U.S. Department of Homeland Security, "National Protection and Programs Directorate – Office of Risk Management and Analysis" (briefing slides, August 6, 2007), 9-14.

Profile. [185] In addition to the above, much of OIP's current work portfolio revolves around the implementation of the National Infrastructure Protection Plan (NIPP), to include a national risk management framework for CI/KR protection.

The Risk Analysis and Management for Critical Asset Protection (RAMCAP™) initiative has been one of OIP's main strategies for advancing the NIPP risk management framework. RAMCAP™ is intended to facilitate the DHS partnership with industry to implement a common and compatible risk assessment regime across industry sectors and levels of government. However, the program has yet to obtain broad acceptance. To date, RAMCAP™ has been adopted for use in three of seventeen CI/KR sectors: chemical manufacturing, nuclear power and energy. Two more are reported to be underway; water and wastewater treatment, and dams. [186] As previously stated, the future application of RAMCAP™ across the remaining twelve CI/KR sectors is uncertain. Moreover, it appears that some functions, previously the domain of units internal to OIP, are in transition to another new DHS organization – HITRAC.

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) – HITRAC is a unique joint program office shared by OIA and OIP and designed to integrate the intelligence and infrastructure capabilities and expertise of these two components. Its purpose is to create and disseminate risk-informed analytic products to influence the prioritization of strategies designed to attain the greatest reduction of risk and best investment of national resources for the protection of critical infrastructure. This blending of intelligence and critical infrastructure protection functions was an intent never realized in the original IAIP and, by default, all but abandoned with the creation of the Preparedness Directorate in 2005. HITRAC products are intended to "support the security planning of state and local governments and CI/KR owners and operators, as well as an integrated national response to emergent threats or immediate incidents." [187]

---

[185] U.S. Department of Homeland Security, "Improving Use of Risk-Informed Decision-Making in DHS - Report to Congress in Response to House Report 109-476 to the Fiscal Year 2007 Department of Homeland Security Appropriations Bill" (Washington, DC: U.S. Department of Homeland Security, March 2007), 9-10.

[186] Carolyn Maloney, letter.

[187] Melissa Smislova and Brandon Wales, "The Homeland Infrastructure Threat and Risk Analysis Center" (briefing presented at the First Annual Conference of the Security Analysis and Risk Management Association, Washington, DC, May 22, 2007) 3-4.

As a joint program of OIA and OIP, direction is set by an executive board that consists of the undersecretary of the NPPD, the assistant secretaries of OIA and OIP, and the deputy assistant secretary of Intelligence and Analysis for Intelligence, or their designees.

Two primary functions within HITRAC are the Infrastructure Analysis Branch and the Risk Integration and Analysis Branch. Infrastructure Analysis analyzes threats and risks to critical infrastructure by sector and sub-sector and prepares reports in coordination with and in support of federal, state and local authorities and the private sector. Risk Integration and Analysis coordinates and develops the National CI/KR Risk Profile and the Strategic Homeland Infrastructure Risk Assessment (SHIRA). It develops lists of the most critical CI/KR assets to support DHS grant programs; lists that serve as the focal point of OIP's critical infrastructure protection planning activities with all of its stakeholders. The branch also identifies new and improved risk methodologies to support new or updated infrastructure risk analysis and other CI/KR risk-related programs. [188]

Based on the limited information obtained to date, it is yet unclear as to what the relationship and division of labor is between HITRAC functions and the role of RMA and OIP. This is particularly important as it relates to the identification and implementation of new risk assessment methodologies and coordination with non-federal partners in the implementation of the NIPP risk management framework. Nor is it clear how risk practices established at the national level and in use by HITRAC will integrate with, and both inform and be informed by, risk practices in use by or to be implemented within individual CI/KR sectors and/or by other DHS components (i.e., ODP, TSA, and USCG).

[188] U.S. Department of Homeland Security, "Requested Materials Produced for John P. Paczkowski, Director of the Office of Emergency Management, Port Authority of New York and New Jersey" (August 24, 2007), 2-6.

IV. STRATEGIC CHANGE, PUBLIC POLICY, AND COMPLEXITY

A. MANAGING STRATEGIC CHANGE

1. Change and Strategic Management in the Public Sector

In his seminal work *Leading Change*, John Kotter describes the powerful social and economic forces at work that drive major strategic change in organizations. Though he acknowledges how major change efforts have helped some organizations adapt to the new realities of a volatile marketplace, he also cautions that his study of over one hundred major change efforts reveals, more often than not, that change has "been disappointing and the carnage has been appalling, with wasted resources and burned-out, scared, and frustrated employees." [189] In his view, however, much of this waste and anguish is avoidable if managers can learn from the most common mistakes of the past. In a similar way, Rick Jackson describes the results of a 2005 workshop of senior government and private sector leaders that addressed strategic change in the federal government. He cites the numerous "transformation initiatives" under way by major governmental agencies and opines that, despite the best efforts of the people involved, many of these initiatives will not survive changes in leadership and what he calls the "gravitational pull of the status quo." [190] Like Kotter, he too acknowledges that there have been success stories, but reinforces the need to learn from the past.

A white paper by the Public Governance Institute, in association with noted change consultant Daryl Conner, provides another stark and sobering view of the realities of achieving large-scale change, particularly in the public sector and as it relates to homeland security policy. The paper describes how when major changes are announced, typical senior policy-makers may see it as the end of their work when, in reality, the real struggle is just beginning, with a long hard road that stretches from the initial statement

---

[189] John Kotter, *Leading Change* (Boston: Harvard Business School Press, 1996), 3-4.

[190] Rick Jackson, "Achieving Strategic Change in Government," *Public Manager* 34, no. 1 (Spring 2005): 40-50.

of a policy's intent to the realization of its aims. It goes on to describe how the business landscape is "littered with the carcasses of impeccable solutions that either failed outright or achieved much less than was expected." [191] A large number of change initiatives that failed to realize their original intent, it contends, end up on "history's garbage heap" after accomplishing little. Too often public policy change efforts to address critical problems fall short of what policy-makers, organizations, and/or government agencies originally intended. The reason the paper gives is poor implementation and a failure of the leaders responsible to understand the dynamics involved in managing these changes effectively. Both private and public sector strategic change in this modern age involve increasing levels of organizational complexity and are, more often than not, conducted in an environment that is turbulent and often hostile to the change intended.

According to Theodore Poister and Gregory Streib, strategic management is vital to good public governance in that it integrates all major activities and functions and directs them toward advancing an organization's strategic change agenda, particularly as it relates to substantive policy. In their view, strategic management provides a "systematic, coherent, and effective approach to establishing, attaining, monitoring, and updating an agency's strategic objectives." [192] Strategic management, they say (a) focuses attention across functional boundaries and organizational levels on common goals, themes, and issues; (b) ties internal management processes and program initiatives to desired outcomes in the external environment; and (c) links operational, tactical, day-to-day decisions to longer-term strategic objectives. Though Poister and Streib state that public sector managers have a number of options for influencing people and programs and bringing about organizational change, they suggest that these options cannot be used effectively without the clear sense of vision, mission, values, and strategy that comes from strategic management. It provides them with the ability they need to identify emerging issues and understand their implications; craft viable strategies and mobilize

---

[191] Public Governance Institute, "White Paper – Launching Change Versus Realizing New Outcomes" (Public Governance Institute – Leading Public-Sector Change, n.d.), http://www.publicgov.org/LeadChange/WhitePaper/intro.html [Accessed: July 15, 2007].

[192] Theodore Poister and Gregory Streib, "Strategic Management in the Public Sector: Concepts, Models, and Processes," *Public Productivity & Management Review* 22, no. 3 (March 1999): 308-325.

support; communicate the vision in a compelling way; and build the relationships and management structure needed to implement and sustain change.

In Lewis Carol's Alice in Wonderland, the Cheshire cat says to Alice, "If you don't know where you are going, any road will take you there." A strategic management framework is an essential foundation from which to identify the need for and guide strategic change, whether an internal transformation effort or the implementation of a far-reaching homeland security policy having national scope. However, though essential, it is not in itself sufficient. In undertaking any major public-policy change, whether it be health care reform or homeland security, it is vital for those involved in policy implementation to fully understand the political and organizational dynamics, the forces arrayed both for and against the change proposed, and what can reasonably be accomplished by which methods according to a certain time horizon. It will also be vital to learn from prior experience and use of proven change management techniques.

2. Models for Understanding and Guiding Strategic Change

There are numerous theories and models related to the dynamics of organizational performance and change management. Salvatore Falletta provides a useful guide which provides an overview of eleven of the most popular models employed by practitioners of organizational change. These range from the older and better known Force Field Analysis by Kurt Lewin to the more comprehensive Technical Political Cultural (TPC) Framework by Noel Tichy and Causal Model of Organizational Performance and Change developed by Warner Burke and George Litwin, also known simply as the Burke-Litwin Model. Organizational models are not designed to be an exact representation of an organization or organizational system, but instead are intended to help managers understand more clearly the range of dynamics at work in such systems and the relationship of these dynamics to one another. Armed with this understanding, managers may then more deliberately and effectively assess an organizational system's current state and design strategies to achieve the changes desired, either in the system's performance or the implementation of new policy or both. According to Falletta, without such models, managers and change practitioners must rely on intuition and hunches as they deal with

the massive amounts of information and complexity associated with major organizational change efforts. [193] Doing so could lead to missing key factors and result in the failure of the change effort to achieve its aims.

Models are not prescriptive and no single model can fully represent all of the factors relevant in all possible settings. Some models may fit a particular circumstance and some may not. Likewise, using just one model runs the risk of seeing the challenge from only one perspective and thus it may be appropriate to apply multiple approaches to gain alternative views. It is with this caution that only two approaches – the Burke-Litwin Model and the TPC Framework – are highlighted here as representative of the diverse and complex set of factors to be considered in any large-scale change effort.

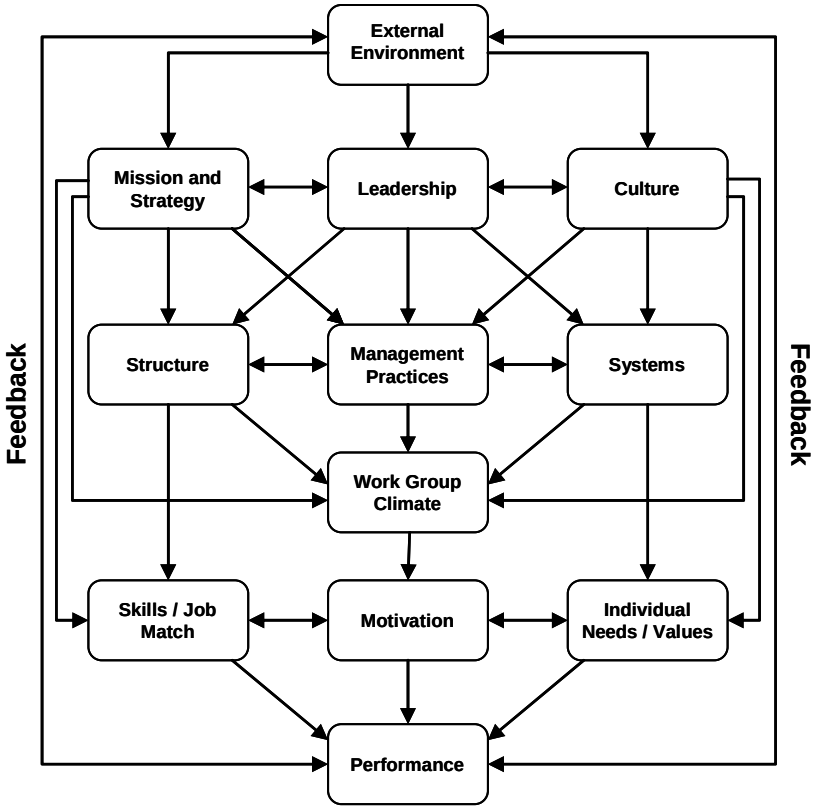

Figure 7. Burke-Litwin Model of Organizational Performance and Change.

[193] Salvatore Falletta, "Organizational Diagnostic Models: A Review & Synthesis – White Paper" (Leadersphere, Inc. 2005) 3-5.

As discussed by Falletta, the Burke-Litwin Model is relatively new and includes several key features which go beyond previous approaches (see Figure 7). As described by Burke and Litwin, it identifies twelve organizational variables; depicts the difference between the culture and the climate of an organization; distinguishes transformational from transactional dynamics; specifies the nature and direction of influence of the variables; and is well grounded in organizational development theory and practice. [194] With the realistic recognition of influences coming from the external environment, and the representation of a feedback loop, the model demonstrates the "open systems" theory that underlies its design. It is particularly well suited to understanding organizational performance issues and guiding organizational transformation efforts within a single organization.

Less complicated, and perhaps more germane to the discussion of organizational and strategic change issues related to public policy implementation, is Tichy's Technical Political Cultural (TPC) Framework or what he also refers to as The Network Model. In this model, Tichy views organizational systems not as management hierarchies, but as systems of social networks or clusters of people joined together by a variety of formal and informal relationships, with only part of the structure officially prescribed. He suggests that the dynamic relationships among the various parts of this system, and the degree to which the system is aligned, must be assessed from three different perspectives: technical, political, and cultural. [195] These perspectives are closely interrelated and, to underscore this point, Tichy uses the metaphor of a rope where each of these perspectives represents an individual strand. Most significant in the TCP Framework is his emphasis on the importance of "emergent networks" (see Figure 8).

Tichy recognizes that unplanned, informal social structures or networks emerge in all organizational settings. He sees them as having both desirable and undesirable characteristics for change, depending on how they are managed. Informal networks often emerge because formal structures are unresponsive, too slow, or perhaps even

---

[194] Warner Burke and George Litwin, "A Causal Model of Organizational Performance and Change," *Journal of Management* 18, no. 3 (1992): 523-545.

[195] Noel Tichy, *Managing Strategic Change – Technical, Political, and Cultural Dynamics* (New York: John Wiley & Sons, 1983), 69-73.

counterproductive to the need for change. To paraphrase Tichy, individuals may develop informal relationships to reformulate or reinterpret the mission or policy, change prescribed processes, alter technology or methods, and otherwise differentially respond to changing environmental conditions. [196] Such networks can hinder strategic change, but still others can serve to enhance and accelerate it.

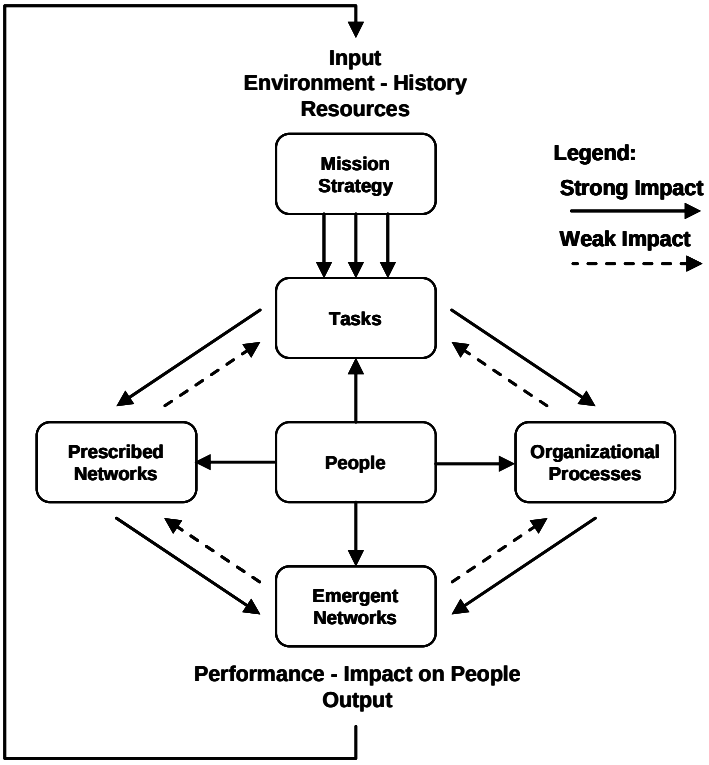

Figure 8. Technical Political Cultural (TPC) Framework.

Emergent networks breed emergent change. Karl Weick takes the view that "planned transformational change, complete with its talk of revolution, discontinuity, and upheaval, presents a distorted view of how successful change works." [197] This, he contends, has caused some to overestimate the problem of inertia and the centrality of managerial planning, and to underestimate the importance of innovative sense-making, the ability of small experiments to travel, and the extent to which change is actually a continuous process. He makes the case that emergent, continuous change is a significant

[196] Noel Tichy, *Managing Strategic Change – Technical, Political, and Cultural Dynamics* (New York: John Wiley & Sons, 1983), 93-94.

[197] Karl Weick, "Emergent Change as a Universal in Organizations," in *Breaking the Code of Change*, ed. Michael Beer and Nitin Nohria (Boston: Harvard Business School Press, 2000), 223-241.

factor predicting whether episodic change (i.e., a major transformation effort or implementation of national policy) will succeed or fail. According to Weick, among the advantages of emergent change are its capability to increase readiness for and receptiveness to planned change; sensitivity to local contingencies; suitability for experimentation, learning, and sense-making; likelihood of satisfying needs for autonomy, control, and expression; proneness to swift implementation; the ability to exploit tacit knowledge; and shortened feedback loops from results to action. He adds that actual change is less management-induced and more a function of the choices and actions of frontline stakeholders. Weick concludes his discussion by suggesting that managers must recognize the power of emergent change within the context of their planned change efforts. Thus, understanding the nature of emergent networks, avoiding their negative aspects, and exploiting their full potential can be vital to success in dealing with the complexity of large-scale change.

3. Determinants for Success in Strategic Change

In 1995, John Kotter published an article in the *Harvard Business Review* entitled "Leading Change: Why Transformation Efforts Fail." Compared to much of the theoretical leadership and organizational development literature of the time, it posed a commonsense analysis of why change efforts rarely achieve their desired results and what practical steps might be taken to increase the chances of success. More than a decade later, this *HBR* article and his book, *Leading Change*, remain fundamental guides for change agents in both private and public sector organizations. [198] In Kotter's study of over 100 large-scale change efforts, he found that only a few were actually successful, a few others were utter failures, and most fell somewhere in between, with most not being very successful at all. His analysis of those efforts resulted in the identification of eight common mistakes leaders make in implementing change and strategies to avoid them.

[198] John Kotter, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review* 73, no. 2 (March-April 1995): 59-67.

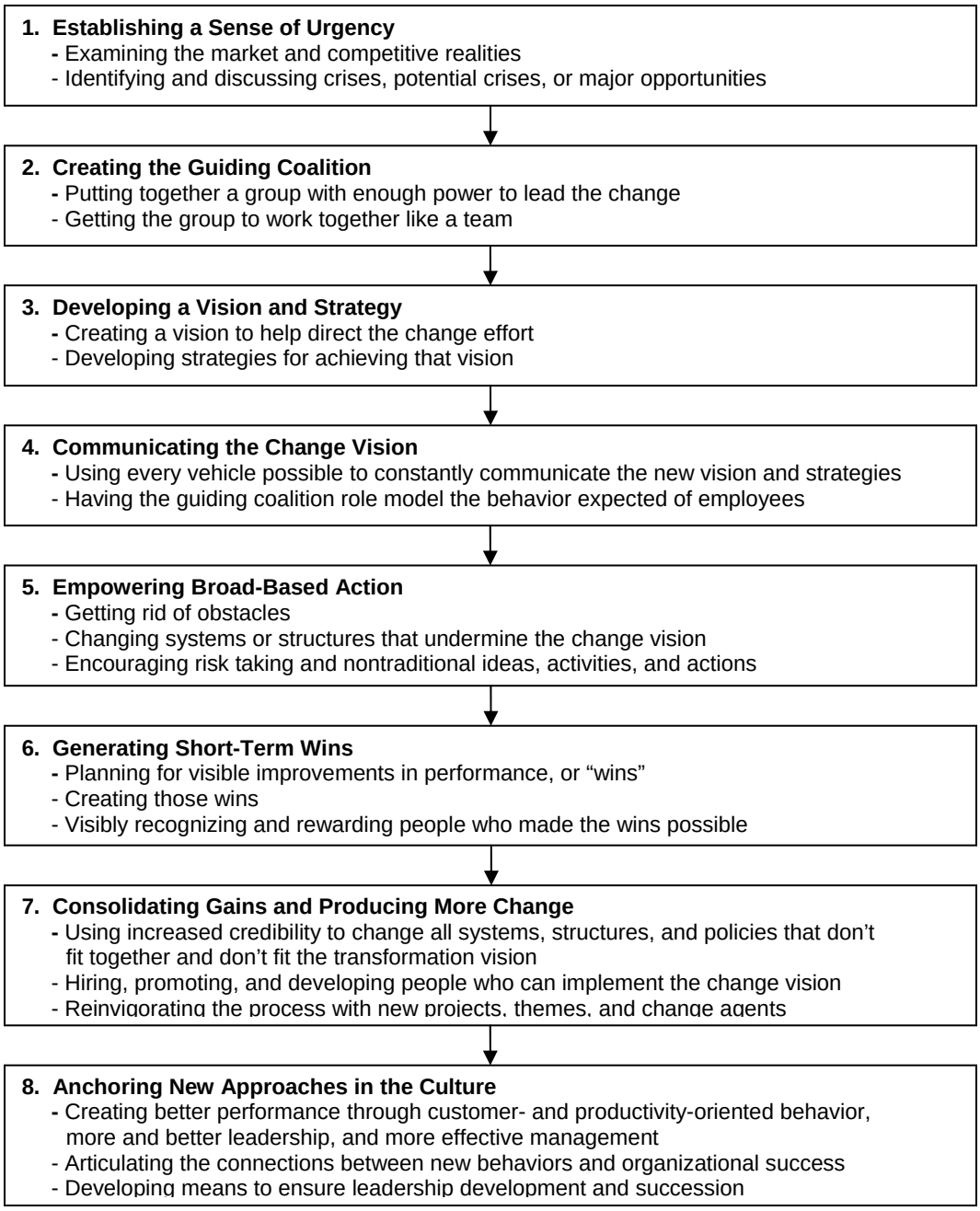

Figure 9. The Eight-Stage Process of Creating Major Change. [199]

In presenting his Eight-Stage Process for Creating Major Change, Kotter states that the common mistakes he outlines are not inevitable and that the key lies in understanding the dynamics involved, how a deliberate multi-stage process can mitigate

[199] Kotter, *Leading Change*, 61.

potential errors, and more significantly, how strong effective leadership is required throughout. The underlying theme of his work is that managers tend to underestimate the level of effort involved, and the fact that change is a people process that must be led rather than simply managed. Moreover, he emphasizes that this process must move through deliberate stages and that bypassing any stage, or getting too far out of phase, always creates difficulty and could sow the seeds of failure (see Figure 9). [200]

Kotter acknowledges that, unlike his other research, the concepts contained in his work on *Leading Change* are not drawn from the ideas of others but on his own firsthand experience and extensive analysis of real-world, large-scale strategic change efforts. However, his eight-stage process has received further support through the work of Sergio Fernandez and Hal Rainey, who have done an extensive review of organizational change research as it may apply to large-scale planned strategic change in the public sector. These authors cite the lack of current research on organizational change in government and the complex, confusing, and sometimes conflicting array of research findings and theories that serve to confound public sector managers looking for guidance.

