Managing for Performance and Results Series

Strategic Risk Management in Government: A Look at Homeland Security

Improving Strategic Risk Management at the Department of Homeland Security

David H. Schanzer
Associate Professor of the Practice
Sanford School of Public Policy
Duke University

Joe Eyerman
Senior Research Methodologist
Director, Health Security Program
RTI International

Applying Strategic Risk Management to Allocating Resources for Homeland Security: A Case Example of Port Security

Veronique de Rugy
Senior Research Fellow
Mercatus Center
George Mason University

IBM Center for
The Business of Government

2009

MANAGING FOR PERFORMANCE AND RESULTS SERIES

Strategic Risk Management in Government: A Look at Homeland Security

Improving Strategic Risk Management at the Department of Homeland Security

David H. Schanzer
Associate Professor of the Practice
Sanford School of Public Policy
Duke University

Joe Eyerman
Senior Research Methodologist
Director, Health Security Program
RTI International

Applying Strategic Risk Management to Allocating Resources for Homeland Security: A Case Example of Port Security

Veronique de Rugy
Senior Research Fellow
Mercatus Center
George Mason University

IBM Center for
The Business of Government

TABLE OF CONTENTS

TABLE OF CONTENTS

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, "Strategic Risk Management in Government: A Look at Homeland Security," which includes two papers describing how the federal government can increase its capability to undertake strategic risk management in safeguarding the nation. In recent years, the government has devoted increased attention to the use of strategic risk management. The challenge now facing government is to begin to link strategic risk management to resource allocation.


Albert Morales

This report is focused on strategic risk management, which is the process by which decisions are informed by an analysis of risk. Risk management, as defined by the Department of Homeland Security, is the "process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost." Risk management can be applied at several levels: tactical risk management, operational level decisions, and strategic risk management.


David A. Abel

In their paper, "Improving Strategic Risk Management at the Department of Homeland Security," David H. Schanzer and Joe Eyerman describe the recent history of strategic risk management in the department and set forth a series of findings and recommendations directed to the Executive Office of the President, the Department of Homeland Security, and Congress. A key recommendation is that the department enhance the analytical capability necessary for strategic risk management. The recent creation of an Office of Risk Management and Analysis is an important step toward the department's increasing its strategic risk management capability.

In her paper, "Applying Strategic Risk Management to Allocating Resources for Homeland Security: A Case Example of Port Security," Veronique de Rugy presents a case example of how government can link strategic risk management to resource allocation. Dr. de Rugy uses port security as an example of how strategic risk management can be used to analyze threats to the nation, develop scenarios, pose key questions, and develop resource allocation

options. To illustrate the potential of strategic risk management, she presents three resource allocation options as to how the federal government might reallocate its present resources to more cost-effectively respond to security threats to the nation based on risk analysis.

A future line of research involves the assessment and analysis of the types of risk that DHS and federal policymakers should treat as high priorities. For example, what is a risk to a critical infrastructure that an individual business owner or locality should be concerned about which does not rise to the level of a national or homeland security risk? In contrast, which risk passes a threshold "test" and should be classified as a strategic national or homeland security concern? In other words, when does a security risk cease being a purely local or private matter and have the potential to create enough "externalities" to become a matter of strategic concern for the federal government?

Together, the two papers presented in this report provide important information on how the federal government can develop new approaches to using strategic risk management as a tool to assess threats to the nation and begin to allocate resources based on the likelihood and potential consequences of those threats. We hope this report will help federal departments and agencies better understand the use of strategic risk management.

Albert Morales
Managing Partner
IBM Center for The Business of Government
albert.morales@us.ibm.com

David A. Abel
Vice President and Partner
IBM Global Business Services
Homeland Security Account Team
david.abel@us.ibm.com

Improving Strategic Risk Management at the Department of Homeland Security

David H. Schanzer
Associate Professor of the Practice
Sanford School of Public Policy
Duke University

Joe Eyerman
Senior Research Methodologist
Director, Health Security Program
RTI International

Introduction

America awoke on September 12, 2001, to a world in which our vulnerabilities to previously unimaginable acts of violence now seemed limitless. Al Qaeda had laid bare that our massive infrastructures, our globalized, interconnected economy, and the openness of our society could easily be exploited to cause massive harm to persons, property and our national psyche. In the weeks and months following the attacks, it seemed that only the limits of one's imagination could confine the number of scenarios in which terrorists could inflict death and destruction on the United States.