In response to the need for clear advice to public sector managers, Fernandez and Rainey have assessed the major theoretical perspectives on organizational change to include a range of change management models and frameworks such as those discussed in the previous section. They also considered research related to governmental reform, innovation, and policy implementation as a way to filter out factors that are most relevant to large-scale strategic change in the public sector. Finding significant congruence on key points within the research literature, they developed a set of Determinants for Successful Implementation of Organizational Change in the Public Sector. [201] These eight propositions are very similar to the eight-stage process proposed by Kotter, but have been synthesized from the research and tailored to the public sector (see Figure 10). This list is adapted from the original presented by Fernandez and Rainey, and has been edited for purposes of brevity. Though elements of both lists have merit, like the organizational

---

[200] Kotter, *Leading Change*, 20-49.

[201] Sergio Fernandez and Hal Rainey, "Managing Successful Organizational Change in the Public Sector: An Agenda for Research and Practice," 1-24.

change models, they are only a guide, and various elements may be more salient in some situations and not others. Public sector leaders will need to adapt their use accordingly.

Ensure the Need Managerial leaders must verify and persuasively communicate the need for change.	- Convince organizational members of the need and desirability for change. - Craft a compelling vision of change. - Communicate the need for change.
Provide a Plan Managerial leaders must develop a course of action or strategy for implementing change.	- Devise a strategy, with milestones and a plan. - The strategy should be clear and specific. - The strategy should rest on sound causal theory for achieving the desired end state.
Build Internal Support / Overcome Resistance Managerial leaders must build internal support and reduce resistance to change through widespread participation in the change process.	- Encourage participation and open discussion. - Avoid criticism, threats, and coercion. - Commit sufficient time, effort and resources to manage participation effectively.
Ensure Management Support / Commitment An individual or group within the organization should champion the cause for change.	- An "idea champion" or guiding coalition should advocate for and lead the transformation process. - Should have the skills needed to marshal support. - Political appointees should support the change.
Build External Support Managerial leaders must develop and ensure support from political overseers and key external stakeholders.	- Build support for and commitment to the change among political overseers. - Build support and commitment among interest groups with a stake in the organization.
Provide Resources Successful change usually requires adequate resources to support the change process.	- Provide adequate financial, technological, and human resources to implement change. - Avoid overtaxing organizational members. - Capitalize on synergies in resources.
Institutionalize Change Managers and employees must effectively institutionalize the changes.	- Displace old behaviors; institutionalize new ones. - Monitor the implementation of change. - Institutionalize change before shifts in leadership cause commitment and support to diminish.
Pursue Comprehensive Change Managerial leaders must develop an integrative, comprehensive, approach to change that achieves subsystem congruence.	- Implement a comprehensive and consistent set of changes to the subsystems of the organization. - Analyze and understand interconnections between subsystems before pursuing congruence.

Figure 10. Determinants of Successful Organizational Change in the Public Sector. [202]

[202] Fernandez and Rainey, "Managing Successful Organizational, 7, Table 1 (Adapted by the author for brevity.).

4. Leadership and Strategic Change

As can be seen from the organizational change models and the determinants of success discussed on the preceding pages, central to any major large-scale strategic change effort is leadership. Determining what kind of leadership is exercised by whom, under what circumstances, and when, is truly the art of executing any transformation, even one to bring about a new public policy or program. Establishing a vision, organizing resources, motivating and guiding participation, overcoming resistance, and maintaining accountability for success are all vital leadership tasks. Though much has been written on the matter of leadership, and specifically on leading large-scale strategic change, there are still differing views on which approaches are most effective.

Jay Conger takes the traditional view that top-led strategic change has a far better chance of success than that driven by lower levels of an organization. He argues top-led strategic change generally results from major shifts in strategy or the reengineering of core processes. Given the magnitude of such change, the level of investment, and the high stakes involved, he states that top executives are in a much better position to lead it. Conger cites three factors that support top-led strategic change. [203] First, members of top management have a "breadth of perspective" and a vantage point that permits them to see the change in all its dimensions. Second are the "attributions of leadership," where senior executive positions have symbolic importance that permit them to use events and their own behaviors to send messages about what is important and where attention should be placed. Third, Conger notes they have "power of position"; while this is the most obvious factor and often overestimated, is more than that of subordinates. Despite political influences that can limit their power, senior executives still have the ability to set priorities, allocate resources, and hire, fire, reward, and sanction behavior as necessary to shape the direction and dynamics of change. Though he favors top-led change, Conger does not underestimate the value of a team approach or engaging lower levels of the organization as active participants. Important here is his emphasis on the continuous and direct involvement of top management with the power to make things happen.

---

[203] Jay Conger, "Effective Change Begins at the Top," in *Breaking the Code of Change*, ed. Michael Beer and Nitin Nohria (Boston: Harvard Business School Press, 2000), 99-112.

Celebrated author and consultant on leadership Warren Bennis observes that the vision of the single heroic leader is a myth, one tied to our own tendency to deify social, political, and industrial icons. He states that a society as complex and technologically sophisticated as ours requires leadership and contributions from all levels and all spheres. According to Bennis, in any large-scale endeavor, there are too many problems to be solved and too many connections to be made to think that any one leader could influence it all. He sees the top-down leadership model as "maladaptive" in an environment of extraordinary complexity, ambiguity, and uncertainty. He further opines that "exemplary leadership and organizational change are impossible without the full inclusion, initiative, and cooperation of followers." [204] Going beyond simple participation, Bennis suggests that complex messy problems, involving many stakeholders, require complex and diverse alliances. He points out that, as today's organizational structures are evolving into networks, cross-functional teams, temporary systems, and ad hoc task-forces, leaders must have not the loudest voice but the most attentive ear and exercise leadership that values and encourages participation, diversity of views, and dissent.

The paradox of top-down versus participative leadership is that both views are correct. In assessing this paradox, Dexter Dumphy leaves no doubt that executive leadership is essential to change management. [205] However, as traditional, vertically integrated, bureaucratic organizations become a thing of the past, they are being increasingly replaced by alliances, interest groups, and temporary fluid relationships. As such, the nature of leadership must change as well. Dumphy reiterates the call by Bennis for a new kind of alliance between the leaders and the led. He also supports the continued need for a unified executive team to develop strategic intent, but goes on to suggest that the executive team must also invest the time and resources necessary to create the environment and structure for such participation. They must systematically invest in key personnel, professional, and corporate capabilities that support meaningful participation. So leadership is still vital to change, but in a different way.

---

[204] Warren Bennis, "Leadership of Change," in *Breaking the Code of Change*, ed. Michael Beer and Nitin Nohria (Boston: Harvard Business School Press, 2000), 113-121.

[205] Dexter Dumphy, "Embracing Paradox," in *Breaking the Code of Change*, ed. Michael Beer and Nitin Nohria (Boston: Harvard Business School Press, 2000), 123-135.

The discussion of leadership on the preceding pages is somewhat limited in that it mostly addresses change from within single organizations, and mostly from a private sector business perspective. Traditional views of top-down leadership of strategic change are even less valid in the inter-agency public sector arena, and especially so regarding the implementation of strategic change in the form of major homeland security public policy. Most officials in government bureaucracies have the power of legislation and regulation to influence compliance with new public policy, but this is not always so for homeland security policy, which requires the often voluntary compliance of others. Though not faced with the same leadership challenges of a Gandhi or Martin Luther King, when working simultaneously across federal departments, down through layers of government, and with private sector industry, homeland security leaders must often lead without authority and find ways to influence change through other means.

Richard Heifetz points out that since we are used to seeing leadership and authority as two sides to the same coin, the notion of leadership without authority is alien to us, and as such, analysts have generally not paid much attention to the problems and opportunities of mobilizing work from positions of little or no authority. Leadership, he states, is primarily about engaging people to address problems. Since addressing problems requires learning, the task of leadership is primarily one of education; choreographing and directing that process through introducing new ideas and changing attitudes and behaviors. According to Heifetz, leading without authority often involves raising questions that disturb the status quo, focusing on a single issue and not having to contend with meeting the expectations of multiple constituencies all at once, and getting closer to stakeholders to obtain frontline information necessary to achieve the leader's aims. This is essential since the leader has little control over the environment. As Heifetz puts it, one can shape the stimulus, but one cannot manage the response. [206] He thus describes leadership without authority as a process of modulating provocation. It requires attracting attention to an issue and directing that energy to the questions that must be addressed, while at the same time providing a context for action. This also requires mobilizing stakeholders in support as a growing base of legitimacy.

---

[206] Ronald Heifetz, *Leadership Without Easy Answers* (Cambridge: Belknap Press of Harvard University Press, 1994), 183-231.

B. IMPLEMENTING PUBLIC POLICY

1. The Public Policy Process

Through their research, Deborah McFarlane and Marilyn Gruebel make the point that public management and public policy implementation are inextricably linked. An understanding of the process of public policy implementation and the factors that decide success or failure are vital to effective governance. Public agency executives and policy makers need to know "what levers to pull" to successfully implement programs to achieve public policy aims. [207] Thomas Birkland sees the study of public policy as encompassing "those decisions made (or implicitly accepted) by government and non-governmental actors to address a problem that a significant number of people and groups consider to be important and in need of a solution." [208] Though he acknowledges that there is no consensus on a definition of public policy, he lists some basic definitions offered by other researchers. A melding of a few of those definitions may serve to set the stage for the discussion that follows. Accordingly, public policy can be defined as "…political decisions for implementing programs to achieve societal goals…" and represents "…the sum of government activities, whether acting directly or through agents, as it has an influence on the life of citizens." [209] It is firmly grounded in the political process, the exercise of power, interplay among interests groups, the institutions that make policy, and the ways in which policy is formulated and implemented.

In their book on public policy implementation, Michael Hill and Peter Hupe acknowledge that the results of policy implementation are sometimes disappointing, and perhaps even worse. They state that the standard reaction to a failure of public policy to achieve its aims is to blame the implementers of that policy, whether justified or not. [210] These researchers point out that public policy implementation is to a great degree

---

[207] Deborah McFarlane and Marilyn Gruebel, *Public Management and Policy Implementation: Intersection, Subset, or Neither?* (paper presented at the Fall Conference of the Association for Public Policy Analysis and Management, Madison, Wisconsin, November 3, 2006).

[208] Thomas Birkland, *An Introduction to the Policy Process: Theories Concepts and Models of Public Policy Making, 2nd ed*. (Armonk, NY: M.E. Sharpe, Inc., 2005), 5-18.

[209] Ibid., 5-18.

[210] Michael Hill and Peter Hupe, *Implementing Public Policy* (London: Sage Publications, 2002), 161.

impacted by the context in which the policy will be implemented and the way policy objectives are understood or interpreted by policy framers, implementers, and the frontline stakeholders, the latter being the actors who must put the policy in effect. Hill and Hupe opine that policies as formulated at the national level may be seen as less clear and directive to implementers and front-line stakeholders than the original policy-makers may think. Policies are also often a matter of politics and compromise and, as these researchers suggest, are "seldom the fruit of pure intellectual cognition." [211] As such, Hill and Hupe state that the messages to implementers can be ambiguous and that it is little wonder that there is difficulty in knowing not only what to implement but how to implement a given policy.

If implementers in the middle are uncertain about ambiguous policy objectives, so too will be those actors on the front line who must put that policy into practice. This difficulty is compounded by the number of horizontal and vertical relationships that may be involved, and differing agendas and perceptions of the policy and its implications. To manage these issues, Hill and Hupe offer an adaptive approach to governance of the public policy implementation process across three levels of activity: managing the policy process, managing inter-organizational relations, and managing internal and external contacts. Depending on the contingencies involved, they recommend three basic perspectives for implementers to consider when formulating implementation strategy. Governance-by-authority is an enforcement perspective and implies well-defined policy objectives, explicit responsibility, clarity on procedures, and an ability to motivate compliance. In governance-by-transaction, implementation is from a performance perspective, where emphasis is on prescribed outputs and managing contract compliance. As such, the focus is on interfaces and inter-organizational relations and clarity of expectations in the performance contract itself. When the policy objectives and methods are less clear, governance-by-persuasion becomes the appropriate implementation perspective. It emphasizes co-production, with a focus on managing outcomes as shared results. This perspective involves forming partnerships, inviting stakeholders to participate, and allowing discretion in achieving implementation objectives and

[211] Hill and Hupe, *Implementing Public Policy*, 162-163.

coordinated service delivery. It also involves professionalization, institutionalizing participation, peer assessment, and mutually agreed upon procedures for compliance. [212]

Birkland describes a set of public policy models that have evolved over time as representations of what is otherwise a chaotic and sometimes unpredictable process of development and implementation. The Systems Model of politics and policy he describes is represented by a simple set of inputs, policy-making, and outputs. Inputs include issues, pressures, information, and the influence of decision makers, and outputs are the resulting decisions, procedures, regulations, and laws. In between is a political "blackbox" that transforms political policy intent through structural, social, political, and economic environments that influence policy-making activity. Another representation of the policy process outlined by Birkland is the Stages Model where policy activity moves through a cycle of issue emergence, agenda setting, alternative selection, enactment, implementation, and evaluation. [213] Though useful as simple metaphors for the policy process, such models may be overly simplistic to be of much use in understanding formulation of complex policy such as that related to homeland security.

John Kingdom goes beyond the Stages Model in assessing the research and relates the policy process to "organized anarchy," which he describes as having three general properties: problematic preferences, unclear technology, and fluid participation. As more precision is applied to initially "fuzzy" political goals, conflict emerges. In organized anarchies, the process or technology involved is not clearly understood, and learning is through trial and error. With regard to policymaking, Kingdom describes three streams of activity: problem recognition, the formation and refining of policy proposals, and politics. Involved, according to Kingdom, are a diverse range of actors – bureaucrats, Hill staffers, academicians, special interest groups, and researchers, all with their own perspective on the issues and solutions to them. This process goes on, as he describes it, in a political environment shaped by swings in national mood, election results, changes in administration, and interest group pressure campaigns. In such a chaotic environment, these streams occasionally converge to form what Kingdom calls a "policy window"

---

[212] Hill and Hupe, *Implementing Public Policy*, 187-190.

[213] Ibid., 201-225.

when the conditions are right for implementation. Miss the window and stakeholders must wait for the next opportunity. Thus policy implementation is not only dependent on understanding a chaotic process, but a matter of timing opportunity as well. [214]

2. Alternative Perspectives on Public Policy Implementation

In a review of policy implementation research, Richard Matland outlines a decision model offering alternative strategies to guide successful management of public policy implementation, and frames these strategies relative to the degree of ambiguity and conflict associated with the policy's original intent. Not unlike the approaches to organizational leadership previously discussed, he describes the two basic schools of thought in the policy implementation literature as top-down and bottom-up. According to Matland, the top-down approach emphasizes that policy designers alone are the central actors, policy goals should be clear and consistent, and responsibility for implementation should lie with the central agency most supportive of the policy's goals. Implementation is for the most part administrative in nature, and political influence is ignored or somehow eliminated, with local actors seen as potential impediments that need to be controlled. [215] He notes that legislation often requires ambiguous language and contradictory goals to obtain support and win its passage, and that it is rarely possible to separate politics and special interests from policy administration. He further cautions that attempts to insulate inherently political subject matter from politics may lead directly to policy failure. This would logically include not only elected leaders and inter-agency politics, but outside stakeholder influence as well.

As Matland describes it, the alternative bottom-up view is based on the premise that policy is really made at the local level and that local actors have expertise and knowledge of the issues essential to successful policy implementation. The bottom-up approach argues that local discretion is so great that it is simply unrealistic for a central

---

[214] John Kingdom, *Agendas, Alternatives, and Public Policies, 2nd ed.* (New York: Addison-Wesley Educational Publishers Inc., 2003), 84-89.

[215] Richard E. Matland, "Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation," *Journal of Public Administration Research and Theory* 5, no. 2 (April 1995): 145-174.

authority to control the action. Matland indicates that bottom-up theorists see policy implementation, by necessity, occurring at two levels. Central actors devise a program to implement a policy and then local actors react to those plans, possibly developing and implementing their own programs in response. He cites research which suggests that most problems arise in the implementation of policy by local actors, with central actors (i.e., federal agencies) only indirectly influencing local factors. Matland concludes, there can be wide variation in how national policy is implemented at the local level.

Matland goes on to say that, according to bottom-up theorists, local context can dominate the implementation of policy, leaving central actors unable to fully control the process. These theorists see implementation as anything but context free in that it actually takes place as a function of the interaction of policy and its local implementation setting. Thus "the goals, strategies, activities, and contacts of the actors involved in the implementation process must be understood in order to understand implementation." [216] Success, bottom-uppers argue, depends on the knowledge and abilities of local actors who can adapt policy to local conditions. Central authority, they believe, actually has little influence on the final outcome. Absence of local freedom to adapt the program, they argue, will likely be another factor that could cause implementation of a policy to fail.

In the literature on leading strategic change, there exists a paradox of top-down versus bottom-up approaches in the implementation of national public policy that must be considered by federal policy-makers and public sector managers. Public policy at the national level is complex and fraught with potential disagreement. The initial strategic intent of such policy may be ambiguous and uncertain, and central implementers may have little idea about how to carry out this intent. The degree of ambiguity and conflict inherent in any initial statement of public policy may be a significant factor in determining how to organize and manage its implementation successfully.

[216] Matland, "Synthesizing the Implementation Literature, 148-150.

3. Ambiguity and Conflict in Policy Implementation

According to Matland's research on policy implementation, policy conflict will exist when the actors involved are interdependent with one another, one or more sees the policy as directly relevant to its interests, and/or when there are differing views over the policy's objectives or the manner in which the policy is to be carried out. The intensity of conflict increases with an increase in incompatibility of concerns, and with an increase in the perceived stakes for each actor; the higher the stakes, the more aggressive the behavior. It is possible to make some policies more acceptable by limiting or otherwise adjusting the scope or rate of change, or by creating incentives for the parties involved. However, Matland goes on to state that some policies are, by their nature, controversial and it is not possible to adjust them to entirely avoid conflict. He suggests that, depending on the level of conflict, approaches to resolution may vary. If the level of conflict is low, simple analytical or problem solving methods may suffice. If the level of conflict is high, bargaining and coercion are common strategies. [217]

Matland contends that ambiguity in policy implementation falls into two broad categories: ambiguity of goals and ambiguity of means. For some researchers, the clarity of a policy goal is seen as an important factor in achieving policy success. Ambiguity, they argue, leads to misunderstanding, uncertainty, and ultimately failure to implement the policy and achieve its objectives. However, ambiguity of goals also has a positive side. Matland posits that one way to limit conflict is through ambiguity. He suggests that if a policy goal is too precise, it is more likely to trigger conflict because some actors essential to implementation become more aware of their own self-interests, and may act to inhibit implementation. Matland notes that ambiguity is often a prerequisite for getting a new policy adopted. Likewise, he says that there may be ambiguity of means when the methods or technology needed to implement a policy and achieve its goals do not exist, or it is uncertain what roles various actors are to play. He further states that means are also ambiguous when the degree of complexity present makes it difficult to know which tools to use, how to use them, and what the effects of their use will be.

---

[217] Matland, "Synthesizing the Implementation Literature, 155-157.

Matland describes how policy compromise often depends on the ambiguity that permits various actors to assume their own understanding of goals and means; what he describes as "a natural and inevitable result of the working of political process." It is important to note here that beyond their broad strategic intent, legislators and senior policymakers are often too far removed from the action to know precisely what goals are achievable or in precisely what way. These questions are often left to implementing agencies and other stakeholders. Matland cites John Tukey who in 1962 noted, "Far better an approximate answer to the right question, which is often very vague, than an exact answer to the wrong question, which can always be made precise." [218] In referencing other research, he describes policy implementation as a process of discovery, learning, and experimentation. Policy implementation, he suggests, not only provides an opportunity to learn new methods, it also provides an opportunity to reach new goals, testing the vision, principles, and state of technological knowledge along the way.

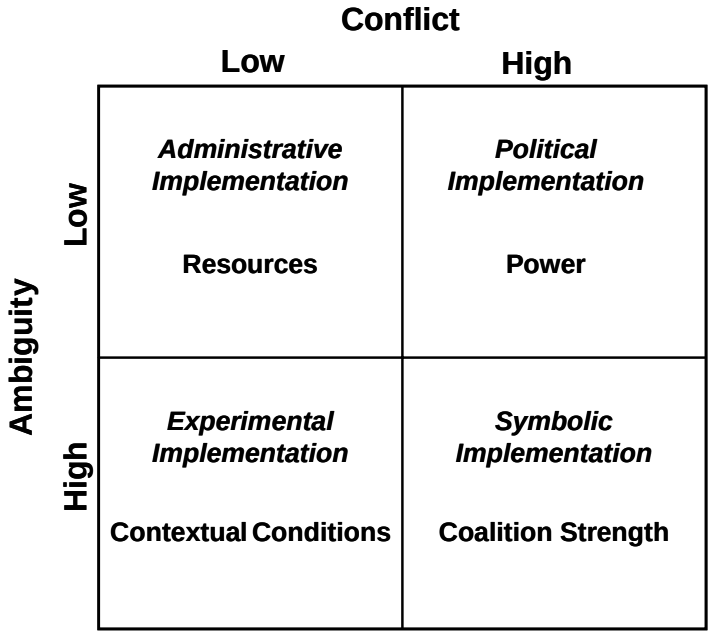

Figure 11. Ambiguity-Conflict Matrix: Policy Implementation Process. [219]

[218] Matland, "Synthesizing the Implementation Literature, 157-159.

[219] Ibid., 160, Exhibit 1.

As depicted in Figure 11, Matland offers a model that attempts to characterize policy in the context of the degree of ambiguity and conflict such policy may present. In doing so he offers a window through which implementers may develop strategies to ensure greatest chance of success. Each pane in that window suggests the principle influences and possible pitfalls involved, and what approach may be more appropriate.

Low Ambiguity and Low Conflict – Administrative Implementation: Under these conditions Matland's research suggests the conditions are appropriate for a rational decision-making process. Explicit policy goals are given and the means for achieving them are known and agreed to. In such a setting, outcomes are determined largely by the simple availability of resources. Roles, responsibilities and methods are clearly spelled out. Implementation occurs in a top-down manner and the central authority has the information, resources, and power necessary to achieve success. Given the stable nature of the system, outcomes are predictable and uniform across agencies and at the lowest levels of implementation. Matland opines that under these conditions, compliance is largely a function of carrying out orders already perceived as legitimate by those charged with implementation. In those cases where compliance is an issue, the central authority has the power to either threaten sanctions or provide other incentives. [220]

Low Ambiguity and High Conflict – Political Implementation: This setting is described by Matland and the research he cites as typical of political decision making. Though goals are clearly defined, there is disagreement and dissension among those involved; conflict that naturally extends to the means of implementation as well. This conflict emerges early and can be vigorous as implementation develops. In low ambiguity and high conflict situations, outcomes are decided by power – who has it and how it is used. Here Matland suggests that a single actor or coalition may have the power needed to force implementation from either direction, or at least to wield sufficient influence to drive bargaining and compromise on goals and/or means. Actors essential to implementation may not fully comply and may even refuse to participate. Often compliance is reached through negotiated agreement forced from the top. [221]

---

[220] Matland, "Synthesizing the Implementation Literature, 160-163.

[221] Ibid., 163-165.

High Ambiguity and Low Conflict – Experimental Implementation: According to Matland, when these factors are present, outcomes will depend largely on the parties most involved and what resources they bring to the table. Since that involvement is fluid and may vary widely, a range of outcomes can be expected. He describes a process having "streams of actors, problems, solutions, and choice opportunities combining to produce outcomes that are hard to predict." [222] This can result in different organizations implementing different versions of the policy. Matland goes on to say that these mutations can be viewed as "experiments" and learning opportunities that can help shape policy goals and means, so bottom-up implementation is favored under these conditions. However, he warns that ambiguity can also breed gaps in accountability and spawn small fiefdoms with individual actors pursuing their own interests, which may have little, if any, connection to the broader public good. Learning is likely random and, thus, monitoring, evaluation, and feedback are vital.

High Ambiguity and High Conflict – Symbolic Implementation: Though Matland cites research suggesting ambiguity can lessen conflict, at least initially, he also outlines other cases where highly significant symbols (important public policy matters) can produce a high degree of conflict even when the policy is vague. He describes coalitional strength at the local level as a key determinant of success. Differing perspectives and competition over the "vision" will develop, and variations in coalition strength and dominance will result in variations in implementation. He states that professions are likely to play an important role in this vacuum because stakeholders with professional training will advance solutions rooted in their own disciplines. Competition among professional camps, Matland suggests, form the core of competing coalitions, with the battles likely being long and bitter. Disagreements, he says, are resolved through coercion or bargaining. Though central authority does exercise influence by offering resources and incentives, and by focusing attention on the issue, the process is likely to be highly political and dominated by local actors. A necessary dynamic tension and balance between both top-down and bottom-up approaches is thus indicated here. [223]

---

[222] Matland, "Synthesizing the Implementation Literature, 165-168.

[223] Ibid., 168-170.

4. Public Policy Implementation Challenges

At the risk of oversimplifying the matter, challenges associated with public policy implementation can be roughly divided into two distinct categories – definition of success and the definition of the means to achieve that success. With regard to the definition of success, Matland again differentiates between the views of top-down and bottom-up theorists. He sees the pivotal question as being whether implementation of the policy designers' plan itself is the goal, or rather what matters more is the ultimate outcome of the policy once implemented (i.e., whether it achieved its intended effects). This is not a trivial distinction because it is not uncommon for central policy implementers to take a top-down view of implementation as complying with the letter of the policy's intent as originally expressed by a statute, an elected official, or an agency's chief executive.

Conversely, a bottom-up view, and one most accepted by local actors, is that success is ultimately a function of a policy's "positive effects." This should not be surprising since those closest to the action, those who must expend time, resources and political capital to implement the policy at the grass roots level, are most impacted by the perception of its success or failure among their own constituencies. Thus they have a greater stake in actual results. Assuming there is no doubt that the definition of success should be the ultimate performance of the policy, and that the participation and commitment of local actors in shaping the policy and its implementation are essential to that aim, then the question becomes one of how that participation and commitment is achieved. [224] According to Harold Seidman,

> Straight lines of authority from the President down through department heads with no entity exercising power independent of its superior are not adapted to current circumstance. Straight lines of authority and accountability cannot be established in what has become in major degree a non-hierarchical system. Federal agencies now rely for service delivery

[224] Matland, "Synthesizing the Implementation Literature, 145-174.

> on third parties who are not legally responsible to the President and subject to his direction. Federal powers are limited to those agreed upon and specified in grants and contracts. [225]

Lester Salamon sees government administration as transitioning from a traditional hierarchical structure to the management of organizational networks. He describes this network view as "third-party government" based on the intimate inter-relationships and interdependencies that exist among federal, state and local governments and the private sector. Nowhere is this network of relationships more apparent than in the arena of homeland security policy. Salamon cautions that "third party government" poses major challenges that are not fully appreciated by public administration researchers or public sector managers. [226]

As Thomas Stanton puts it, the problem is more than just power and control. He suggests that state and local governments and the private sector may possess a more sophisticated understanding of many of the critical facts that the federal government must know to do its job well, particularly in the area of homeland security. He further suggests that the hierarchical model of federal administration, with its imposition of policy from above, "often on the basis of limited consultation with the affected parties," is unlikely to be effective in dealing with the complex problems associated with this domain.[227] The challenge instead calls for an understanding of systems thinking, complexity, and the effective management of intra- and inter-organizational networks.

---

[225] Harold Seidman, Foreword to Thomas H. Stanton, Benjamin Ginsberg, eds., *Making Government Manageable: Executive Organization and Management in the Twenty-First Century* (Baltimore MD: Johns Hopkins University Press, 2004).

[226] Lester Salamon, "The New Governance and the Tools of Public Action: An Introduction," in Lester Salamon, ed., *Tools of Government: A Guide to the New Governance*, 11-14.

[227] Thomas Stanton, *Improving Federal Relations with States, Localities, and Private Organizations on Matters of Homeland Security: The Stakeholder Council Model*, 1-2.

C. OPEN SYSTEMS, COMPLEXITY, AND NETWORKS

1. Organizations as Open Systems and Complexity

The rubric of systems theory has evolved over the years as a way to better understand all manner of scientific, engineering, biological, and social constructs. In its simplest form, a system is an organized set of parts or subsystems that are related to accomplish a common purpose. It has various inputs, processes and outputs. The parts or subsystems are interdependent so if one part of the system is changed, the nature of the overall system will often change as well. [228] With regard to its application in the sociology of organizations, the systems approach emphasizes the dynamic inter-relationships between the system's individual parts and as well as the system as a whole within its external environment. As that interchange occurs, the system adapts and new properties emerge. Thus systems theory provides "a view of organizations that focuses on the arrangement of roles and responsibilities, internal operations, and boundary-spanning activities that enable the organization to persist and evolve over time." [229]

Stephen Littlejohn defines an open system as…"a set of objects with attributes that interrelate in an environment. The system possesses qualities of wholeness, interdependence, hierarchy, self-regulation, environmental interchange, equilibrium, adaptability, and equifinality." [230] Equifinality is the theory that organizations, using the same inputs, can arrive at the same end or goal through different means. Open systems theory not only reinforces the fact that organizations operate in and interact with the external environment, but that they are also embedded in another, larger system. That system consists of other organizations and external processes that exert various political, social, technological, and/or economic forces on the organization, which in turn influences performance, change, and organizational survival. A system that changes its

---

[228] Carter McNamara, "Basic Definition of Organization - Organizations as Systems," adapted from *Field Guide to Consulting and Organizational Development* (Minneapolis: Authenticity Consulting, LLC, 2007).

[229] Patricia Andrews and Richard Herschel, *Organizational Communication - Empowerment in a Technological Society* (Boston: Houghton Mifflin Company, 1996), A-20.

[230] Stephen Littlejohn, *Theories of Human Communication,* 2nd ed. (Belmont, CA: Wadsworth Publishing Company, 1983), 32.

behavior in response to its environment is often known as an adaptive system. Open systems theory is well suited to understanding complex public sector organizations and the bureaucratic structures responsible for the implementation of public policy, in that the sole purpose of government is to be responsive to the public and the greater public good.

Garnett Williams defines a complex system as one where numerous independent elements constantly interact and spontaneously organize and reorganize into more and more elaborate structures over time. This complexity consists of a) a large number of similar but independent elements or agents; b) persistent movement and responses by these elements to other agents; c) adaptiveness so that the system adjusts to new situations to ensure survival; d) self-organization, in which order in the system forms spontaneously; e) local rules that apply to each agent; and f) progression in complexity over time so that the system becomes larger and more sophisticated. Accordingly, the behavior of such complex systems cannot be predicted and may evolve to a point somewhere between order and chaos. [231]

2. Complex Adaptive Systems and Emergence

The concept of complex adaptive systems, like complexity and chaos theory before it, attempts to expand further the research on complex phenomena, especially in the social and organizational sciences. John Holland, a leading researcher on complexity theory considers the following to be among the features of complex adaptive systems: [232]

> Many agents acting in parallel in an environment produced by its interactions with other agents in the system; because agents are constantly acting and reacting to each other, nothing in its environment is fixed;
>
> Control is highly dispersed and any coherent behavior there might be arises from competition and cooperation among the agents themselves; there are many levels of organization, with agents at one level serve as building blocks for the next;
>
> All have niches they can exploit, filling up one niche often opens up new ones that can be exploited; thus they never reach equilibrium, and though they can improve on some dimensions, they never optimize;

---

[231] Garnett Williams, *Chaos Theory Tamed* (Washington, DC: Joseph Henry Press, 1997), 234.

[232] John Holland, *Hidden Order* (Reading, MA: Addison-Wesley, 1995), 1-40.

> There is constant rearrangement as a result of learning, experience, evolution, and adaptation; the richness of the interactions within the system allows the system as a whole to undergo spontaneous adaptation and self-organization.

Self-organization is a process "whereby new emergent structures, patterns and properties arise without being externally imposed on the system. Not controlled by a centralized, hierarchical command-and-control center, self-organization is usually distributed throughout a system." [233] To paraphrase consultant Beverly Parsons, self-organizing systems are in a continuous state of disequilibrium, and exhibit behaviors that are unexpected. She describes this state as characterized by contradiction and contentions, simultaneous cooperation and competition, and the coexistence of interdependence and independence. Though there is no real overall control, patterns emerge as members make adjustments to each other and respond to changing conditions in their environment. She posits that there may be agreement on the system's general direction, but movement in that direction is largely self-motivated and relies on the independent and interdependent actions of the people or groups involved. According to Parsons, actions and patterns naturally emerge over time as people make adjustments to their own and each other's behavior, and the environment around them. [234]

It is important for leaders to recognize and understand the nature of complex adaptive systems and especially the forces at work that build momentum in the direction of desired outcomes; outcomes that can neither be fully planned or controlled. As Parsons suggests, leaders must align attention and resources to help accelerate the movement in a natural direction even though it is unplanned or uncontrollable. She also outlines two factors that researchers have identified as relevant to understanding the influence of complexity on organizations. Similar to the previous discussion of conflict and ambiguity in public policy implementation, these factors are the degree of agreement and degree of certainty present in the system. Agreement refers to the shared sense of congruence about the principles, purpose, and activities of the system. Certainty refers to the predictably of conditions, cause-and-effect relationships, and the consequences of the

---

[233] Brenda Zimmerman, Curt Lindberg, Paul Plsek, *Edgeware: Insights from Complexity Sciences for Health Care Leaders* (Irving TX: VHA, Inc. 2001), 270.

[234] Beverly Parsons, "Attending to Self-Organizing Systems in Cluster/Initiative Evaluation" (paper presented at the In-BC Interprofessional Network Conference, Vancouver, Canada, March 18, 2007).

system's behavior. Parsons indicates that complexity researchers see these factors as determining the orderliness of the system and the implications for decision-making.

Drawing on the work of others, Parsons offers a graphic (Figure 12 below) which attempts to depict the general relationships between levels of agreement and certainty in a system and the nature of organizational behavior that results from variations in those dimensions. When levels of certainty and agreement are high, the situation is generally stable, organized, and predictable.

When levels of certainty and agreement are low, the situation is random and unorganized; a state of chaos. As Parsons describes it, a system may be far from being stable and organized but not yet totally unorganized or entering a state of chaos. In between exists a region of complexity and complex adaptive systems. In this region, dissent, learning, experimentation, evolution, and adaptation will emerge, with or without leader influence. It is a region fertile for change.

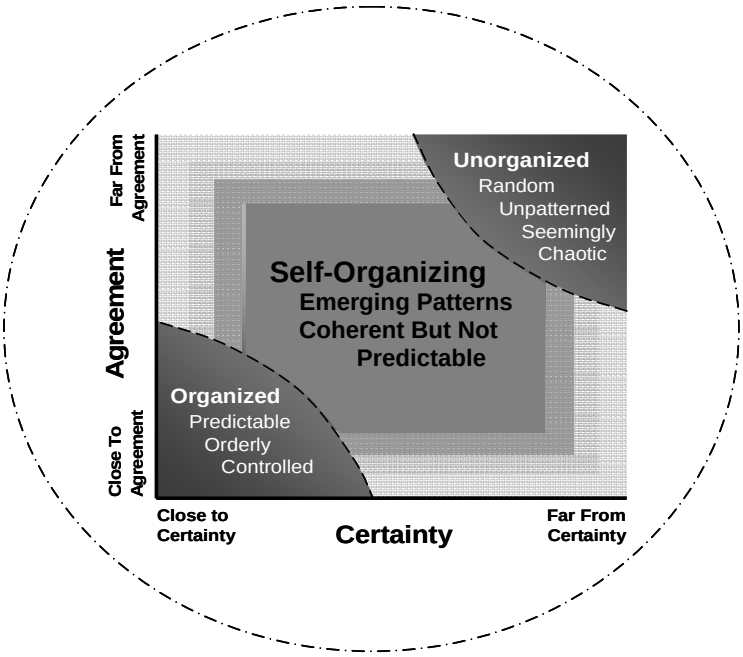

Figure 12. Three Subsystems of a Social System and its Context. [235]

[235] Beverly Parsons, "Attending to Self-Organizing Systems in Cluster/Initiative Evaluation" 2.

Organizational systems rarely fall neatly within any one particular category, as different elements may operate at different levels of complexity at different times. As Parsons puts it, these three variations in dynamics — organized, self-organizing, and unorganized — can be thought of as "extensively over-lapping and entangled." Nonetheless, as a general framework, it helps provide some understanding of system behavior under complex conditions, and may assist leaders and stakeholders to better assess and guide efforts to achieve organizational change. The challenge for leaders will be to lead in non-traditional ways that foster, stimulate, and facilitate the kind of dissent, learning, experimentation, evolution, and adaptation that naturally emerge in such systems. Capitalizing on this emergence will require leaders to also be open to learning and adaptation themselves, understanding the need to be guided by the collective energy and intelligence inherent in the larger system.

3. Wicked Problems and Complexity

Complex systems almost by definition exist to deal with complex and seemingly intractable problems. In response, Horst Rittel and Melvin Webber originated the classification and study of "wicked problems." According to Tom Richey, wicked problems are typically "ill-defined, ambiguous and associated with strong moral, political, and/or professional issues." Strongly stakeholder-dependent, he suggests there is often little consensus as to the nature of the problem or how it should be resolved. [236] Rooted in complexity, Richey sees wicked problems as sets of "complex, interacting issues evolving in a dynamic social context" constantly in motion, with new wicked problems emerging as a result of the system trying to understand and solve existing ones. Rittel and Webber define wicked problems as meeting most or all of the following ten criteria: [237]

---

[236] Tom Ritchey, "Wicked Problems - Structuring Social Messes with Morphological Analysis" (2005), http://www.swemorph.com/pdf/wp.pdf [Accessed July 27, 2007].

[237] Horst Rittel and Melvin Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4, no. 2 (June 1973):155-169.

There is no definitive formulation of a wicked problem. Formulating the problem and the solution are essentially the same thing. Each attempt at creating a solution changes the understanding of the problem.

Wicked problems have no stopping rule. Since you cannot define the problem, it is difficult to tell when it is resolved. The problem solving process ends when resources are depleted, stakeholders lose interest or political realities change.

Solutions to wicked problems are not true-or-false but good-or-bad. Since there are no unambiguous criteria for deciding if the problem is resolved, getting all stakeholders to agree that a resolution is 'good enough' can be a challenge.

There is no immediate and no ultimate test of a solution to a wicked problem. Solutions to wicked problems generate waves of consequences, and it is impossible to know how all of the consequences will eventually play out.

Every implemented solution to a wicked problem has consequences. Once the web site is published or the new customer service package goes live, you can't take back what was on-line or revert to the former customer database.

Wicked problems do not have a well-described set of potential solutions. Various stakeholders will have differing views of acceptable solutions. It is a matter of judgment as to when enough solutions have emerged and which should be pursued.

Every wicked problem is essentially unique. There are no 'classes' of solutions that can be applied to a specific case. "Part of the art of dealing with wicked problems is the art of not knowing too early what type of solution to apply."

Every wicked problem can be considered a symptom of another problem. A wicked problem is a set of interlocking issues and constraints, which change over time, embedded in a dynamic social context.

The causes of a wicked problem can be explained in numerous ways. There are many stakeholders who will have various and changing ideas about what might be a problem, what might be causing it, and how to resolve it.

The planner (designer) has no right to be wrong. A scientist is expected to formulate hypothesis, which may or may not be supportable by evidence. A designer doesn't have such a luxury, they are expected to get things right.

Jeff Conklin views complexity as contributing to fragmentation, "a condition in which the people involved see themselves as more separate than united, and in which information and knowledge are chaotic and scattered." [238] With problems becoming ever more complex, the number and diversity of players increases, further adding to that complexity. According to Conklin, diversity of players makes harnessing collective intelligence a challenge and consensus virtually impossible. As the network of players grows flatter and crosses social, organizational and technical boundaries, there is an expanding range of stakeholders representing different dogmas, disciplines, agencies, organizations, and special interests, each with their own ideas on what the issues are and what needs to be achieved. Conklin points out that in "many political situations, each stakeholder's position about what the problem is reflects the mission and objectives of the organization (or region) they represent." [239]

Conklin muses that wicked problems have become so commonplace that the sense of chaos and futility that often accompanies them is sometimes accepted as inevitable. He cautions that in failing to recognize "wicked problems" for what they are, leaders persist in applying traditional linear thinking and problem solving methods that are inappropriate for the complex and nonlinear challenges they face. Such complexity, he suggests, requires new understandings, processes, and tools that are better suited to the "fundamentally social and conversational nature of work." Though the natural evolution of problem solving in this realm may appear chaotic on the surface, Conklin opines that it reflects a deeper natural order. In pursuing answers to complexity, problem solving and learning are closely interdependent and, according to Conklin, the flow of this learning process is collaborative and opportunity-driven. The harder and more unstructured the problem, the more learning involved and the greater the need for collaboration. Just like linear thinking, traditional top-down command-and-control style leadership is absolute folly when dealing with wicked problems. [240]

---

[238] Jeff Conklin, "Wicked Problems and Social Complexity" (2006), 2, http://cognexus.org/wpf/wickedproblems.pdf [Accessed July 28, 2007].

[239] Conklin, "Wicked Problems and Social Complexity," 14.

[240] Ibid., 3-9.

Conklin recommends that the key to dealing with wicked problems, and the fragmentation associated with them, is to achieve coherence. Coherence means that stakeholders have "shared meaning for key terms and concepts, that they are clear about their role in the effort, that together they have a shared understanding of the background for the project and what the issues are, and that they have a shared commitment to how the project will reach its objectives and achieve success." With increased coherence, more collective intelligence becomes available to deal with change and complexity. He suggests that leaders must understand collective intelligence as a natural property of complex social systems. [241] That intelligence — the experience, knowledge, expertise, and perspectives of stakeholders — if tapped, can be an enabler to collaboration that unleashes the creativity and resourcefulness needed to address the problem and advance change.

4. Networking and Collaboration

Laurence O'Toole has written of the growing need for and the emergence of networks and collaboration in public administration. His review of the literature confirms that this trend is not a passing fad and that government leaders must increasingly deal with the sort of wicked problems defined by Rittel and Webber. He reinforces the point that wicked problems, particularly in the area of complex and often ambitious public policy, cannot be addressed simply by dividing up the pieces and delegating authority. According to O'Toole, given limits on the expertise and reach of government, public sector managers charged with developing and implementing public policy must often balance the need for central program authority with the practical and political demands for inclusion and broader influence. This in turn suggests the use of networked structures in response. However, though real-world examples of this sort of networking exist, O'Toole points out that there is no comprehensive theory to guide how public sector managers organize and lead networks. He further suggests that, in the

[241] Conklin, "Wicked Problems and Social Complexity," 18.

absence of such theory, current efforts may either be relying on inappropriate organizational models or adapting conventional structures ill-suited to meet these challenging demands. [242]

O'Toole echoes the previous discussion on complex adaptive systems when he posits that complexity and diffuse structure of authority makes behavior and performance somewhat unpredictable and the shared nature of network leadership extremely challenging. Networks involve interdependent and often loosely organized relationships among multiple organizations, or parts of organizations, where there is little or no formal hierarchy, and where one element is not merely the subordinate of another in a way that compels compliance. Multiple needs and interests of different actors must be addressed in a way that motivates and moves the network toward its intended goals. He further states that "managers in networked systems do not supervise most of those on whom their own performance relies, monitoring channels are typically diffuse and unreliable, and common organizational culture exercises a limited and indirect influence." [243] O'Toole cautions that public sector leaders cannot be expected to exercise direct control as a function of their official position. He suggests that, to avoid being ineffectual, these leaders will need to adjust their conventional notion of management and be open to new networked organizations. Given previous discussions in this chapter, the answer to what those organizations should look like and how they should function may lie within the larger stakeholder group itself, making not only the structure of the network important but also the nature of the interaction among stakeholders as well as the quality of collaboration.

It is commonly understood that collaboration is based on the simple notion of the whole being greater than the sum of the parts, and that organizations and people can accomplish more collectively than they can independently. Though, as O'Toole has stated, there is no unifying theory about networking in the public sector, Nancy Roberts cites a growing body of research from her own examination of issues associated with the

---

[242] Laurence O'Toole, Jr., "Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration," *Public Administration Review* 57, no. 1 (January– February 1997): 45-52.

[243] Ibid., 46-48.

intractable problem of wartime recovery in Afghanistan. As she notes, the core of collaboration is achieving win-win solutions to shared problems – "rather than play a 'zero-sum game' that seeks to distribute pie shares based on winners and losers, they assume a variable sum game that seeks to enlarge the pie for all parties involved." [244] Achieving collaboration to address wicked problems is of course no easy task.

From her own first-hand experience, Roberts suggests that people may need to first "fail" into collaboration before being willing to abandon more authoritative and competitive strategies. This, she advises, is especially important for leaders and cultures that place a high premium on taking charge, making decisions, being competitive, and using authorities and experts to settle whatever disputes arise. Roberts suggests three basic steps to facilitate collaboration. First, avoid authoritative strategies where the situation is complex, conflict-ridden, and power is diffuse. Second, get all the parties that make up the system into the same room to develop shared meaning about the problem and what has been referred to by Conklin as coherence. Deciding on what the system is and which stakeholders are involved will be challenging, continuous, and evolve over time, and not all stakeholders may always agree. However, it is a key formative step. Third, be open to self-organization and co-evolution. Leadership of complex adaptive systems operating at the edge of chaos requires courage and a willingness to trust the process, accepting emergent "experimentation, groping along and muddling through." [245]

In a comprehensive study of the leadership role in collaboration spanning ten years, Chris Huxham and Siv Vangen outline three "media" through which collaborative leadership is exercised:

> Structure relates to organizations and individuals involved and the connections between them. It is a key driver in shaping agendas in that it determines who participates, who has power, and what resources are used. Alternative structures may emerge as members influence the agenda and they adapt to the complexity of the task.

---

[244] Nancy Roberts, "Wicked Problems and Network Approaches to Resolution," *The International Public Management Review* 1, no. 1 (2000): 1-19.

[245] Ibid., 12-19.

> Processes they define as the formal and informal methods by which communications take place. The type and frequency of communications influences the sharing of information and can either help or hinder common understanding of issues, empower members' participation or strip power from them.
>
> Participants themselves exercise leadership in that those with power and know-how often take lead roles. Though the leverage of official leadership is diminished, members may acknowledge leaders either by position, location in the organization having the lead, role as dominant convener, or through boards or committees. [246]

Huxham and Vangen see three activities central to such leadership: 1) managing power and controlling the agenda by using position power to influence the action in an appropriate direction; 2) representing and mobilizing member organizations' roles and ensuring that the needs of those organizations are represented; and 3) enthusing and empowering those who can deliver collaboration aims by getting buy-in to the role and purpose. They have discovered that those leading are frequently confronted with challenges that inhibit success. In almost all cases, these leaders had little real control over the media of collaboration. In addition, the complexity of the task, the structure of collaboration, or the logistics involved proved key distractions. Failure to get buy-in as well as not establishing trust were also factors, along with shifts in policy and changes in leadership.

Huxham and Vangen conclude that successful collaboration requires significant energy, commitment, skill, and continual nurturing on the part of the leaders involved. These researchers conclude that wherever leaders achieved success, it was due to the significant personal attention they paid to championing the cause and managing the media of collaborative leadership.[247] They cite other studies that reinforce the point that active involvement (or the absence of it) by top public sector executives has a determining influence on the success or failure of any collaboration.

---

[246] Chris Huxham and Siv Vangen, "Leadership in the Shaping and Implementation of Collaboration Agendas: How Things Happen in a (Not Quite) Joined-Up World," *Academy of Management Journal* 43, no. 6 (December 2000): 1159-1175.

[247] Ibid., 1168-1171.

THIS PAGE INTENTIONALLY LEFT BLANK

V. REVIEW OF RISK MANAGEMENT POLICY IMPLEMENTATION

A. NEED FOR A HYBRID MODEL OF CHANGE MANAGEMENT

1. Integrating Strategic Change, Policy, and Systems Theories

When considering the nature of homeland security and its tremendous interdependence with all aspects of American society, it becomes evident that homeland security leaders will need new tools for understanding the challenges involved and effectively influencing strategic change. This means looking across prior research and experience, adapting old models, developing new ones, and incorporating this learning into the way future homeland security policies and programs are conceived, developed, implemented, and maintained. The central purpose of this paper is to consider the public policy reflected in the National Infrastructure Protection Plan (NIPP) risk management framework as representative of homeland security strategic change and to apply current change management models, public policy constructs, and emerging open systems and complexity theory in a way that better informs its implementation and provides initial grist for additional research in this area. In so doing, it is the intent of this paper to encourage homeland security leaders to consider the importance of managing the change process itself and applying relevant change management theory and lessons learned to advance the practice within this field.

If leadership, in its simplest form, is getting people to do things that achieve a certain outcome, it is then by definition about transformation and making change. In leading major strategic change, it is not uncommon for leaders, in any sector of society, to focus more on the financial, technological, and institutional aspects of the intended change than on leading the change process itself. As Kotter points out in his review of over 100 large-scale change efforts, only a few such changes actually achieve their intended aims, while others are complete failures, with most falling somewhere in

between. [248] Nowhere in our public life as a nation is it more important to get change right than in the implementation of homeland security policy and programs. If a major U.S. corporation fails at strategic change and falls victim to the marketplace, there may be momentary consequences, but the economy rights itself and augers on. If there is failure in the implementation of change in homeland security, vulnerabilities go unaddressed, precious resources are squandered or misapplied, and the likelihood of a major catastrophe, for which the nation is unprepared, only increases as the nature of the threat changes and adapts faster than our ability to respond. The human, economic, and political consequences of such a failure could be enormous.

Chapter IV of this paper provides a brief overview of some of the current literature and perspectives on managing the implementation of large-scale change. It summarizes the challenges involved and offers frameworks and approaches for leaders to consider when dealing with the complexity such change presents, often in the form of what are now referred to as wicked problems, the latter being typical of the sort of challenges the nation now confronts in the still-emerging field of homeland security. Given the emergent nature of homeland security, there is precious little in the research literature dealing specifically with homeland security leadership and change management. There is however, a rich history of research on leadership in general to include managing strategic change, although this research has typically been conducted within corporate settings and not the public sector. Most research addressing change management in government has had to do with the implementation of public policy, focusing on its greater political and social dimensions. Transcending all of this is a rapidly growing body of knowledge about organizations as open systems, complexity theory, adaptation and emergence, and social networking and collaboration.

Like much in the leadership and change management literature, there are many definitions for the phrase "strategic change." For purposes of this paper, one definition that may fit best is viewing strategic change as "a difference in the form, quality, or state

[248] John Kotter, *Leading Change*, 3-4.

over time in an organization's alignment with its external environment." [249] In this context, many homeland security initiatives certainly qualify as strategic change. This includes airline passenger screening, the Southern Border Initiative (SBI), and of course, critical infrastructure and key resource (CI/KR) protection through the implementation of the NIPP, the NIPP sector partnership model, and the risk management framework. In addition to being strategic change, the NIPP is also significant public policy, and not just federal policy, but policy that is national in scope.

Given that its purpose is to serve the people, government in general can be classified as an open system having tremendous interdependence with its external environment. Nowhere is this truer than in homeland security, and especially in the area of CI/KR protection. As evidenced in the sector partnership model, implementation of the NIPP and the Sector-Specific Plans (SSPs) are highly interdependent with thousands of public and private sector CI/KR owners and operators across the country. The highly networked nature of the nation's critical infrastructure itself is reflected in the complex adaptive system formed under the NIPP – the Critical Infrastructure Partnership Advisory Council (CIPAC). This nationwide network of over five hundred member entities spread across thirty-six different councils and seventeen different CI/KR sectors requires public/private sector collaboration on a scale possibly not seen since World War II. And certainly, all of this qualifies the implementation of the NIPP, and especially the implementation of the national risk management framework so central to its success, as a wicked problem.

Implementation of the risk management framework outlined in the NIPP can be viewed through the multiple lenses of conventional change management theory, as national public policy, and as a highly complex wicked problem. In considering main-stream change management theory, a combination and adaptation of Kotter's Eight-Stage Process and the Determinants of Successful Organizational Change offered by Fernandez and Rainey will be applied. In addition, Tichy's Technical Political Cultural (TPC) Framework will be overlaid onto what is known of NIPP risk management framework

---

[249] Nandini Rajagopalan and Gretchen Spreitzer, "Toward a Theory of Strategic Change: A Multi-lens Perspective and Integrative Framework**,"** *The Academy of Management Review* 22, no. 1 (January 1997), 48-79.

implementation to date. In considering the risk management framework as public policy, change management issues will be explored using Matland's Ambiguity – Conflict Matrix. And finally, implementation of the NIPP risk management framework will be viewed through the lens of open systems theory, complexity, and wicked problems for additional insights on change management and leadership.

2. Conventional Models Applied to Homeland Security Change

In their review of the change management research, Sergio Fernandez and Hal Rainey identify points of consensus in the literature and offer a set of eight propositions that they describe as key determinants of successful organizational change in the public sector. [250] These propositions are very similar to the Eight-Stage Process of Creating Major Change presented by John Kotter, the most notable difference being that Kotter's Eight-Stage Process was based on his own personal experience and research, while Fernandez and Rainey were later able to tie their change propositions directly to the research literature and the commonalities they identified across major theoretical perspectives. [251] Though risking over-simplification of a complex and dynamic process, the easy-to-understand checklist format all three of these authors present make it an attractive lens through which to assess strategic change in homeland security.

While Kotter expresses his Eight-Step Process in terms that reflect more the art of change leadership, like empowering broad-based action, Fernandez and Rainey take a more conventional management approach with the expression of straightforward tasks. Nonetheless, there is much in common between the two lists, and both provide valuable insight into the elements of effective change. Some elements of both translate almost directly: developing a vision and strategy (Kotter) and providing a plan (Fernandez and Rainey), while others are unique to each list. For example, Kotter emphasizes the need for generating short-term wins, while Fernandez and Rainey state the need to provide resources. Though the article by Fernandez and Rainey is perhaps more grounded in the

[250] Sergio Fernandez and Hal Rainey, "Managing Successful Organizational Change in the Public Sector: An Agenda for Research and Practice," 7.

[251] John Kotter, "Leading Change: Why Transformation Efforts Fail," 61.

research of others, Kotter presents an important intangible quality based on his own extensive firsthand experience — that it is the role of the leader to energize, inspire, and influence the change process. The following questions are based extensively on the work of Kotter and Fernandez and Rainey. It is a blending of the two approaches, adapted in a way that might provide a simple generic guide tailored for use by homeland security leaders.

Assessing Leadership of Strategic Change

What is being done to ensure the need and establish a sense of urgency?

Conduct a careful examination of the scope of the problem and the attendant issues and implications. Identify internal and external stakeholders and their possible positions relative to the issues. Formulate a cogent argument supporting the need for change and the consequences of failing to act. Articulate a compelling vision and set of policy goals for what the change will achieve. Persuasively communicate these in a way that wins the support of the influential leaders that will form a guiding coalition.

Has a guiding coalition been established and policy-maker commitment obtained?

Identify clear responsibility for being the advocate and "idea champion" for the change. Organize the group to work as a team and ensure it has the power, authority, stature, skills, and resources needed to effectively lead the change process. Manage the group outside the normal hierarchy and provide it with the senior leadership support and protection necessary to deal with resistance. Bring appointees, political leaders, and other policy-makers on-board early and obtain their understanding and commitment.

Has a refined vision been developed, and a change strategy and plan prepared?

As the guiding coalition takes hold, it should refine the vision and develop an initial plan for achieving it, building shared ownership along the way. The plan must translate the vision and policy goals into specific objectives, strategies, milestones, accountabilities, and measures for success. It must also demonstrate a sound causal link between the actions outlined and the outcomes desired to ensure consistency in approach, as well as provide a means for managing coordination and congruence among all parties involved.

How is the vision being communicated and broad-based action mobilized?

Constantly communicate the vision, policy goals, and strategy across all stakeholder groups, through every vehicle possible. Senior leaders and the guiding coalition must walk-the-talk and role-model behaviors expected of those whose buy-in and participation are essential to success. Encourage risk-taking and paradigm-breaking initiatives and ideas consistent with the vision, across as wide a front as possible. Remove, neutralize, or by-pass obstacles (i.e., policies, people, systems) that undermine the change effort.

Are needed resources and support being marshaled to overcome resistance?

As momentum builds, ensure adequate financial, technological, and human resources to support and sustain the change. Capitalize on synergies across stakeholder groups, and avoid overtaxing participants. Commit sufficient leadership time and effort to expanding internal and external support. Reduce resistance to change by encouraging widespread participation and an environment conducive to the free and open exchange of ideas. Develop support from political leaders, non-aligned stakeholders, and interest groups.

Are steps being taken to breed success by generating short-term wins?

Consistent with the vision and policy goals, deliberately plan for and achieve interim successes to drive and sustain the change effort. These short-term wins should not only be visible demonstrations of the efficacy of the change, but also provide clear examples of desired behaviors and outcomes. Short-term wins should be widely publicized, the lessons-learned shared, and those involved recognized. As waypoints on the path to change, such wins provide opportunities for experimentation and organizational learning.

How are gains being consolidated to expand and sustain the change?

Begin to institutionalize the vision by using the credibility established through short-term wins. Systematically start to change the behaviors, systems, structures, and policies that don't fit together and/or don't fit the vision. Constantly reinvigorate the process with new projects, themes, and people. Hire, promote, develop and/or enlist the support of people who are capable of and committed to implementing the change. Institutionalize change before shifts in leadership cause commitment and support to diminish.

What efforts are underway to anchor the new approaches in the system?

Show stakeholders the connections between the new way of doing things and the success achieved in attaining the vision and associated policy

> goals. Establish an enduring structure to sustain and adequately support what has been achieved for the long-term, and make the comprehensive system-wide adjustments necessary to ensure subsystem congruence (i.e., alignment of mission, people, processes, etc.). Provide for leadership succession to maintain stability and continuous evolution consistent with the vision.

Tichy's TPC Framework provides another unique lens through which to assess implementation of the NIPP risk management framework as strategic change in public policy. Of the various models of organizations as systems, the TPC Framework, also known as the Network Model, seems to lend itself best to an examination of the fluid organizational networks of the type found in homeland security strategic change.[252] Such change efforts often involve complex social networks that are a combination of formally structured and informally structured relationships across levels of government, private sector business and industry, elected officials, political interests, and other non-governmental stakeholder groups.

While the steps or determinants of successful change offered by Kotter and Fernandez and Rainey provide guidance on the process of change, Tichy's representation of the network model provides a way to look at the basic components of an organization as a network and examine not only the congruence between those components but also their dynamic interrelationships. [253] As Tichy describes the components of the Network Model, the organization or network exists as an open system and is interdependent and constantly interacting with its environment. That environment drives the organization's mission and strategy, which in turn drives the tasks that the organization must perform to carry out that mission. [254] In a homeland security context, the environment includes national-level assessments of threat and vulnerability, guidance from the president and the Congress on program priorities and funding, and the opinions and actions of other elected leaders, senior policy-makers, special interest groups, private sector executives, and the public. As tasks are defined, they determine the processes the organization will employ and the formal structure or, as Tichy refers to it, the prescribed networks, through

---

[252] Noel Tichy, *Managing Strategic Change – Technical, Political, and Cultural Dynamics*), 69-73.

[253] Ibid., 73.

which it is expected those tasks will be accomplished. Government agencies do not have the flexibility of the private sector to rapidly change structure or realign processes, given the nature of legislative mandates from Congress and the limits imposed by congressional oversight and control of funding. This is no less true for the homeland security domain.

People are the central component in Tichy's model, with the key dimensions being leadership and motivation. The quality of that leadership, the level of management skill, and ability to motivate and inspire performance to achieve expected outcomes are critical determinants of success. [255] Homeland security, and especially the advancement of the NIPP and sector partnership model, requires the ability of leadership to motivate the commitment and contributions of a broad range of stakeholders, most of whom are outside the formal homeland security structure. Those relationships may be made more formal through constructs such as the partnership model. However, even with moves to formalize structure, informal relationships will emerge and must be planned for.

As change advances and the normal order of things is altered, new and unplanned relationships, alliances, structures and processes will emerge, both within the prescribed structure and outside of it. These emergent networks occur as people tend to react to, formulate, reformulate, understand, abide by, and/or seek to alter the mission or intended change of the organization. Emergent networks could have significant impact on the nature, direction, and degree of success of strategic change. As Tichy points out, these emergent networks can have double-edged consequences and either work against or in support of the change. [256] Homeland security leaders will need to be aware of these dynamics and alert to the influence they may have on strategic change. A key challenge will be to harness and direct that energy in a way that aligns it with the total effort.

Tichy assesses the health of an organization, and thus its ability to manage strategic change, by looking carefully at the functioning of its technical, political, and cultural (TPC) subsystems. The technical subsystem consists of those tangible aspects that are knowable, such as physical assets, technologies, processes, or resources. The

---

[254] Noel Tichy, *Managing Strategic Change,* 78-87.

[255] Noel Tichy, *Managing Strategic Change,* 86-90.

political subsystem consists of the views and influence of dominant groups, both within and outside the organization or network. The cultural subsystem consists of the shared symbols, beliefs, and values that make up the organizational culture and the culture of other groups active within the political subsystem. The premise behind the model is that a well-designed organization should exhibit alignment between its components and subsystems. [257] Tichy examines this alignment from four perspectives that are outlined here to provide a way to look beyond the process orientation of Kotter and Fernanez and Rainey, and better appreciate TPC dynamics, as these may impact the change process.

Assessing Organizational Alignment for Leading Strategic Change

> How well are the parts of the organization aligned with each other for solving the organization's technical problems?
>
> How well are the parts of the organization aligned with each other for solving the organization's political problems?
>
> How well are the parts of the organization aligned with each other for solving the organization's cultural problems?
>
> How well aligned are the three subsystems of the organization, the technical, political, and cultural?

3. Homeland Security Change and Public Policy Theory

In his assessment of the public policy process, Guy Peters describes American government as "a massive, complex, and often confusing set of institutions" that lack any central organizing principle. [258] The often ad hoc nature of American government has evolved to address particular problems at particular times. According to Peters, this complex and diffuse structure exacerbates the problems inherent in implementation, which is the most vital step in the public policy process. He further states that difficulties involved in public policy implementation are commonly underestimated, and as a result the process becomes one of either "threatening or cajoling organizations into complying with stated objectives or convincing those organizations that their goals can best be

---

[256] Ibid., 93-94.

[257] Salvatore Falletta, "Organizational Diagnostic Models: A Review & Synthesis – White Paper," 17.

accomplished through the programs that have been authorized." [259] In his review of the research, Peters concludes that there is no single answer directing public policy implementation and suggests that "it all depends." [260] He says that the real task for public policy implementers is to identify what factors serve as contingencies that determine the success or failure of implementation (i.e., political, organizational, etc.).

Matland's Ambiguity-Conflict Matrix (page 102) provides yet another lens through which to assess approaches to the implementation of homeland security policy as strategic change, in that it offers a construct to identify the sorts of contingencies suggested by Peters that may determine the success or failure of implementation. As outlined in the prior chapter, Matland describes public policy implementation in the context of the extent of potential ambiguity and conflict. He says that for conflict to exist there must be interdependence of actors, an incompatibility of objectives, and a perceived zero-sum aspect to the interaction. The conflict may arise due to differing views on the objectives of the policy, the means of carrying out that policy, or both. According to Matland, the level of conflict is related directly to the incompatibility over ends and/or means and the perception of individual actors as to what and how much is at stake. Ambiguity, he posits, can likewise be associated with the same two issues – uncertainty over ends and/or means. [261] The Ambiguity-Conflict Matrix offers insights into what implementers may do to increase the opportunity for successful implementation.

Situations involving low ambiguity and low conflict, as viewed by Matland, are administrative in nature with the focus largely on the management of resources. The objectives are well-defined, authority is clear, and implementation is driven from the top. In a homeland security context, an example of policy in this category might be the implementation of the 3-1-1 rule for screening airline passenger carry-on baggage. The Transportation Security Administration (TSA) implemented the 3-1-1 policy "in response to the thwarted liquid explosive bomb plot in the United Kingdom in August of 2006.

---

[258] B. Guy Peters, *American Public Policy* (Washington, DC: CQ Press, 2007), 122.

[259] B. Guy Peters, *American Public Policy*, 122.

[260] Ibid., 121-122.

[261] Richard E. Matland, "Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation," 160-163.

Today, the wide-spread acceptance of that policy demonstrates the international understanding of the threat." [262] In this case, the need was clear and widely accepted, TSA had the authority and a comprehensive plan to implement it, and there was considerable cooperation from local airport authorities and law enforcement agencies.

Matland refers to implementation situations involving high ambiguity and low conflict as experimental in nature. Homeland security examples would typically include activities in the realm of research and development or pilot programs. One example is the need to detect and interdict radiological and nuclear devices to keep them from entering the U.S. and making their way into a major metropolitan center, as is the mission of the joint Department of Homeland Security (DHS)/New York Police Department ((NYPD) Securing the Cities program. [263] There is little disagreement over the general intent, but there is not much known about either the precise strategy to pursue or the technical means to achieve that strategy. In this case, context is what is important, and success depends greatly on ground-level implementation with select local actors having significant influence on the outcome. Each iteration of the policy becomes an experiment that produces learning for the next. However, as what began as an experiment becomes operationalized, ambiguity may go down but conflict over elements like cost, accountability, and jurisdictional prerogatives may increase. [264]

Matland classifies situations involving low ambiguity and high conflict as political in nature. The goals and means may be known but there is disagreement over competing interests or values. In such cases, outcomes are determined by the application of power, and policy is typically driven from the top down. Homeland security examples might include controversial elements of the USA Patriot Act that are perceived to impact civil liberties. [265] Compliance with policy goals is through coercion. Initial support won

---

[262] Transportation Security Administration, "3-1-1 Gains International Acceptance," http://www.tsa.gov/press/happenings/311_intl_acceptance.shtm [Accessed July 11, 2007].

[263] U.S. Department of Homeland Security, "Remarks by Homeland Security Secretary Michael Chertoff and DNDO Director Vayl Oxford at a Press Conference to Announce Spectroscopic Portal (ASP) Program Contracts" (July 14, 2006), http://www.dhs.gov/xnews/releases/press_release_0953.shtm [Accessed July 11, 2007].

[264] Richard E. Matland, "Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation," 165-168.

[265] Larry Neumeister, "Judge Strikes Down Part of Patriot Act," *Associated Press*, September 6, 2007.

in the policy adoption phase may have been a function of political pressure or not wanting to appear contrary to the dominant mood. Such support, if not reinforced, could evaporate during implementation and result in undoing of the policy. [266]

Matland's final cell in the matrix defines situations involving the potential for high policy ambiguity and high policy conflict. He classifies these situations as symbolic in nature and has posited that they are typically linked to important values and principles. With only a referential goal, differing perspectives and a proliferation of interpretations of the vision will emerge, according to Matland. He suggests that substantial variation in programs and coalition strength will occur across locations (or stakeholder groups). The strength of these coalitions, he says, is the determining factor in the success or failure of policy implementation. As Matland describes it, in symbolic implementation, expert professions play an important role and provide direction and influence. The conflicts that can emerge between expert professionals may be long and fierce. He suggests that expert professionals may exercise their influence from the core of competing coalitions, exacerbating conflict and the degree of competition at the local (execution) level. [267]

Though the NIPP lays out a vision for nationwide CI/KR protection, it is much less clear where the NIPP risk management framework is headed. The burden and costs of risk assessment and CI/KR protection improvements fall almost entirely on the shoulders of CI/KR owners and operators, the great majority of whom are in the private sector and function in a highly competitive marketplace. There are a number of different risk assessment approaches in use, but no clear standard. Given this ambiguity and potential for conflict over long-term CI/KR protection initiatives, and the current policy regarding the NIPP risk management framework in particular, application of Matland's Ambiguity-Conflict Matrix would seem appropriate. The questions below are derived from his discussion of symbolic (high ambiguity / high conflict) implementation. [268] They are offered here as a possible way to assess the NIPP risk management framework as implementation of high ambiguity / high conflict public policy in homeland security.

---

[266] Richard E. Matland, "Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation," 163-165.

[267] Ibid., 168-170.

What local- or execution-level coalitions exist; what are their positions on the matter of the policy to be implemented; what power or influence do they exert; and what relative effect might they have on the implementation process?

What expert professional or academic stakeholders may be involved; what are their positions on the matter of the policy to be implemented; with what local- or execution-level coalitions might they be aligned with and supporting?

What steps are being taken to reduce the ambiguity surrounding the policy's goals by working with both the originating policy-makers and political stakeholders on one end, and the various local- or execution-level constituencies on the other?

What change management framework has been established to manage ambiguity and conflict by coordinating implementation efforts across governmental agencies, among execution-level coalitions, and between expert professional stakeholders?

4. Homeland Security as a Complex Wicked Problem

In his July 2006 paper on Risk and Decision-Making in Homeland Security, Robert Ross quoted General Alexander Haig who said, "When there is confusion in the center, there is chaos at the periphery." [269] In assessing the confusion that seems to exist around the implementation of risk management policy in homeland security, Ross cogently describes the issues of complexity, uncertainty, and ambiguity that surround questions associated with risk management decision-making as a wicked problem. He puts his finger squarely on the matter when stating, "When potential alternative solutions adversely affect stakeholders representing legitimate but irreconcilably opposed public and/or private goods, 'wickedness' will be due not so much to the nature of the problem in a technical sense as to the environment in which the decision-maker must decide." [270] Though the technologies associated with risk assessment and management are

---

[268] Richard E. Matland, "Synthesizing the Implementation Literature," 170-171.

[269] Robert Ross, *Risk and Decision-Making in Homeland Security*, 2-3.

[270] Robert Ross, *Risk and Decision-Making in Homeland Security*, 11-12.

challenging enough, it is also the social context in which these approaches must be developed and implemented that contributes greatly to making it a wicked problem.

To illustrate his point, Ross provides a graphic that could easily apply to the implementation of just about any other major strategic change in homeland security policy, but is especially true concerning implementation of the NIPP risk management framework, one that is national in scope and must stretch across all levels of government and the private sector (see Figure 13). He further suggests that the challenges faced by DHS decision makers in addressing the complexity of risk, to include gaps in understanding and credibility among stakeholders, may have much to do with a tendency to address truly wicked problems with decision-making approaches more suited to conventional or "tame" problems. [271] This finding echoes the words of Jeff Conklin in his discussion of wicked problems and complexity when he asserts that the sense of chaos and futility that often accompany wicked problems causes some leaders to accept the situation as inevitable. According to Conklin, leaders often fail to recognize wicked problems for what they are and persist in applying traditional linear thinking and problem-solving methods that are inappropriate for the complex and nonlinear challenges they face. He suggests that this complexity requires new understandings, processes, and tools better suited to the "fundamentally social and conversational nature of work." [272]

[271] Robert Ross, *Risk and Decision-Making in Homeland Security*, 13-14.

[272] Jeff Conklin, "Wicked Problems and Social Complexity," 3.

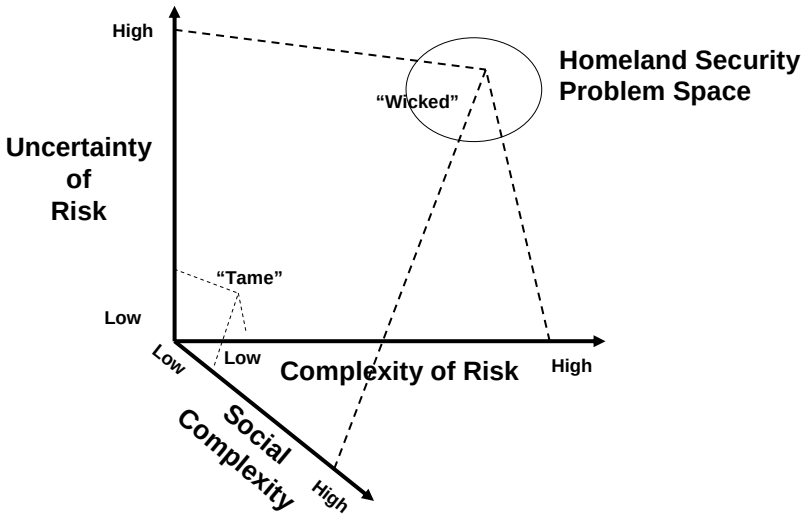

Figure 13. The Homeland Security Decision-Making Environment [273]

To paraphrase John Holland, complex adaptive systems include these features: many agents constantly acting and reacting to each other; highly dispersed control with many levels or layers of interaction; all agents having niches to exploit which are constantly evolving or propagating so they never reach equilibrium; constant rearrangement as a function of learning, experience, evolution, and adaptation; and spontaneous self-organization. [274] By their nature, critical infrastructure and key resource (CI/KR) protection efforts by private and public sector organizations across the nation, whether formally sponsored by DHS or not, represent a large-scale complex adaptive system. Only one part of this system, albeit perhaps the most formal part, is represented in the sector partnership model under the NIPP, which itself is a complex adaptive system. As such, the activities and outcomes associated with the sector partnership model can neither be fully planned nor controlled by DHS alone. This includes the implementation of the NIPP risk management framework.

As suggested by Beverly Parsons, leaders must align attention and resources in such a way as "to help accelerate the movement in a natural direction, even though it is

[273] Robert Ross, *Risk and Decision-Making in Homeland Security*, 13, Figure 2.

[274] John Holland, *Hidden Order*, 1-40.

unplanned or uncontrolled." [275] Parsons describes complex adaptive systems as living in a world somewhere between being stable and organized, but not yet fully unorganized or in chaos. In this in-between world, a complex adaptive system strives to self-organize and bring coherence through dissent, learning, experimentation, evolution, and adaptation, with new patterns constantly emerging, but in a way that is unpredictable and largely uncontrollable. In considering the problems and opportunities of mobilizing work from a position of little or no authority, Ronald Heifetz offers that that task of leadership in such a context is primarily one of education, and choreographing and directing that learning through new ideas and the shaping of attitudes and behaviors. [276] Recognizing that they do not have total control of outcomes, leaders must facilitate the natural process of learning and adaptation by helping to generate agreement and certainty across the system. The greater the level of agreement and certainty, the more order and predictability will follow. The less agreement and certainty, the more the system will tend toward chaos.

Conklin points out that complexity contributes to fragmentation, where a large and diverse set of actors perceive themselves as more separate than united, and information and knowledge are chaotic and scattered, making the harnessing of collective intelligence and achieving consensus challenging or even virtually impossible. [277] He suggests that complexity, problem solving, and learning are closely interdependent and that the flow of this learning is collaborative and opportunity driven. The harder the problem, the more organizational learning involved, the greater the need for collaboration. To energize such learning and collaboration, the fragmentation of the system must be addressed by achieving coherence. Coherence means fostering a collective sense of meaning, clarity about roles, a common understanding of the problem, and a shared sense of commitment to address it. Coherence helps increase the level of agreement and decrease uncertainty, as described by Parsons. This makes it easier to advance collaboration and the sharing of collective intelligence, inherent across the larger

---

[275] Beverly Parsons, "Attending to Self-Organizing Systems in Cluster/Initiative Evaluation," 3.

[276] Ronald Heifetz, *Leadership Without Easy Answers*, 183-231.

[277] Jeff Conklin, "Wicked Problems and Social Complexity," 13.

system, as needed to solve the problem. On leading collaborative networks in the face of complexity, Chris Huxham and Siv Vangen outline three media they view as essential to success. Similar to Tichy's Technical, Political, Cultural (TPC) framework, Huxham and Vangen suggest leaders focus on structure – how the network is arranged and what organizations and people participate; processes – formal and informal communications, and how and what information is transmitted and shared; and people – the roles they play and how leadership is acknowledged, distributed, and exercised. [278]

Coherence, networking and collaboration, information sharing, and organizational learning are key to leading complex systems in the implementation of public policy as strategic change. Absent any real prescriptive guide or even general theory for homeland security leaders to manage complex systems and address wicked problems, the following questions are offered based on the review of the ideas and research presented previously. Like the questions outlined earlier in this chapter, this list is by no means comprehensive or totally reflective of current theory. It is simply provided as another lens through which to assess the implementation of strategic change in homeland security policy, and in this case, the implementation of the NIPP risk management framework.

Assessing Leadership of Complex Adaptive Systems

> What strategies are in place to achieve shared meaning of key terms and concepts; clarify organizational and participant roles and responsibilities; ensure a common understanding of the problem; and generate a shared commitment to implementation?
>
> How are networking and collaboration being structured and facilitated; what groups, organizations, and individuals are involved; how is leadership being defined and distributed; and how are emergent networks being accommodated and encouraged?
>
> What mechanisms have been established for communication and information sharing; how are research, emerging concepts, and lessons-learned being propagated; and what framework has been set up for knowledge management and organizational learning?

[278] Chris Huxham and Siv Vangen, "Leadership in the Shaping and Implementation of Collaboration Agendas: How Things Happen in a (Not Quite) Joined-Up World," 1159-1175.

> How much time and attention are leaders devoting to nurturing the social process of change as opposed to its mechanics; and how are leaders being prepared to lead others in a highly complex, often ambiguous, and potentially conflict-prone environment?

B. ASSESSMENT OF THE CURRENT SITUATION

1. The Challenge of Implementing Risk Management Policy

The National Infrastructure Protection Plan (NIPP), Sector-Specific Plans (SSPs), and the NIPP risk management framework represent a translation of the strategic intent of both the president and the Congress as national policy for critical infrastructure and key resource (CI/KR) protection to include the implementation of a risk management approach. The challenges involved in implementing this policy are well articulated in Kentucky's State Official's Guide to Critical Infrastructure Protection, produced in 2003.

> Implementing a comprehensive national critical infrastructure effort requires extraordinary organization, clarity of purpose, common understanding of roles and responsibilities, accountability, and a detailed and clear process of coordination. The overlap of Federal, state and local governance and the ownership structure of our critical infrastructures present significant protection challenges. The stakeholders and entities involved, both public and private, are multiple and diverse, and the level of understanding of roles and responsibilities varies. The range of protective activities that each must undertake is vast and changes across infrastructures. And the protection authorities across Federal, state and local jurisdictions overlap in many instances and vary greatly. [279]

The implementation of the NIPP as well as its risk management framework as national policy requires the cooperation and commitment of not only the 500 or so entities participating in the sector partnership model, but thousands of individual public and private sector CI/KR owners and operators across the country that these entities represent. Except in cases where new federal regulations have been enacted (i.e., the chemical industry), non-federal participation in NIPP implementation is largely voluntary. Nonetheless, the NIPP sector partnership model represents a framework for

---

[279] Barry Hopkins, *State Official's Guide to Critical Infrastructure Protection* (Lexington, KY, Council of State Governments, 2003), 39.

public-private sector networking and collaboration for homeland security unprecedented in its scope. As remarkable as this partnership may be, there are signs that the hardest part may be yet to come, and fault lines in the partnership may be emerging.

A July 2007 review of the SSPs by the GAO found that, given the differences in the plans to-date, it is unclear to what extent DHS will be able to identify gaps and critical interdependencies across the sectors as part of any national roll-up. Perhaps most significant among GAO findings was that there are differing views regarding the value of the SSPs. The GAO report said that, while 10 of the 32 council representatives interviewed reported that they saw the plans as useful, representatives of 8 councils disagreed. [280] The central element of those plans is a sector-specific approach to the risk management framework guidance provided by DHS. Of the SSPs not restricted and available for public review, only the transportation and water sectors had a robust discussion of the sector's general approach to risk management. However, neither described a common and integrated approach to risk assessment, the core element of any risk management framework. Though the NIPP itself outlines a basic approach to risk management, it does not provide a common method or metrics for risk assessment. Instead it suggests only a set of baseline criteria for risk assessment methodologies that may be employed by individual sectors, and little else.

Notwithstanding the fact that implementing the NIPP risk management framework is a complex and truly wicked problem, it does reflect the will of the president, the Congress, and the secretary for Homeland Security to implement a compatible national program for risk assessment and risk management. Though some progress has been made within individual DHS components, development of unique and incompatible CI/KR risk methodologies continues, and efforts to coordinate integration have been fragmented and, at times, hindered by significant changes in organizational structure and leadership. The bottom line is that, as of this date, other than the NIPP baseline criteria, there are no common lexicon, no organizing schema, and no national risk assessment standard that respond effectively to the guidance received. To repeat the words of

---

[280] Government Accountability Office, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*, 3-6.

Alexander Haig, "When there is confusion in the center, there is chaos at the periphery." If DHS cannot implement an integrated department-wide risk assessment and risk management program, how can it be expected that industry sector coordinating councils will be able to effectively implement and sustain sector-specific programs, compatible within themselves, across other sectors, and with DHS? Despite the incredible accomplishment achieved in the establishment of the NIPP sector partnership model, and the delivery of initial sector-specific plans, the realization of the overarching goal of the NIPP will be slowed unless there is accelerated and compatible progress in the implementation of the risk management framework that is so central to its success. The risk management framework is the proverbial "long pole in the tent" when it comes to national CI/KR protection. It is what everything else hinges on.

The 2007 Homeland Security Appropriations Bill states, "Unfortunately, the fiscal year 2007 budget request offers no details of how risk assessment was used in its formulation or even which DHS agency was tasked with prioritizing risks and assigning them resources….The Committee directs DHS to report by January 16, 2007, on the direction that will be taken to make certain all elements of the Department involved in risk assessment activities are using compatible risk assessment methodologies including risks from all hazards and are coordinated with each other." [281] The March 2007 DHS report to Congress in compliance with its request was largely unresponsive.

Though the DHS report to Congress did indicate that progress had been made, and identified the responsibilities and efforts of individual DHS components, it outlined no plan for integration or the implementation of compatible risk methodologies as directed. Though the report acknowledged general agreement within DHS that standardization of policies, definitions, methodologies, and metrics were needed, it also acknowledged a lack of internal agreement over the particulars of how that standardization should be achieved. The report correctly asserted that there is no one "right way" to assess risk and

[281] U.S. Department of Homeland Security, "Improving Use of Risk-Informed Decision-Making in DHS - Report to Congress in Response to House Report 109-476 to the Fiscal Year 2007 Department of Homeland Security Appropriations Bill," 1.

that DHS manages risk differently across different operating environments. [282] However, this masks the fact that, particularly within the area of critical infrastructure protection, there is still a great degree of compatibility that can be achieved, as reinforced by GAO audits cited earlier in this paper as well as the independent progress made by individual components, like the Coast Guard and its Maritime Security Risk Assessment Methodology (MSRAM) and Maritime Assessment and Strategy Toolkit (MAST) programs.

The DHS report to Congress itself cited a December 2005 GAO audit that stated, "Success will depend partly on continuing to improve various technical and management processes that are part of risk management... In the longer term, progress will depend increasingly on how well risk management is coordinated across agencies, because current approaches in many ways are neither consistent nor comparable." [283] The GAO went on to say that the "danger in using different methods is that if agencies develop systems and methodologies without some overall coordination, they may end up with redundant or incompatible systems that have little or no ability to inform one another. Even more important, these systems may provide decision makers with unreliable or incomplete data." [284] In response, DHS indicated steps it intends to take, to include validating existing risk assessment methods; providing a conceptual foundation, guidelines, and defined processes for developing new methods; conducting reviews of assessment processes; and embracing a mechanism that permits credible comparison. [285] However, these steps have not been implemented, more than a year and a half later.

Clearly DHS has been challenged to implement risk policies, concepts, standards, and methodologies that provide for an appropriate level of compatibility and integration. It is suggested here that despite heroic efforts to wrestle with this challenge, conventional program management approaches have thus far failed. Only through a candid assessment

---

[282] U.S. Department of Homeland Security, "Improving Use of Risk-Informed Decision-Making," 3.

[283] Government Accountability Office, *Risk Management – Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, 94.

[284] Ibid., 94.

[285] U.S. Department of Homeland Security, "Improving Use of Risk-Informed Decision-Making in DHS - Report to Congress in Response to House Report 109-476 to the Fiscal Year 2007 Department of Homeland Security Appropriations Bill," 4.

of how it manages strategic change will the department come to grips with this very complex and wicked problem. The following pages attempt to consider implementation of the NIPP risk management framework as strategic change, and apply a basic set of questions, adapted from the research, as a way to assess opportunities for improvement. Information available to support this research was limited, and thus the analysis that follows is intended to only be representative of how homeland security leaders may apply change management, public policy, and complexity theory to better organize and facilitate large-scale strategic change. It is hoped that this work will spur further research into the development of change management models for homeland security.

2. Assessing Management of the Strategic Change Process

This section attempts to apply the questions for Assessing Leadership of Strategic Change outlined earlier in this chapter to the implementation of major homeland security policy, as represented by the National Infrastructure Protection Plan (NIPP) risk management framework. These questions have been adapted from the work of John Kotter and his Eight-Stage Process of Creating Major Change, and Sergio Fernandez and Hal Rainey in their synthesis of the research resulting in the Determinants of Successful Organizational Change in the Public Sector. The combined work of these researchers, as presented here, has significant empirical and theoretical support and can be applied with a high degree of confidence by homeland security leaders when considering the basic steps to employ in organizing, implementing, and assessing large-scale strategic change. However, given the political and bureaucratic nuances of public policy implementation, and the additional challenges involved in addressing issues of high ambiguity and complexity, it is suggested that the questions outlined here be augmented with alternative perspectives from both the public policy and complexity theory disciplines. Accordingly, additional questions from these perspectives are posed in sections 3 and 4 that follow.

<u>What is being done to ensure the need and establish a sense of urgency</u>?

The basic need and sense of urgency for the application of risk management approaches as national policy to guide homeland security decision-making and resource allocation has been well established in directives from the president, in federal legislation by the Congress, and in strong and frequent statements of strategic intent by the

Homeland Security secretary himself. This sense of urgency has been echoed in numerous reports published by the Government Accountability Office (GAO) and the Congressional Research Service (CRS). Moreover, in statements before Congress and elsewhere, experts from DHS, prestigious research institutions, academia, other government agencies, and the private sector have reinforced the basic wisdom of applying risk management and risk assessment approaches to homeland security.

Has a guiding coalition been established and policy-maker commitment obtained?

Despite its complexity and the extensive impact it will have on the entire homeland security community, there is not yet a multi-disciplinary, public/private sector governance body to establish the long-term vision for a NIPP risk assessment framework and guide the planning and implementation efforts necessary to achieve that vision. Largely in response to stakeholder concerns, the department implemented an internal Risk Assessment Policy (RAP) working group. The purpose of RAP was to exchange information among DHS components and address compatibility issues across methodologies. Based on GAO assessments to date, the group apparently made little headway. It had no authority and was typically attended by lower-level staff that had no measurable influence on DHS risk policy. The RAP group has since shifted focus to the integration of risk assessment results across DHS for purposes of internal priority setting and budgeting under the Risk Assessment Process for Informed Decision-making (RAPID), jointly managed by the Policy Directorate and Chief Financial Officer. [286]

Until just this year, with the creation of the Office of Risk Management and Analysis (RMA), DHS did not have a central body solely focused on coordinating and integrating its risk assessment efforts. Guidance to RMA is provided by an internal Risk Steering Committee (RSC), chaired by the undersecretary for National Protection and Programs, with membership from the various DHS components. [287] The creation of RMA is clearly an important step forward. However, other than what may ultimately

[286] U.S. Department of Homeland Security, "Improving Use of Risk-Informed Decision-Making in DHS - Report to Congress in Response to House Report 109-476 to the Fiscal Year 2007 Department of Homeland Security Appropriations Bill," 3-4.

[287] U.S. Department of Homeland Security, "National Protection and Programs Directorate – Office of Risk Management and Analysis," 9-14.

surface through the NIPP sector partnership model, there is no external participation in homeland security risk policy decision-making from academia, the private sector, state and local government, or professional associations representing related disciplines. Failure to effectively tap these constituencies may inadvertently slow the implementation of the NIPP risk management framework and work against broad-based acceptance and commitment to the goals of this important evolution in homeland security policy.

Has a refined vision been developed, and a change strategy and plan prepared?

The vision for risk management, at least as it pertains to critical infrastructure and key resource (CI/KR) protection, is outlined in the National Infrastructure Protection Plan (NIPP). The description of the NIPP risk management framework defines the basic elements of the risk management process and assigns roles and responsibilities for DHS, federal Sector-Specific Agencies (SSAs), state and local government, and the private sector. In an effort to bolster a sense of urgency and advance this vision, DHS required SSAs to develop Sector-Specific Plans (SSPs) that were to include measures to implement risk management practices within each sector. However, as discussed in previous chapters, results have been mixed and GAO has raised questions concerning the completeness of the plans and the ability of DHS to integrate the results of sector-based risk assessments, given the absence of compatible methodologies. [288] These results seem to indicate that there is not the degree of readiness or commitment needed to fully implement risk management approaches across private sector industry and state and local government. This may stem from the advancement of the vision in a way that outpaced, or neglected, the involvement and influence of important non-DHS stakeholders.

Under considerable pressure to advance a national risk assessment framework, DHS may be inadvertently outrunning the very stakeholders essential to its execution — public and private sector CI/KR owners and operators who have a huge stake in the game. Though a governance structure for overall NIPP implementation has been organized, no such supporting structure has been established for risk management as the core element of the NIPP. Absent a guiding coalition with the requisite authority and

[288] Government Accountability Office, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*, 3-6.

expertise to steer the change effort, DHS lacks a detailed change management plan with specific objectives, strategies, milestones, accountabilities, and measures for success. Beyond setting a vision, that plan must focus attention not only on important technical issues, like how compatibility across risk assessment methodologies will be resolved, but also on how the political and social dynamics of change will be managed. This includes how the buy-in and commitment of non-federal partners will be achieved.

How is the vision being communicated and broad-based action mobilized?

The secretary for Homeland Security has been an energetic advocate of risk-supported decision-making for homeland security throughout his tenure. Reference to his strategic intent in this regard is made in almost every public statement. To advance the implementation of the NIPP, the department has organized a groundbreaking partnership with the private sector and other governmental agencies. Through that partnership, it has communicated not only the vision for national CI/KR protection, but the vision for a national risk management framework as well. In DHS sponsored conferences, sector council meetings, and in an extensive array of print and electronic media, DHS has worked hard to get the word out about the NIPP and its risk management framework. But that, it seems, is as far as it goes concerning the risk management framework. SSAs have been delegated the responsibility for pursuing the advancement of SSPs to include a sector-specific approach to risk management, consistent with the overall NIPP framework. But unlike the general administrative support provided to the councils by DHS, there is little, if any support evident for the coordinated pursuit of sector-specific risk management programs.

It appears that SSAs and industry Sector Coordinating Councils (SCCs) are on their own, and even those within DHS do not appear to be working together to advance compatible risk assessment regimes, according to recent GAO and CRS reports. Risk management expertise in DHS is limited to a select few people in key roles, and most such work is actually performed by various consultants working for different DHS components, using different methodologies. With notable exceptions (i.e., the nuclear industry), such expertise is likely minimal or nonexistent in the SCCs. Without a guiding coalition, a change management plan, and a support network of like-minded experts to

energize and coordinate grass-roots risk management efforts, it will be difficult, if not impossible, to mobilize broad-based action to implement national risk policy. Active engagement across all stakeholder groups by leaders in the guiding coalition is especially important to demonstrate commitment. Leaders must walk-the-talk, breaking deadlocks, uncovering and removing obstacles, encouraging risk-taking and innovation, and visibly promoting success. This is too large a task for DHS leaders alone. A top-level, multi-disciplinary, public-private, coalition is needed to build broad-based support.

Are needed resources and support being marshaled to overcome resistance?

As John Kotter points out, the nature of strategic change is that the lack of one or more steps in the process can have a cascading effect and decide the ultimate success of the change itself. Absent a guiding coalition, a change management plan, and broad-based support, there is little foundation for deciding on where and how to apply limited leadership time and resources to build the momentum necessary to overcome resistance. Given the state of risk management activities within DHS, and the fact that SSAs and SCCs are on their own in establishing risk programs, it would seem that few if any resources are being applied to front-line implementation of the risk assessment framework. Those resources are not just financial and technological but human as well. Implementing the risk policy will require a tremendous commitment of leadership time, and a support network of risk experts, that can assist grassroots implementation. There is significant leadership potential and knowledge resident across the entire sector partnership. Identifying these leaders, providing the needed resources, and developing a cadre of like-minded risk experts must be important parts of any change management strategy.

Are steps being taken to breed success by generating short-term wins?

Nothing breeds success like success. A key role of change leaders is to model and promote desired behavior. Risk management is not only central to the implementation of the NIPP, but is a key pillar for everything that DHS does in the name of homeland security. Nonetheless, this significance does not seem to be reflected in the level of activity among DHS risk professionals in national conferences, professional associations, or in academic or research forums. For example, at the 2006 Grants & Training

Conference attended by the author and hundreds of other homeland security leaders from across the country, there was not one DHS risk professional on the only panel dealing with the subject. Moreover, DHS has not sponsored a conference devoted to this issue as a way to stimulate the sharing of best practices. Despite successful risk programs by the Coast Guard and the former Office for Domestic Preparedness, there appears to be little promotion of these successes, no assessment of their performance, and little sharing of lessons learned. Nor have any additional resources been devoted to reinforcing "change leaders" who exemplify the spirit of the change vision and goals.

How are gains being consolidated to expand and sustain the change?

There does not seem to be a deliberate effort to leverage change by capitalizing on the success of existing CI/KR risk assessment programs. Both the Coast Guard and the Office of Grant Programs have been advancing risk assessment for the port and transit sectors respectively since shortly after the terrorist attacks of September 2001. Though there is much in both of these programs that can be applied generically across sectors, their success, it seems, has been all but ignored in the pursuit of a single cross-sector approach in the Risk Analysis and Management for Critical Asset Protection (RAMCAP) program. With the exception of the creation of RMA, there is little to suggest that DHS has begun to aggressively institutionalize risk management as general policy, skill, or discipline, though the NIPP does indicate that a CI/KR protection qualification course is in development. There are only two risk assessment courses currently offered for non-DHS personnel by the DHS Training and Education Division (TED), and these were developed independently from all other DHS risk assessment programs. [289]

What efforts are underway to anchor the new approaches in the system?

Though it may have made progress in advancing the use of risk-based decision-making within DHS, it is not apparent that the department has attained any measure of success in going beyond risk assessment and running the full risk management cycle. This is essential if it is to demonstrate the efficacy of the policy to stakeholders and generate enduring support in a way that will help anchor the change. RMA is still new,

[289] Federal Emergency Management Agency, "Training and Education Division - Course Catalog," 10, http://www.ojp.usdoj.gov/odp/docs/TED_Course_Catalog2007.pdf [Accessed august 10, 2007].

and its initial focus appears to be on getting the DHS house in order before expanding its reach outside to things like the CI/KR risk assessment. It could not be determined, either from discussions with DHS staff and consultants, or from the available literature, how RMA, or DHS as a whole, plans to align or realign organization or processes to further advance its risk management policy. Lessons from the Coast Guard's experience with institutionalizing risk management throughout the service may be instructive for the entire department, and merit study and consideration as a possible model to follow.

How well are the organization's systems and subsystems aligned?

The prior question, as adapted from the research of Kotter and Fernandez and Rainey, deals with the work of making system-wide adjustments in the way the organization functions as necessary, to anchor and sustain the change over the long-term. This work does not just occur at the end of the implementation process, but is continuous throughout. An organization's systems and subsystems must be in alignment with the purpose of the change, and each other, if the change is to be successful. One way to consider this alignment is through Noel Tichy's Technical, Political, and Cultural (TPC) Framework. Though certainly not intended to be a comprehensive assessment, the following provides a representative look at NIPP risk management implementation across the various elements of the TPC Framework in a way that demonstrates its utility.

External Environment – The cost of homeland security is enormous, and the administration is increasingly challenged to manage discretionary spending while balancing national security needs with other domestic priorities. Congress has become impatient with DHS on the matter of risk management decision-making to guide homeland security investments, and this impatience is fueled by recurring reports from GAO and CRS that point to the pace of progress and the challenges that must be overcome. State homeland security directors feel they have been left out of the policy-making process and that they lack an understanding of the DHS approach to risk. Private sector partners in NIPP implementation question the utility of Sector-Specific Plans and have not uniformly implemented risk management regimes within their industry sectors.

Mission and Strategy – The strategic intent to implement risk-based decision-making to guide homeland security priorities and investment has been clear and emphatic – from the president, the Congress, and the secretary for Homeland Security. A plan for organizing national CI/KR protection efforts has been developed to include a vision for risk management. The description of the NIPP risk management framework defines the basic elements of the risk management process and assigns roles and responsibilities to various stakeholders. However, it does not clarify what specific changes are necessary in the way things are being done now, and simply leaves it up the stakeholders to figure out how to implement their part of the change. Absence of a definitive change management plan that specifies objectives, strategies, milestones, accountabilities, and measures for success will hamper the definition of tasks and ultimate accomplishment of the change.

Tasks – If the mission and strategy are out of alignment, so too will be the tasks necessary to carry them out. In implementing the NIPP risk management framework, various tasks must be performed by a large and diverse number of stakeholders, both across DHS and the larger CI/KR protection community. It is not enough to identify and assign a task and expect it to be executed in harmony with the rest of the system, particularly if the owner is not even in the same organization. The capability and the means to carry out the task must also be considered. At present, risk management tasks, and especially risk assessment methods, are inadequately defined, and the capability to carry these out at the grassroots level is open to question. The complexity of these tasks, and the uncertainty involved, have significant implications for the alignment of the structures, processes, and people, essential to implementing the vision for change.

Prescribed Networks – Once tasks, and what is needed to carry them out, are known, the prescribed networks of jobs and their interrelationships can be defined. Two key factors here are the division of labor, or differentiation among units, and how these units interact to integrate their work. Though the NIPP defines basic division of labor for risk management, it does not define well how the efforts among stakeholders will be integrated to accomplish its goals. Nor does it appear from the NIPP or SSPs that the relationships to support risk management within sectors have been identified to include the type and placement of new capabilities that will surely be needed. The prescribed

network of the sector partnership model provides DHS with a unique framework through which to engage industry and other stakeholders. Building on and extending that network to adequately support sector risk management will be vital to the success of the NIPP.

Organizational Processes – Particularly in networks such as the NIPP sector partnership model, common processes for communication, management control, and problem solving are what bind the network together. As the sector partnership model evolves, the processes for administering the risk management framework will need to evolve with it. That partnership relies on a hierarchy of sector councils and crosscutting councils to manage communications across the network. Communications and management control through such a structure may not be the most effective way to develop and implement complex and still uncertain risk management practices. A new network of subject matter experts may be needed that is more agile in advancing sector-based risk management programs, driving technical compatibility and integration with DHS, and pursuing policy issues like information security and private sector incentives.

People – Almost exclusive responsibility for CI/KR protection rests on the shoulders of owners and operators. Motivation to participate in NIPP risk management efforts is largely voluntary and assumed to come from good corporate citizenship and enlightened self-interest. DHS has been very successful in motivating high-level private sector participation in the NIPP sector partnership. However, there are significant legal and economic concerns, and the burdens of risk management bureaucracy and perception of uncertain returns could dampen commitment. New incentives are needed, and DHS must demonstrate the efficacy of its risk management framework or stand to lose much of what it has gained. Accelerating its efforts will require not only new risk processes, but also a new cadre of security risk managers across government and industry. This will mean the creation of an entirely new professional discipline and national network.

Emergent Networks – Concurrent with the prescribed networks of any enterprise are unanticipated informal networks that emerge as people and groups react to and in one way or another attempt to influence (or hold the potential to influence) the direction of change. The NIPP sector partnership is so large and complex that emergent networks, which could either help or hinder risk management implementation, may go unnoticed or

simply be neglected. Neutralizing the effects of negative influences and capitalizing on, and even encouraging, positive ones could help accelerate the pace of change. Likely sources within the sector partnership include trade groups, industry associations, and individual corporate alliances. Outside the partnership, emergent networks may be found in professional associations like the Security Analysis and Risk Management Association (SARMA), or in academic partnerships among risk analysts and researchers. Wherever these networks lie, they should be considered, and when possible, exploited. There is no indication that NIPP implementation considers the implications of emergent networks.

3. Assessing Change as Public Policy Implementation

In many ways, the implementation of public policy can be more challenging and conflict-ridden than almost any other type of strategic change. Risk management for homeland security is an example of just such a policy. Given the high degree of ambiguity, extreme complexity, and high potential for conflict, homeland security leaders must not only consider the mechanics of the change process, but also its political and social context, and factor these into any change management strategy. The questions below are derived from the summary of high ambiguity - high conflict policy implementation in Chapter IV. These questions, and the brief analysis that follows each, are offered as representative of the kind of self-assessment homeland security leaders might make when considering the implementation of a major public policy initiative. The analysis that follows is limited by the availability of information from open sources.

What local or execution-level coalitions exist; what are their positions on the matter of the policy to be implemented; what power or influence do they exert; and what relative effect might they have on the implementation process?

Though SSAs are responsible for coordinating CI/KR protection planning, in reality it is the SCCs and CI/KR owners and operators who must implement industry and asset-level risk management activities. Though the NIPP, sector partnership model, and SSP process were an imposition from above, there was a remarkable degree of cooperation across the board. However, advancement of the risk management framework by the SSAs, absent any global coordination and resolution of risk assessment

compatibility issues (i.e., terminology, metrics, standards, methods, training etc.), is bound to lead to friction as DHS continues to strive for a more integrated and compatible framework overall. Moreover, as a higher degree of granularity is obtained concerning sector vulnerabilities and risks, it is possible that additional conflict between DHS and private sector stakeholders will emerge as pressure mounts for industry-wide application of countermeasures. Given that much of the burden will fall on their shoulders, industry stakeholders can exert powerful influence on the outcome of the NIPP risk management framework. It will be important, therefore, to facilitate development and implementation of risk management and assessment methods in a way that justifies industry confidence.

State Homeland Security Advisors (HSAs) have responsibility for coordinating CI/KR protection initiatives within their states. Most have ongoing programs to work with CI/KR owners and operators on security efforts, and some have advanced state legislation to enforce security standards. They are the conduits for data into the DHS National Asset Database (NADB), which is used to assess national-level risk and to inform risk-based grant allocation. These officials also drive state-level homeland security planning and provide stewardship for risk-based grant requests for CI/KR protection. However, the majority feels insufficiently involved in the policy-making process and that DHS has not adequately explained how to calculate risk. Though SCCs have been in operation for over a year, DHS has just recently organized the State, Local, Tribal, Territorial Government Coordinating Council (SLTTGCC) to represent the states in NIPP implementation. HSAs are powerful stakeholders and wield considerable clout through their governors and state congressional delegations. Having them onboard in support of risk policy implementation as well as advancing the use of compatible methodologies within their states would be a force-multiplier to the overall effort.

Building industry confidence in the efficacy of national risk management policy and obtaining strong HSA commitment will require devoting sufficient resources and expertise to working with and in support of SSCs and the states in their individual risk management efforts, while simultaneously advancing the state-of-the-art in risk management practice to include pursuit of national standards.

What expert professional or academic stakeholders may be involved; what are their positions on the matter of the policy to be implemented; with what local- or execution-level coalitions might they be aligned with and supporting?

Though individual academic institutions are independently providing various levels of research support to CI/KR protection efforts, there does not seem to be any national-level academic network sponsored by DHS to advise on the overall problem of homeland security risk management policy, integration, and standards. The first DHS funded "center-of-excellence," the Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California, is devoted to developing models and tools for evaluating the costs and risks of terrorism. The Center for Risk Management of Engineering Systems at the University of Virginia is also a source of top-level risk expertise with a highly regarded research program. The Wharton Risk Management and Decision Processes Center is yet another such institution. However, it does not appear that these schools are being tapped in an integrated way to help guide national risk management policy and practice. The exception is the Critical Infrastructure Protection Program at George Mason University, which is providing direct advisory assistance to the Office of Infrastructure Protection (OIP), the Partnership for Critical Infrastructure Security (PCIS), and select SCCs in support of NIPP implementation. [290]

The American Society of Mechanical Engineers (ASME) strongly supports the application of risk management approaches to design and decision-making. In 2004, ASME was tapped by DHS to develop the Risk Analysis and Management for Critical Assets Protection (RAMCAP) methodology, cited in the NIPP as a principal approach to analyzing CI/KR risks across sectors. Two associations specifically devoted to the risk analysis profession are the Society for Risk Analysis (SRA) and the Security Analysis and Risk Management Association (SARMA). SRA is a multi-disciplinary organization whose members and interests span the entire risk analysis spectrum. The mission of SARMA is devoted entirely to advancing the standing and competency of security and risk analysts focused on risks from man-made threats. By far, the largest group representing public and private sector security professionals is the American Society for

[290] George Mason University, "Externally Funded Projects," http://cipp.gmu.edu/projects/ [Accessed July 10, 2007]

Industrial Security (ASIS), with 35,000 members worldwide. ASIS sponsors training and credentialing programs and is advancing its All Hazards Risk Management Best Practices Standard. Among its members are those on the front line of CI/KR protection efforts.

Academic institutions and professional associations can add considerable value to NIPP risk management implementation. This includes the advancement of common practices and standards and the education and certification of the next generation of security and risk analysts needed to ensure the long-term success of national CI/KR protection policy. Fully harnessing this capability will require creation of new national-level councils dedicated to guiding the development of risk practices, technologies, education, and certification as an integral part of the NIPP sector partnership model.

What steps are being taken to reduce the ambiguity surrounding the policy's goals by working with both the originating policy-makers and political stakeholders on one end, and the various local- or execution-level constituencies on the other?

Managing the process of change as public policy is mostly about managing ambiguity and conflict. Reducing uncertainty about the vision and clarifying specific and realistic goals and objectives for policy implementation are essential to setting expectations and winning the support of elected officials and other senior policy-makers. It is also essential to obtaining the commitment and active contribution of those who must execute the policy at the grassroots level. If you don't have the first, you are unlikely to get much of the second. The NIPP, for the first time, sets out a national vision for risk management. Though the NIPP risk management framework defines the basic elements of the risk management process, and assigns roles and responsibilities for governmental and private sector partners, the NIPP itself says little about the "how" or specifically "what" will be implemented. The details have essentially been left for the SSAs to work out with their respective SCCs and reflect in their individual sector plans. Based on GAO assessments, and the author's review of the sector plans recently issued, there is still ambiguity about how, if at all, DHS will be able to measure and aggregate risk within and across sectors. As the saying goes, you can't manage what you can't measure.

It is not evident from any of the materials openly available that DHS has a deliberate change management plan with objectives and milestones that describe how it

will facilitate the realization of the risk management framework outlined in the NIPP. If you don't know where you are going, any road will take you there. It is reasonable to assume that the lack of a definitive change management plan, and the wherewithal to implement it, has been what has hindered DHS in the pursuit of risk management implementation to date. A considerable amount of planning, outreach, and promotion has gone into the advancement of the NIPP and SSPs. But the "long pole in the tent" is still the risk management framework and, within that, the compatible risk assessment methodologies that must be at its core. As in the development of the NIPP, the implementation planning process becomes the medium for dialogue with policy-makers on one side and policy-executers on the other. Unless conditions have changed with the creation of Risk Management and Analysis (RMA), a review of the March 2007 DHS report issued to Congress on the status of efforts to date did not provide assurance that a plan for implementation of risk management policy yet exists; no plan, no basis for dialogue. With no basis for dialogue, ambiguity and conflict persist and the vicious cycle continues. Time goes by, leadership changes, policy shifts, and the process repeats itself.

As difficult as it has been to establish the NIPP sector partnership model and deliver SSPs, it will be even more challenging and complex to realize a national framework for CI/KR risk assessment as envisioned by DHS. It will require, at minimum, the same sort of planning and stakeholder engagement that has made the NIPP initiative itself so successful to date. In harmony with the existing sector partnership model, a new set of players will need to be brought to the table; ones who can help untie the Gordian Knot that has become homeland security risk management policy.

What change management framework has been established to manage ambiguity and conflict by coordinating implementation efforts across governmental agencies, among execution-level coalitions, and among expert professional stakeholders?

One strategy to deal with the complexities of advancing public policy, finding solutions to implementation challenges, and building commitment to the intended change is a process that "gets all the players in the room" called the Stakeholder Council Model. This model has been used with great effect thus far in the advancement of the NIPP through the Critical Infrastructure Partnership Advisory Council (CIPAC). CIPAC provides the structure through which different levels of government and the private sector

now collaborate on CI/KR protection planning and initiatives. As described in Chapter III, it is a far-reaching collaborative network-of-networks that is largely self-managed, diverse in character, and national in scope. It is a remarkable unsung achievement of DHS and its CIPAC members, and likely one of the most innovative government/industry collaborations since World War II. Cross-sector coordination and integration is to be achieved through government and private industry cross-sector councils that span the CIPAC. This sort of framework is vital to overall NIPP governance. However, it is questionable whether the CIPAC alone, as structured, is adequately suited to resolving the highly complex technical aspects of developing and installing risk management and assessment programs within individual industry sectors in a way that ultimately leads to internal, cross-sector, regional, and national integration. Moreover, the evolution of CIPAC initially emphasized the DHS and SSA relationship with industry sectors and has largely left state and local governments out of the picture. This is notwithstanding the fact that much DHS focus is otherwise targeted on CI/KR protection efforts at a state or urban region level as part of the Homeland Security Grant Program (SHGP), which is increasingly becoming a risk-driven process.

It is important to note the fact that risk management and assessment for high consequence-low probability events, especially terrorism, is a brand new field. There is no common lexicon; there are no common practices; and there are no professional standards or training programs to provide for consistency and compatibility, unlike the fields of accounting or engineering. The implementation of the NIPP risk management vision cannot assume that individual sectors will be able to nurture and grow these on their own. A variety of risk assessment methodologies already exist, but were developed for specific applications and in isolation from one another. Though different settings may require different approaches, the general lack of compatibility is still problematic, as pointed out on numerous occasions by GAO.

If the NIPP vision is to be realized, it will be incumbent on DHS to invest in and accelerate the development of this new professional field at the same time it is working to foster technical integration. DHS cannot do this in isolation. New alliances and networks will need to be established with academia and professional associations like

SARMA and ASIS for harmonization of professional practices, the development of standards, and the training and education of CI/KR risk management and security analysts and leaders. Just as the sector partnership model was an innovative solution to a new and complex problem, DHS will need to think anew about how it partners with subject matter experts from academia, the professional associations, and the practitioner community to address this need, which is on the critical path to NIPP implementation. It will also require engaging state and local government as important allies in the process. State and local governments are closest to CI/KR owners and operators in their respective jurisdictions and are in the best position to facilitate asset-based and regional risk assessment and management.

4. Assessing Change in Complex Adaptive Systems

CIPAC and the sector partnership model is by definition a complex adaptive system that has been organized by DHS to respond to a truly wicked problem – that of securing the nation's vast and highly interdependent critical infrastructure and key resources. As Garnett Williams defines them, the properties of complex adaptive systems include a) a large number of similar but independent elements or agents; b) persistent movement and responses by these elements to other agents; c) adaptiveness so that the system adjusts to new situations to ensure survival; d) self-organization, in which order in the system forms spontaneously; e) local rules that apply to each agent; and f) progression in complexity over time so that the system becomes larger and more sophisticated. Accordingly, the behavior of such complex systems cannot be predicted and may evolve to a point somewhere between order and chaos. [291]

Though CIPAC appears to be very orderly when presented in the NIPP, it is likely to be anything but that in reality, as different sector councils are at different stages of maturity, with different cultures, perspectives, industry demands, and levels of commitment and leadership. As CIPAC matures, DHS must be open to the dynamic and seemingly chaotic nature of complex adaptive systems and understand that the behavior, direction, and evolution of such systems can never be fully planned or controlled.

[291] Garnett Williams, *Chaos Theory Tamed*, 234.

Influencing the performance of these systems has perhaps more to do with facilitating the natural process of learning and adaptation than trying to steer the actual content of the work itself. The following questions are derived from the discussion of open systems, complexity, and networks in Chapter IV. They are presented here as yet another lens through which homeland security leaders may assess strategic change in a highly networked environment. Adapted by the author from a blending of emerging theory, they are only representative of how leaders may think about these issues from another perspective. Different situations may prompt different questions. The supporting analysis is restricted to what information was immediately available from open sources at the time of this writing, and the author's own limited exposure to the problem space.

What strategies are in place to achieve shared meaning for key terms and concepts; clarify organizational and participant roles and responsibilities; ensure a common understanding of the problem; and generate a shared commitment to implementation?

Absent forces to the contrary, the complexity of wicked problems tends to move an organization or system toward increasing degrees of fragmentation, where information and knowledge are scattered and isolated. The larger the system, the greater the tendency toward complexity, and the more there will be the potential for fragmentation. As an organization fragments and tends closer to chaos, it attempts to self-regulate and adapt to cope in a way that brings greater order. Leaders can facilitate this process by helping to bring coherence to the system. DHS and the SSAs walk a fine line as responsible delegates at a federal level for critical infrastructure and key resource protection, but absent the firm hand of regulation, have correspondingly little control over the ground-level security of most of the nation's critical assets, particularly the large majority of infrastructure resources in private sector hands. Too firm a hand and voluntary industry participation will begin to evaporate. No influence at all and the sectors will evolve in isolation and, as complexity grows, so too will the fragmentation level and a tendency toward chaos.

The NIPP brings coherence to the national effort to protect critical infrastructure. It establishes common goals, definitions, and concepts; defines roles and responsibilities; and organizes the complex adaptive system that is now CIPAC. This coherence is further advanced by the activities of the SCCs and cross-sector councils that support self-

governance and intra- and inter-sector coordination and information sharing. The irony here is that the very structure that gave the CIPAC life can also be the thing that strangles it if the structure is too restrictive and not itself open to change and adaptation. The more CIPAC members accept the mantel of self-governance, the more the SCCs will tend to evolve in unanticipated ways, and possibly not consistent with the view from the ivory tower. DHS must support and accelerate this evolution and not restrain it. It must also be prepared to change and adapt itself accordingly.

Given uncertainty and complexity, implementation of the risk management framework as a cornerstone of the NIPP will require change and adaptation in CIPAC and possibly DHS itself. DHS must facilitate this adaptation if it has any hope of influencing CIPAC behavior in the direction of a common, compatible, well integrated, and yet differentiated risk management framework. At present, there does not appear to be an overarching plan for risk management implementation, and it seems there are no structures or mechanisms in place to bring coherence and influence the direction of risk management efforts by SCCs and industry partners. Like the larger problem of CI/KR protection, implementation of a national risk management framework is a wicked problem, one requiring its own complex adaptive system, its own network-of-networks.

How are networking and collaboration being structured and facilitated; which groups, organizations, and individuals are involved; how is leadership being defined and distributed; and how are emergent networks being accommodated and encouraged?

The sector partnership model is the primary organizational structure for coordinating national CI/KR protection activities. The model is based on voluntary self-governance, with DHS providing overall guidance, tools, and support consistent with the NIPP. At the core of the partnership are the SCCs as the principal entity for coordinating with the government on CI/KR protection initiatives. SCCs are self-organized and self-managed enterprises that represent the interests of the broad base of owners and operators in a sector. [292] DHS and SSA leadership from the federal side is determined by assigned roles and responsibilities within the federal agency hierarchy. Leadership from within the cross-sector councils and the SSCs is largely self-determined and/or self-selected. Rules governing membership and leadership are typically spelled out in a council charter.

[292] Garnett Williams, *Chaos Theory Tamed*, 54.

While the sector partnership model provides a formal networking structure, it is unclear how it facilitates flexibility for timely adaptation and change, or how it deals with emergent networks that may be a precursor to the need for that change. One example of the need for change is the process necessary to implement sector-specific risk programs consistent with the overall vision for a risk management framework. The NIPP essentially assigns out the task of advancing sector-specific risk programs to the SSAs. However, as Laurence O'Toole points out in his discussion of wicked problems in public administration, such problems cannot be addressed simply by dividing up the pieces and delegating authority. [293] If DHS lacked the internal knowledge and expertise to address the challenge of risk management implementation within the department until now, as evidenced by repeated GAO reports cited earlier in this paper, why would farming out the problem to the SAAs under the sector partnership model get better results? The only exception thus far may be the Coast Guard with its MSRAM and MAST programs.

The Coast Guard and its risk management partners work with individual port communities, and can be viewed as an emergent network that responded, on its own, to changing environmental conditions (i.e., the need and overarching policy for CI/KR risk management). Likewise, ODP's work with the Port Authority of New York and New Jersey in 2002 to develop a risk assessment model that morphed into the successful Port and Transit Risk Assessment Technical Assistance Program can also be viewed as an emergent network. The work of George Mason University with the National Capital Region on regional CI/KR protection is yet another. DHS must examine how existing or new emergent networks are accommodated in the sector partnership model and, perhaps more importantly, how these networks may be exploited to accelerate the pace of change toward a national risk management framework. Especially important here is what can be learned from emergent networks and how DHS and industry sectors exchange lessons learned and manage knowledge transfer. Under conditions of complexity, shared knowledge provides the basis for addressing ambiguity, lessening fragmentation, and achieving greater coherence in the system.

---

[293] Laurence O'Toole, Jr., "Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration," 45-52.

What mechanisms have been established for communication and information sharing; how are research, emerging concepts, and lessons-learned being propagated; and what framework has been set up for organizational learning and knowledge management?

Cross-sector government and industry coordinating councils are one means by which the NIPP sector partnership model attempts to provide for communication and information sharing across sectors. The previously established Information Sharing and Analysis Centers (ISACs) have also provided and continue to provide this function within individual industry sectors. In addition, DHS has implemented the Homeland Security Information Network (HSIN) in an effort to interconnect and provide information sharing among homeland security communities of interest. HSIN is identified in the NIPP as yet another possible method for CI/KR collaboration. Procedural or transactional methods such as these and other "publish and subscribe" formats for information sharing may facilitate the cataloging and storage of information, but do little to advance organizational learning. As discussed earlier, learning is a key characteristic of an adaptive organization.

It is not apparent from a review of the open source material that risk assessment and management research, emerging concepts, and lessons learned are being effectively directed, coordinated, shared, and applied as a part of an integrated overarching strategy within DHS or across the NIPP sector partnership model. What is apparent is that different DHS components have at different times, and with different kinds of outside expert assistance, advanced independent efforts absent any unifying risk schema. Some of these efforts have blossomed into apparently successful large-scale risk assessment programs within a given industry sector or sub-sector (i.e., U.S. Coast Guard MSRAM and MAST programs), while others have not matured beyond initial fielding. Though there is apparently some significant research underway to address discrete analytical challenges, academic research and development in support of homeland security risk assessment initiatives does not seem to flow from a coherent research and development plan specifically tied to a change management strategy for implementation of the national risk management framework. As important as that work may be, absent an integrated risk assessment and management framework, it may not achieve its full potential.

In his assessment of wicked problems and social complexity, Jeff Conklin suggests that complexity, problem solving, and learning are closely interdependent, and the flow of this learning is a social process that is collaborative and opportunity driven.[294] In a complex adaptive system, like the sector partnership model, control is highly dispersed and distributed throughout the network; there is no hierarchical command and control, and behavior is unplanned and for the most part uncontrollable. In such a system, leadership is about influencing behavior in the desired direction by facilitating the process of organizational learning and adaptation. In 1990, Peter Senge described the "leader's new work" in learning organizations as "the ability to build shared vision, to bring to the surface and challenge prevailing mental models, and to foster more systemic patterns of thinking. In short, leaders in learning organizations are responsible for building organizations where people are continually expanding their capabilities to shape their future – that is, leaders are responsible for learning." [295]

Fostering collective organizational learning within the sector partnership model will be essential to advancing the change and adaptation necessary to implement the NIPP risk management framework. Like CI/KR protection in general, implementing a national risk management framework across 17 industry sectors, in a way that can provide risk comparisons both within and across those sectors, is a very complex and wicked problem. There is still no common risk lexicon and no common and compatible set of methodologies for CI/KR risk assessment. Developing these, and building a new profession around CI/KR risk assessment and management at the same time, is beyond the capacity of DHS and the current members of the partnership alone. It will require effectively tapping and networking, in a more coordinated and integrated way, the expertise and problem-solving capability that resides in research and academic institutions, in professional associations, and in an emerging network of risk practitioners in both government and the private sector. Now that the CIPAC is substantially formed, and the first iterations of SSPs have been submitted, this should be the primary focus of effort for DHS and the SSAs. It will require developing a knowledge management

---

[294] Jeff Conklin, "Wicked Problems and Social Complexity," 3-9.

[295] Peter Senge, "The Leader's New Work: Building Learning Organizations," *Sloan Management Review* 32, no. 1 (Fall 1990): 7-23.

framework for risk assessment and risk management best practices as well as the training and education channels and curricula necessary to produce a new generation of CI/KR security and risk management leaders.

How much time and attention are leaders devoting to nurturing the social process of change as opposed to its mechanics, and how are leaders being prepared to lead others in a highly complex, often ambiguous, and potentially conflict-prone environment?

Establishing a vision, organizing resources, motivating and guiding participation, overcoming resistance, and maintaining motivation for success are all vital leadership tasks. The importance of these tasks is even more acute when leading without formal direct authority, such as within a complex adaptive system like the NIPP sector partnership model. Chris Huxham and Siv Vangen cite research studies verifying that active involvement (or the absence of it) by top executives has a determining influence on the success or failure of any collaboration initiative. [296] Accordingly, they conclude that successful collaboration requires significant energy, commitment, skill, and continual nurturing on the part of the leaders involved. Huxham and Vangen state that wherever leaders achieved success, it was due to the significant personal attention they paid to championing the cause and managing the media of collaborative leadership. [297]

It is clear from public statements and congressional testimony from various senior DHS officials, and the author's own experience in various coordinating council meetings, that considerable DHS and SCC leadership time and attention has been, and continues to be, devoted to NIPP implementation and CI/KR protection initiatives in general. It would likely not have been possible to achieve the successful implementation of the sector partnership model to this point without such a commitment. However, as the partnership expands and the network of relationships and extent of activity grows, this level of DHS senior executive involvement is probably not sustainable over the long term. DHS will need to increasingly rely on an expanded network of leaders across the various coordinating councils and within the various sectors. Ensuring a common vision,

---

[296] Chris Huxham and Siv Vangen, "Leadership in the Shaping and Implementation of Collaboration Agendas: How Things Happen in a (Not Quite) Joined-Up World," 1159-1175.

[297] Chris Huxham and Siv Vangen, "Leadership in the Shaping and Implementation of Collaboration Agenda, 1168-1171.

leadership competence, and alignment with overall national CI/KR objectives will continue to be a challenge without a comprehensive training and education program.

Regular meetings of council leadership groups sponsored by DHS helps to increase coherence and provide opportunities to exchange leader experiences and discuss associated challenges in the search for shared solutions. Most if not all of these leaders are already seasoned executives in industry or government, and so are not new to the task. However, joint development and implementation of a comprehensive change management plan for advancing the NIPP risk management framework will tend to challenge even the most able executives, who, though experts in their own particular industries or government roles, are likely not sufficiently schooled in what is a still the complex and emerging field of CI/KR risk management, with little or no guidance to draw on. Moreover, the cadre of CI/KR security and risk analysts that these leaders will rely on does not currently exist. Nor do the common tools, standards, and practices exist that are necessary, if the NIPP risk management vision is to be realized.

The NIPP recognizes the importance of education and training, and generically describes the types that are unique or essential to CI/KR protection: risk assessment and risk management, risk management cost-benefit analysis, resource allocation based on risk management priorities, CI/KR interdependency analysis, and best practices in CI/KR protection programs. [298] The challenge is that in the absence of better definitions of risk assessment and risk management as applied to homeland security, there does not seem to be significant movement on what the NIPP describes as an education and training effort that will be national in scope. As a strategy for sustainable CI/KR risk management and protection over the long-term, DHS must begin work now to advance risk assessment and risk management standards development and associated training, education, and certification programs, all of which will take time to develop.

To advance comprehensive training and education and certification programs, it will be important for DHS to establish collaborative alliances among select academic institutions at the forefront of developing practices in this area. It will also be important

[298] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 79-82.

to directly engage and network professional associations like SARMA, SRA, and ASIS around professional standards development, training, and certification criteria for CI/KR security and risk analysts, leveraging existing capabilities, delivery mechanisms, and membership to the greatest extent possible. Finally, the Homeland Security and Defense Education Consortium (HSDEC) is another possible vehicle for advancing both CI/KR leadership development and technical skills education, to include risk assessment and management. HSDEC is a nationwide network of teaching and research institutions focused on promoting education, research, and cooperation related to and supporting the homeland security and homeland defense missions. [299]

[299] Homeland Security and Defense Education Consortium, "Introduction," http://www.hsdec.org/default.aspx, [Accessed August 21, 2007].

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FINDINGS AND RECOMMENDATIONS

A. FINDINGS

1. The Sector Partnership Model is a Remarkable Success

The National Infrastructure Protection Plan (NIPP) is a translation of the strategic intent of both the president and the Congress as national policy for critical infrastructure and key resource (CI/KR) protection. The highly networked nature of the nation's critical infrastructure itself is reflected in the complex adaptive network formed under the NIPP – the sector partnership model and the Critical Infrastructure Partnership Advisory Council (CIPAC). This nationwide network of over five hundred member entities spread across thirty-six different councils and seventeen different CI/KR sectors, representing thousands of CI/KR owners and operators nationwide, requires public/private sector collaboration on a scale possibly not seen since World War II. In the author's view, the implementation of CIPAC as a self-managed, collaborative, network-of-networks has been a remarkable success thus far for the Department of Homeland Security and its CIPAC partners.

2. Implementation of Risk Management Policy is Problematic

Over the years, DHS has been challenged to develop and implement a consistent and coordinated approach to risk assessment and risk management. For the first time, the NIPP establishes an initial vision for risk management as applied to CI/KR protection. Unfortunately, DHS has left the development and implementation of sector-specific risk management programs largely up to the Sector-Specific Agencies (SSAs). This, it appears, leaves SSAs and their industry partners on their own to develop what DHS has yet been unable to provide thus far. Risk management is the cornerstone of the NIPP. Risk assessment methodologies are the most vital elements of that process, and possibly the Achilles heel to risk management policy implementation. If compatibility of risk assessment approaches cannot be resolved, then implementation of the risk management framework will be hindered, and achievement of NIPP goals will be compromised.

3. Absence of a Change Management Plan Risks Failure

The protection of the nation's CI/KR assets, to include assessment and management of risks and the priority application of resources in response, is a complex wicked problem. As discussed earlier in this paper, most strategic change efforts tend not to achieve their initial intent, or fail entirely, because key steps in the management of strategic change were either omitted or not sufficiently executed. As a wicked problem, implementation of risk management policy will require the same creative thinking about public/private partnership, networking, and collaboration that has made the CIPAC so successful to date. There does not appear to be any structure or organizing schema to assist the SSAs or otherwise coordinate and integrate efforts across sectors or between levels of government. Absence of a guiding coalition, a comprehensive change management plan, and associated structure and resources to steer implementation of the risk management framework will likely result in a failure to realize its achievement.

4. Not all Essential Resources are being Applied to the Problem

DHS has been valiantly wrestling on its own with the challenge of implementing risk assessment and risk management policies and practices since its creation. Much of this work has been within the department and among its components, with the help of a variety of consultants, not all necessarily working in harmony. Though it is a large and complex problem, it does not appear that the resources applied to date have been either appropriately organized or sufficient given the scope and scale of the problem. There has not been a broad-based effort to engage external stakeholders, other subject matter experts, or non-federal practitioners on the matter of national risk assessment and risk management policy and practice. The implementation of the NIPP risk management framework will have far reaching implications for CI/KR owners and operators, industry sectors, state and local government, other federal agencies, and the protection of U.S. citizens. An entirely new network of partners must now be created and brought into the mix, necessitating change and adaptation for both CIPAC and DHS.

5. Application of Change Management Models can be Useful

Implementation of the NIPP is a unique large-scale strategic change in public policy, and is representative of subsequent homeland security initiatives of similar scope and scale that are also complex wicked problems. Unlike strategic change in the corporate world, failure to successfully implement new homeland security policies and programs could have catastrophic consequences. A primary purpose of this paper was to assess the implementation of the NIPP risk management framework as strategic change in homeland security policy through the lens of change management, public policy, and complexity theory. In reviewing the literature, basic elements were explored and a modest list of questions reflecting core tenants from each set of theories were tailored and applied to the problem. The product was a hybrid change management model developed from a blending of these theories which can be useful to homeland security leaders in the process of either planning for or evaluating the success of large-scale strategic change. It is hoped this work will spur additional study into the application of change management theory and practice in the development and implementation of homeland security policy and programs.

B. RECOMMENDATIONS

1. Candidly Assess Approach to Change Management

Given all that is at stake, and the external stakeholder perceptions of DHS risk management policy and program implementation efforts to date, it is recommended that a comprehensive and candid assessment be made of how these initiatives have been handled as large-scale strategic change. The findings of this assessment should be immediately used to guide the development and implementation of the NIPP risk management framework and the risk management and risk assessment programs of individual industry sectors. The results may also be instructive in the formulation of a generic homeland security change management model to guide future change initiatives.

2. Establish a Nonaligned Risk Management Advisory Board

The implementation of the NIPP risk management framework has far-reaching implications for the entire critical infrastructure and key resources protection (CI/KR) community, and stakeholders range across all levels of government and private sector industry. The stakes are high, the issues complex, and the consequences of failure great. Accordingly, it is recommended that DHS establish a senior-level, independent, non-aligned Risk Management Advisory Board to advise on the direction of national risk management policy for CI/KR protection, provide strategic direction for implementation planning efforts, and ensure accountability and oversight for DHS risk management activities. Both the National Infrastructure Advisory Council [300] and the Congressional Research Service [301] have recommended similar boards.

3. Organize a Risk Management Coordinating Council

The scope, scale, and complexity of implementing and sustaining a national risk management framework for CI/KR protection is beyond what DHS or the Sector-Specific Agencies alone can do. The sector partnership model must now adapt to accommodate the introduction of a network of risk management stakeholders and subject matter experts that can facilitate the development of risk management practices, tools and techniques. It is recommended that a Risk Management Coordinating Council be formed to assist in the development of the recommended change management plan and be the primary implementation mechanism for the NIPP risk management framework, to include assisting SSAs and SCCs with sector-specific risk management programs. In addition to representation from the individual sector councils, participation must be sought from academia, research centers, professional associations, and the practitioner community.

---

[300] National Infrastructure Advisory Council, *Risk Management Approaches to Protection - Final Report and Recommendations by the Council*, 19.

[301] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, 26.

4. Develop a Comprehensive Change Management Plan

It is recommended that a comprehensive change management plan be developed to guide the implementation of the NIPP risk management framework, particularly as it relates to facilitating and influencing the direction of the individual risk programs of the industry sectors. It should be based on strategic guidance provided by the Risk Management Advisory Board and developed with the participation and input of members of the Risk Management Coordinating Council. The plan must translate the vision and policy goals into specific objectives, strategies, milestones, accountabilities, and measures for success. It must also demonstrate a sound causal link between the actions outlined and the outcomes desired to ensure consistency in approach, as well as provide a means for managing coordination and congruence among all parties involved.

5. Accelerate Standards, Training, Education, and Credentialing

As strategy for sustainable CI/KR risk management and protection over the long term, DHS must begin work now to advance risk assessment and risk management standards development and associated training, education, and certification programs, all of which will take time to develop. It is recommended that DHS pursue strategic alliances with professional associations such as Security Analysis and Risk Management Association (SARMA), the Society for Risk Analysis (SRA), and the American Society of Industrial Security (ASIS) to advance the development and delivery of training and certification programs for CI/KR security and risk analysts. It is also recommended that the Homeland Security and Defense Education Consortium (HSDEC) be engaged to take on the task of working with its members to formulate risk management curricula for incorporation into homeland security executive leadership development and career degree programs at leading colleges and universities.

> The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew. We must disenthrall ourselves, and then we shall save our country.
>
> —President Abraham Lincoln, December 1, 1862

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Adler, Peter, and Jeremy Kranowitz. *A Primer on Perceptions of Risk, Risk Communication and Building Trust.* February 2005.

American Society of Mechanical Engineers. *Statement on the Role of Risk Analysis in Decision-making.* http://www.asme.org/NewsPublicPolicy/GovRelations/Position Statements/Statement_Role_Risk _Analysis.cfm (Accessed August 24, 2007).

Andrews, Patricia, and Richard Herschel. *Organizational Communication - Empowerment in a Technological Society.* Boston: Houghton Mifflin Company, 1996.

Auerswald, Philip, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, eds. *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability.* Cambridge: Cambridge University Press, 2006.

———. "The Challenge of Protecting Critical Infrastructure." Working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, October 2005.

Ayyub, Bilal M. *Risk Analysis in Engineering and Economics.* Boca Raton: Chapman & Hall/CRC, 2003.

Baker, George. "A Vulnerability Assessment Methodology for Critical Infrastructure Sites." Paper presented at the DHS Symposium: R&D Partnerships in Homeland Security, Boston, Massachusetts, April 27-28, 2005.

Bardach, Eugene. *A Practical Guide for Policy Analysis - The Eightfold Path to More Effective Problem Solving*. Washington, DC: CQ Press, 2005.

Beer, Michael, and Nitin Nohria, eds. *Breaking the Code of Change.* Boston: Harvard Business School Press, 2000.

Bennis, Warren. "Leadership of Change." In *Breaking the Code of Change,* ed. Michael Beer and Nitin Nohria. Boston: Harvard Business School Press, 2000.

Bieri, Stephen. "Disaster Risk Management and the Systems Approach." *World Institute for Disaster Risk Management Library* (April 12, 2001): 2-5.

Birkland, Thomas. *An Introduction to the Policy Process: Theories Concepts and Models of Public Policy Making, 2nd ed*. Armonk: M.E. Sharpe, Inc., 2005.

Boin, Arjen, Patrick Lagadec, Erwann Michel-Kerjan, and Werner Overdijk. "Critical Infra-structures Under Threat: Learning from the Anthrax Scare." *Journal of Contingencies and Crisis Management* 11, No.3 (September 2003): 99-104.

Burke, Warner, and George Litwin. “A Causal Model of Organizational Performance and Change.” *Journal of Management* 18, no. 3 (1992): 523-545.

Bush, George. *Homeland Security Presidential Directive 7 (HSPD-7) - Critical Infrastructure Identification, Prioritization, and Protection*. Washington DC: The White House, 2003.

———. *National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: The White House, 2003.

———. “This New Era Requires New Responsibilities.” Transcript of speech by President George W. Bush. *Washington Post*, November 9, 2001, A15.

Caruson, Kiki and Susan MacManus. “Homeland Security Preparedness: Federal and State Mandates and Local Government.” *Spectrum: The Journal of State Government* (Spring 2005): 25-28.

Chertoff, Michael. “U.S. Department of Homeland Security Second Stage Review.” Statement before the United States Senate, Committee on Homeland Security and Government Affairs. Washington, DC, July 14, 2005.

Clinton, William. “Executive Order 13010 - Critical Infrastructure Protection,” *Federal Register* 61, no. 138. Washington, DC: U.S. Government Printing Office, July 17, 1996.

———. *Presidential Decision Directive-63 (PDD-63) – Critical Infrastructure Protection.* Washington, DC: The White House, 1998.

Conger, Jay. “Effective Change Begins at the Top.” In *Breaking the Code of Change*, ed. Michael Beer and Nitin Nohria. Boston: Harvard Business School Press, 2000.

Congressional Budget Office. *Homeland Security and the Private Sector*. Washington DC: Congressional Budget Office, December 2004.

Congressional Research Service. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences.* Washington, DC: Congressional Research Service, September 2, 2004.

———. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences.* Washington, DC: Congressional Research Service, January 19, 2007.

———. *State and Local Homeland Security: Unresolved Issues for the 109th Congress*. Washington, DC: Congressional Research Service, 2005.

———. *State and Local Preparedness for Terrorism: Selected Policy Issues*. Washington, DC: Congressional Research Service, 2002.

———. *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress.* Washington, DC: Congressional Research Service, February 2, 2007.

Conklin, Jeff. "Wicked Problems and Social Complexity." (2006), http://cognexus.org/wpf/wicked problems.pdf (Accessed July 28, 2007).

Connor, Daryl. *Leading At The Edge of Chaos: How to Create the Nimble Organization.* New York: John Wiley & Sons, Inc., 1998.

———. *Managing At The Speed of Change.* New York: Villard Books, 1992.

Daniels, Ronald J., Donald R. Kettl and Howard Kunreuther, eds. *On Risk and Disaster Lessons from Hurricane Katrina.* Philadelphia: University of Pennsylvania Press, 2006.

DeGiorgio, Vincent. "Understanding Your Risk: The Risk Assessment Process." *ArupRisk Consulting* (June 26, 2002).

Dizard III, Wilson. "TSA Rolls Dice On Risk Model." *Government Computer News,* June 4, 2007.

Dory, Amanda J., "American Civil Security: The U.S. Public and Homeland Security." *The Washington Quarterly* 27, no. 1 (Winter 2004): 37–52.

Downs, Brady. "The Maritime Security Risk Analysis Model – Applying The Latest Risk Assessment Techniques to Maritime Security." *Proceedings* (Spring 2007): 36-38.

Dumphy, Dexter. "Embracing Paradox." In *Breaking the Code of Change,* ed. Michael Beer and Nitin Nohria. Boston: Harvard Business School Press, 2000.

Eisinger, Peter. "Imperfect Federalism: The Intergovernmental Partnership for Homeland Security." *Public Administration Review* 66, no. 4 (July/August, 2006): 537-545.

Falletta, Salvatore. "Organizational Diagnostic Models: A Review & Synthesis – White Paper." Leadersphere, Inc. 2005.

Federal Emergency Management Agency. *Multi Hazards Identification and Risk Assessment: A Cornerstone of the National Mitigation Strategy*. Washington, DC: U.S. Government Printing Office, 1997.

———. *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*. Washington, DC: Federal Emergency Management Agency, 2005.

———. *Implementation of the Post-Katrina Emergency Management Reform Act*. http://www.dhs.gov/xabout/structure/gc_1169243598416. shtm (Accessed July 20, 2007).

Fernandez, Sergio and Hal Rainey. "Managing Successful Organizational Change in the Public Sector: An Agenda for Research and Practice." *Public Administration Review* 66, no. 2 (March/April 2006): 1-24.

Government Accountability Office. *Aviation Security – Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls.* Washington, DC: Government Accountability Office, June 2004.

———. *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System*. Washington, DC: Government Accountability Office, September 2006.

———. *Combating Terrorism – Threat and Risk Assessments Can Help Prioritize and Target Program Investments*. Washington, DC: Government Accountability Office, 1998.

———. *Critical Infrastructure Protection - Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics.* Washington, DC: Government Accountability Office, October 2006.

———. *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve.* Washington, DC: Government Accountability Office, July 10, 2007.

———. *Critical Infrastructure Protection – Significant Challenges Need to Be Addressed.* Washington, DC: Government Accountability Office, July 24, 2002.

———. *Homeland Security - Applying Risk Management Principles to Guide Federal Investments.* Washington, DC: Government Accountability Office, February 7, 2007.

———. *Homeland Security - A Risk Management Approach Can Guide Preparedness Efforts*. Washington, DC: Government Accountability Office, 2001.

———. *Homeland Security: Guidance and Standards are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts*. Washington, DC: Government Accountability Office, 2006.

———. *Homeland Security – Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks.* Washington, DC: Government Accountability Office, January 2007.

———. *Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery*. Washington, DC: Government Accountability Office, 2006.

———. *Passenger Rail Security - Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*. Washington, DC: Government Accountability Office, 2005.

———. *Risk Management – Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.* Washington, DC: Government Accountability Office, December 2005.

———. *Transportation Security – Federal Action Needed to Help Address Security Challenges*. Washington, DC: Government Accountability Office, June 2003.

———. *Transportation Security - Systematic Planning Needed to Optimize Resources*. Washington, DC: Government Accountability Office, 2005.

Haimes, Yocav. "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures." *Risk Analysis* 26, no. 2 (April 2006): 293-296.

———. "Roadmap for Modeling Risks of Terrorism to the Homeland." *Journal of Infrastructure Systems* (June 2002): 35-41.

Heifetz, Ronald. *Leadership Without Easy Answers.* Cambridge: Belknap Press of Harvard University Press, 1994.

Hill, Michael, and Peter Hupe. *Implementing Public Policy.* London: Sage Publications, 2002.

Holland, John. *Hidden Order.* Reading, MA: Addison-Wesley, 1995.

Homeland Security Act of 2002. Public Law 107-296, 107th Congress, 2d Session. November 25, 2002.

Homeland Security Institute. *Homeland Security Risk Assessment - Volumes I and II*. Arlington, VA: Homeland Security Institute, 2006.

Hopkins, Barry. *State Official's Guide to Critical Infrastructure Protection.* Lexington KY, Council of State Governments, 2003.

Huxham, Chris, and Siv Vangen. "Leadership in the Shaping and Implementation of Collaboration Agendas: How Things Happen in a (Not Quite) Joined-Up World." *Academy of Management Journal* 43, no. 6 (December 2000): 1159-1175.

Jackson, Rick. "Achieving Strategic Change in Government." *Public Manager* 34, no. 1 (Spring 2005): 40-50.

Jaeger, Carlo, Ortwin Renn, Eugene Rosa, and Thomas Webler. *Risk, Uncertainty, and Rational Action.* London: Earthscan Publications Ltd, 2001.

Jenkins, B. D. “Security Risk Analysis and Management – Risk Analysis Helps Establish a Good Security Posture; Risk Management Keeps It That Way.” Countermeasures, Inc., 1998.

Jenkins, William. *Homeland Security - Applying Risk Management Principles To Guide Federal Investments.* Testimony before the Subcommittee on Homeland Security, Committee on Appropriations, U.S. House of Representatives. Washington, DC, GAO, February 7, 2007.

Jiang, Bin. “Risk Management and the Office of Homeland Security’s Antiterrorism Tasks.” *Online Journal of Peace and Conflict Resolution* 4, no. 2 (2002): 30-36.

Kingdom, John W., *Agendas, Alternatives, and Public Policies, 2nd ed.* New York: Addison-Wesley Educational Publishers Inc., 2003.

Kotter, John, and Dan S. Cohen. *The Heart of Change.* Boston: Harvard Business School Press, 2002.

Kotter, John. *Leading Change.* Boston: Harvard Business School Press, 1996.

———. “Leading Change: Why Transformation Efforts Fail.” *Harvard Business Review* 73, no. 2 (March-April 1995): 59-67.

Kunreuther, Howard. “Catastrophic Risks: Dealing with Interdependencies.” Working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, May, 2006.

———. “Risk Analysis and Risk Management in an Uncertain World.” *Risk Analysis* 22, no.4 (2002): 655-664.

———. “Risk Analysis.” Working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, 2004.

Kunreuther, Howard and Arthur Lerner-Lam. *Risk Assessment and Risk Management Strategies in an Uncertain World*. Philadelphia, PA: University of Pennsylvania and Columbia University, June 2002.

Kunreuther, Howard, Erwann Michel-Kerjan, and Beverly Porter. “Assessing, Managing and Financing Extreme Events: Dealing With Terrorism.” Working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, November 20, 2003.

Lanza, Richard. “Does Your Project Risk Management System Do the Job?” *Information Strategy: The Executive's Journal* 17, no.1 (Fall 2000): 6-12.

Lewis, Ted. *Critical Infrastructure Protection In Homeland Security: Defending a Networked Nation*. Hoboken: John Wiley & Sons, Inc., 2006.

Littlejohn, Stephen. *Theories of Human Communication*, 2nd ed. Belmont, CA: Wadsworth Publishing Company, 1983.

Los Alamos National Laboratory. *Critical Infrastructure Protection Decision Support System Overview*. Los Alamos, New Mexico: Los Alamos National Laboratory, 2004.

Maloney, Carolyn. Member of Congress. Letter to the Secretary for Homeland Security Michael Chertoff, May 18,2007.

Matland, Richard E., "Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation." *Journal of Public Administration Research and Theory* 5, no. 2 (April 1995): 145-174.

McFarlane, Deborah, and Marilyn Gruebel. *Public Management and Policy Implementation: Intersection, Subset, or Neither?* Paper presented at the Fall Conference of the Association for Public Policy Analysis and Management, Madison, Wisconsin, November 3, 2006.

McNamara, Carter. "Basic Definition of Organization - Organizations as Systems." Adapted from *Field Guide to Consulting and Organizational Development.* Minneapolis: Authenticity Consulting, LLC, 2007.

Michel-Kerjan, Erwann. "Disasters and Public Policy: Can Market Lessons Help Address Government Failures?" Working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, January 2007.

Michel-Kerjan, Erwann and Burkhard Pedell. "How Does the Corporate World Cope with Mega-Terrorism? - Puzzling Evidence from Terrorism Insurance Markets." Working paper, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, January 15, 2007.

National Academy of Public Administration. *Advancing the Management of Homeland Security: Managing Intergovernmental Relations For Homeland Security.* Washington, DC: National Academy of Public Administration, February 2004.

National Governors Association. *2006 State Homeland Security Directors Survey*. Washington, DC: National Governors Association Center for Best Practices, 2006.

———. *Homeland Security Policy*. Washington, DC: National Governors Association, July 24, 2007.

National Infrastructure Advisory Council. *Risk Management Approaches to Protection - Final Report and Recommendations by the Council*. Washington, DC: National Infrastructure Advisory Council, October, 2005.

National Research Council. *Risk Assessment in the Federal Government: Managing the Process.* Washington, DC: National Academy Press, 1983.

———. *Scientific Review of the Proposed Risk Assessment Bulletin from the Office of Management and Budget.* Washington, DC: National Academies Press, 2007.

National Science Foundation. "Controlling Dangers: The Truth About Risk Assessment." June 1996.

———. *Integrated Research in Risk Analysis and Decision Making in a Democratic Society*. Arlington, VA: National Science Foundation, July 2002.

Neumeister, Larry. "Judge Strikes Down Part of Patriot Act," *Associated Press.* September 6, 2007.

Oak Ridge Institute for Science and Education. *Expert Panels to Identify and Evaluate Risk Assessment Methods – Fact Sheet*.

Office of Homeland Security. *National Strategy for Homeland Security*. Washington, DC: Office of Homeland Security, July 2002.

Office of the Director of National Intelligence. *National Intelligence Estimate - The Terrorist Threat to the US Homeland.* Washington, DC: Office of the Director of National Intelligence, July 2007.

O'Toole, Jr., Laurence. "Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration." *Public Administration Review* 57, no. 1 (January - February, 1997): 45-52.

Parsons, Beverly. "Attending to Self-Organizing Systems in Cluster/Initiative Evaluation." Paper presented at the In-BC Interprofessional Network Conference, Vancouver, Canada, March 18, 2007.

Peters, B. Guy. *American Public Policy Promise and Performance.* Washington, DC: CQ Press. 2007.

Podziba, Susan. "The Human Side of Complex Public Policy Mediation." *Negotiation Journal* (October 2003): 285-290.

Poister, Theodore, and Gregory Streib. "Strategic Management in the Public Sector: Concepts, Models, and Processes." *Public Productivity & Management Review* 22, no. 3 (March 1999): 308-325.

Public Governance Institute. "White Paper – Launching Change Versus Realizing New Outcomes" (Public Governance Institute – Leading Public-Sector Change. http://www.publicgov.org/LeadChange/WhitePaper/intro.html (Accessed: July 15, 2007).

Radvanovsky, Robert. *Critical Infrastructure: Homeland Security and Emergency Preparedness*. Boca Raton: CRC Press Taylor & Francis Group, 2006.

Rajagopalan, Nandini and Gretchen M. Spreitzer, "Toward a Theory of Strategic Change: A Multi-lens Perspective and Integrative Framework**,"** *The Academy of Management Review* 22, no. 1 (January, 1997): 48-79.

Rancich, Thomas. "Combating Terrorism." *Proceedings of the United States Naval Institute* 126, no. 11 (September-October, 2000): 25-32.

Regens, James, Thomas Dietz, and Robert Rycroft. "Risk Assessment in the Policy-Making Process." *Public Administration Review* 43, no. 2 (March - April 1983): 137-145.

Ries, Al. *Focus The Future of Your Company Depends On It.* New York: HaperCollins Publishers, 1997.

Ritchey, Tom, "Wicked Problems - Structuring Social Messes with Morphological Analysis" (2005), http://www.swemorph.com/pdf/wp.pdf (Accessed July 27, 2007).

Rittel, Horst, and Melvin Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4, no. 2 (June 1973): 155-169.

Roberts, Nancy. "Wicked Problems and Network Approaches to Resolution." *The International Public Management Review* 1, no. 1 (2000): 1.

Roberts, Steven. "Critical Infrastructure Protection and Homeland Security." *Perspectives on Preparedness*, no. 15 (July 2003): 1-12.

Rosenthal, Isadore, Albert Ignatowski, and Christian Kirchsteiger. "A Generic Standard for the Risk Assessment Process: Discussion on a Proposal Made by the Program Committee of the JC-JRC Workshop: Promotion of Technical Harmonization of Risk-Based Decision Making." *Safety Science* 40, no. 1 (2002): 75-103.

Rosenzweig, Paul and Alane Kochems. "Risk Assessment and Risk Management: Necessary Tools for Homeland Security." *The Heritage Foundation, Backgrounder,* No. 1889 (October 25, 2005).

Ross, Robert. "Risk and Decision-Making in Homeland Security." Paper presented at the SRA 2006 Annual Meeting - Risk Analysis in a Dynamic World: Making a Difference, Baltimore, Maryland December 3-6, 2006.

Salamon, Lester. "The New Governance and the Tools of Public Action: An Introduction." In Lester Salamon, ed., *Tools of Government: A Guide to the New Governance.* New York: Oxford University Press, 2002.

Sandman, Peter M., "Risk Communication: Facing Public Outrage." *EPA Journal* (November 1987): 21-22.

Seidman, Harold. Foreword to Thomas H. Stanton, Benjamin Ginsberg, eds., *Making Government Manageable: Executive Organization and Management in the Twenty-First Century*. Baltimore MD: Johns Hopkins University Press, 2004.

Senge, Peter, "The Leader's New Work: Building Learning Organizations." *Sloan Management Review* 32, no. 1 (Fall 1990): 7-23.

Shubnick, Martin, ed. *Risk, Organizations, and Society*. Boston: Kluwer Academic Publishers, 1991.

Shum, S. Bunkingham. "Representing Hard-to-Formalise, Contextualised, Multidisciplinary, Organisational Knowledge." Paper presented at the AAAI Spring Symposium on Artificial Intelligence in Knowledge Management, Stanford University, Palo Alto, CA, March 24-26, 1997.

Sjoberg, Lennart, ed. *Risk and Society*. London: Allen & Unwin Publishers, 1987.

Slovic, Paul, and Elke Weber. "Perception of Risk Posed by Extreme Events." Paper presented at the conference Risk Management Strategies in an Uncertain World, Palisades, New York, April 12-13, 2002.

Slovic, Paul. *The Perception of Risk*. London: Earthscan Publications Ltd, 2000.

———. "Informing and Educating the Public about Risk." In *The Perception of Risk*. London: Earthscan Publications Ltd, 2000.

———. "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battle-field." *Risk Analysis* 19, no. 4 (August 1999): 689-701.

Smislova, Melissa and Brandon Wales. "The Homeland Infrastructure Threat and Risk Analysis Center." Briefing presented at the First Annual conference of the Security Analysis and Risk Management Association. Washington, DC: May 22, 2007.

Smislova, Melissa. *Terrorism Risk Assessment at the Department of Homeland Security*. Testimony before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. November 17, 2005.

Smith, Preston. "Managing Risk as Product Development Schedules Shrink." *Research Technology Management* 42, no. 5 (September / October, 1999): 25-32.

Stacey, Ralph. *Strategic Management & Organizational Dynamics*. London: Pitman, 1996.

Stanton, Thomas. *Improving Federal Relations with States, Localities, and Private Organizations on Matters of Homeland Security: The Stakeholder Council Model*. March 18, 2003.

Stern, Paul, and Harvey Fineberg, eds. *Understanding Risk: Informing Decisions in a Democratic Society.* Washington, DC: National Academy Press, 1996.

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

The President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures - The Report of the President's Commission on Critical Infrastructure Protection.* Washington, DC: The White House, October 1997.

The Rockefeller Institute of Government. *The Federalism Challenge - The Challenge for State and Local Government.* Albany, NY: The Rockefeller Institute of Government, June, 2003.

Thompson, George. "Risk Management for Resource Allocation." Briefing presented at the U.S. Department of Homeland Security 2007 S&T Stakeholders Conference, Washington, DC, May 23, 2007.

Tichy, Noel. *Managing Strategic Change – Technical, Political, and Cultural Dynamics.* New York: John Wiley & Sons, 1983.

Transportation Security Administration. *Risk Management – Risk Assessment Tools.* http://www.tsa.gov/approach/risk/assessment_tools.shtm (Accessed May 12, 2007).

Transportation Security Administration. *Risk Management.* http://www.tsa.gov/approach/risk/index.shtm (Accessed July 10, 2007).

Treasury Board of Canada. *Integrated Risk Management Framework.* Ottawa, Canada: Treasury Board of Canada, April 2001.

University Consortium for Infrastructure Protection. *Critical Infrastructure Protection in the National Capital Region - Risk-Based Foundations for Resilience and Sustainability - Volume I.* Arlington, VA: George Mason University, 2005.

USA Patriot Act of 2001, Public Law 107-56, 107th Congress, 1st Session. October 26, 2002.

USA Patriot Act of 2002. HR 3162, 107th Congress, 1st Session. October 24, 2001.

U.S. Census Bureau. *Statistical Abstract of the United States 2007.* Washington, DC: Government Printing Office, 2007.

U.S. Department of Homeland Security. *Charter for the Critical Infrastructure Partnership Advisory Council.* March 20, 2006.

———. *Council Members, Critical Infrastructure Partnership Advisory Council.* http://www.dhs.gov/xprevprot/committees/ editorial_0848.shtm (Accessed July 20, 2007).

———. "DHS Completes Key Framework for Critical Infrastructure Protection" (May 21, 2007). http://www.dhs.gov/xnews/releases/ pr_1179773665704.shtm (Accessed May 27, 2007).

———. *Directorate for National Protection Programs.* http://www.dhs.gov/xabout/structure/editorial_0794.shtm (Accessed July 20, 2007).

———. *Discussion of the FY 2006 Risk Methodology and the Urban Areas Security Initiative*. Washington, DC: U.S. Department of Homeland Security.

———. *FY 2007 Homeland Security Grant Program -Program Guidance.* Washington, DC: U.S. Department of Homeland Security, January 2007.

———. *Homeland Security Advisory Council.* http://www.dhs.gov/ xinfoshare/committees/editorial_0331.shtm (Accessed July 20, 2007).

———. *Homeland Security Advisory Council Charter.* February 20, 2007.

———. *Homeland Security Grant Program - Risk Analysis*. Washington, DC: U.S. Department of Homeland Security.

———. *Homeland Security Grant Program – Risk Analysis – Fact Sheet.* n.d.

———. *Homeland Security: New Challenges for Decision-Making Under Uncertainty - Final Report.* Washington, DC: February 2004.

———. *Homeland Security: New Challenges for Decision-Making Under Uncertainty - Final Report.* Washington, DC: February 2004.

———. "Improving Use of Risk-Informed Decision-Making in DHS." Report to Congress in Response to House report 109-476 to the Fiscal Year 2007 Department of Homeland Security Appropriations Bill. Washington, DC: U.S. Department of Homeland Security, March 2007.

———. *Keynote Address by Secretary of Homeland Security Michael Chertoff to the 2006 Grants & Training National Conference.* Washington, DC, November 28, 2006. http://www.dhs.gov/xnews/speeches/ sp_1164738645429.shtm (Accessed April 12, 2007).

———. *National Infrastructure Advisory Council.* July 3, 2007.

———. *National Infrastructure Protection Plan*. Washington, DC: U.S. Department of Homeland Security, 2006.

———. *National Infrastructure Protection Plan – Risk Management Framework.* Washington, DC: U.S. Department of Homeland Security, 2006.

———. *National Infrastructure Protection Plan – Sector Partnership Model.* Washington, DC: U.S. Department of Homeland Security, 2006.

———. *National Infrastructure Protection Plan – Sector-Specific Plans.* Washington, DC: U.S. Department of Homeland Security, 2006.

———. "National Protection and Programs Directorate – Office of Risk Management and Analysis." Briefing slides, August 6, 2007.

———. *National Strategy for Homeland Security.* Washington, DC: U.S. Department of Homeland Security, 2002.

———. *Office of the Inspector General – Progress in Developing the National Asset Database.* June 2006.

———. "Remarks by Homeland Security Secretary Michael Chertoff and DNDO Director Vayl Oxford at a Press Conference to Announce Spectroscopic Portal (ASP) Program Contracts." July 14, 2006.

———. "Requested Materials Produced for John P. Paczkowski, Director of Emergency Management, Port Authority of New York & New Jersey." August 24, 2007.

———. *Science & Technology – Strategy to Make the Nation Safer.* Washington, DC: U.S. Department of Homeland Security, June 2007.

———. *Securing Our Homeland, U. S. Department of Homeland Security Strategic Plan*. Washington, DC: U.S. Department of Homeland Security, 2004.

———. *Special Needs Jurisdiction Tool Kit Case Study*. Washington, DC: U.S. Department of Homeland Security, 2003.

———. *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan.* Washington, DC, U.S. Department of Homeland Security, May 2007.

Von Winterfeldt, Detlof. *Information Sharing and Terrorism Risk Assessment*. Testimony Before the Subcommittee on Intelligence, Committee on Homeland Security, United States House of Representatives. Washington, DC: November 17, 2005.

Waldrop, M. Mitchell. *Complexity: The Emerging Science at the Edge of Order and Chaos.* New York: Simon & Schuster 1993.

Weick, Karl. "Emergent Change as a Universal in Organizations." In *Breaking the Code of Change,* ed. Michael Beer and Nitin Nohria. Boston: Harvard Business School Press, 2000.

Wharton School of the University of Pennsylvania. *Risk Management and Decision Processes Center.* http://opim.wharton.upenn.edu/risk/index.html (Accessed August 24, 2007).

Wildavsky, Aaron. "No Risk Is the Highest Risk of All." *American Scientist* 67, no. 1 (January 1979): 32-37.

Williams, Garnett. *Chaos Theory Tamed.* Washington, DC: Joseph Henry Press, 1997

Willis, Henry. *Risk Informed Resource Allocation at the Department of Homeland Security.* Testimony Presented Before the House Appropriations Committee, Subcommittee on Homeland Security. Washington, DC: February 7, 2007.

Willis, Henry, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby. *Estimating Terrorism Risk.* Santa Monica, CA: RAND Center for Risk Management Policy, 2005.

Wormuth, Christine. *Homeland Security Risk Assessments: Key Issues and Challenges.* Testimony before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Committee on Homeland Security, United States House of Representatives. Washington, DC: November 17, 2005.

Zimmerman, Rae, and Vicki Bier. "Risk Assessment of Extreme Events." Paper presented at the conference Risk Management Strategies in an Uncertain World, Palisades, New York, April 12-13, 2002.

Zimmerman, Brenda, Curt Lindberg, and Paul Plsek. *Edgeware: Insights from Complexity Sciences for Health Care Leaders.* Irving, TX: VHA, Inc. 2001.

Zycher, Benjamin. *A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures.* Santa Monica, CA: RAND, 2003.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California