One of the strategic responses to the realization of our widespread national vulnerability was the creation of the Department of Homeland Security (DHS), an amalgamation of different agencies and programs from across the government charged with protecting the nation against attacks, reducing our vulnerabilities, and improving our ability to respond to the full range of threats we might face. In signing the legislation to create the department in December 2002, President George H. Bush said:

> With a vast nation to defend, we can neither predict nor prevent every conceivable attack. And in a free and open society, no department of government can completely guarantee our safety against ruthless killers, who move and plot in shadows. Yet our government will take every possible measure to safeguard our country and our people.[1]

Within this statement lies the great challenge and difficulty of homeland security. On the one hand, we face large scale risks of successful attacks causing catastrophic damage, but on the other, the government and our political leaders feel responsible for taking "every possible measure" to protect the public. In a world of constrained resources, however, choices must be made and much potential harm must be left unaddressed. Deciding how much of our societal resources to dedicate to homeland security and how to allocate those resources across the myriad of homeland security domains is an exceptionally difficult public policy problem. DHS's efforts to answer these questions through a process called "strategic risk management" is the subject of this paper. This paper examines DHS's progress integrating strategic risk management concepts into its budget allocation decisions.

Strategic risk management is a highly complex exercise, fraught with difficulties. While significant progress has been made at DHS theoretical, structural, and political obstacles currently frustrate its ability to allocate its resources based on risk management principles:

- Analytic tools have not been fully developed to deal with the risks created by adaptive adversaries or to compare risks across different threat areas
- Even if such tools were fully developed, DHS does not have methods for examining the effectiveness of their programs in reducing risk
- DHS has not developed a core strategic risk management capability as an agency to set priorities and drive budgeting to those priorities
- Risk tradeoffs are often political decisions that require public input, but mature methodologies for receiving such input have not been developed

- Congressional legislation mandating various security policies and programs, much of which is not based on strategic risk management principles, divert DHS from its risk reduction mission

With new leadership taking office at DHS in January 2009, it is appropriate to evaluate whether DHS is meeting the need to incorporate risk management principles into its resource allocation decisions.

This paper seeks to bolster the Obama administration's efforts by first explaining the difficulty of transferring well-established risk management principles and methodologies to the new, still developing field of homeland security. The paper then summarizes DHS's current approach toward risk based resource allocation based on numerous interviews with agency personnel and congressional staff and identifies the hurdles the agency and Congress face in attempting to develop budgets informed by the concept of risk. The final section contains recommendations for the Obama administration and Congress on steps that they can take to enhance government's ability to allocate efficiently the resources available for homeland security to fulfill the constitutional duty to "provide for the common defense."[2]

The Challenge of Applying Strategic Risk Management To Homeland Security

The concept of strategic risk management is not new. Businesses are constantly assessing the risks they face and taking steps to adjust to changing circumstances—whether it be selling or purchasing new assets, taking on or reducing debt, or increasing or reducing their workforce. On a micro level, families are risk managers as well. We are constantly assessing risks that we face and responding. We purchase insurance to shift certain risks to others. We take steps like fixing an old roof or getting more exercise to mitigate risks to our property or personal health. Certain risk we choose to accept —like the risk of driving to work or allowing an old tall tree to remain right next to our home. The range of choices we make in our lives are, in a sense, a form of strategic risk management.

Application of strategic risk management to the concept of homeland security, however, is relatively new and a poorly understood topic. This section discusses the need to apply strategic risk management to homeland security and identifies many of the difficult challenges of incorporating concepts and tools developed in other areas to this new and evolving area.

The Imperative to Manage Homeland Security Risks

The September 11 attacks (followed shortly thereafter by the anthrax attacks through the U.S. mail) revealed that our society was facing a high level of risk to a variety of types of potential terrorist attacks. In response, the concept of "homeland security"—which had slowly begun to develop during the Clinton administration—emerged as a societal commitment to reduce that risk by strengthening our defenses, reducing our vulnerability, and enhancing our societal resiliency.

At first, the institutional structure for homeland security consisted of a special office within the White House, led by former Pennsylvania governor Tom Ridge, as well as new organizations, programs, and legal authorities enacted by Congress in a whirlwind of legislative activity following 9/11.

In 2002, Congress began working on legislation to create a new federal department to coordinate and at least partially centralize our national homeland security effort. President Bush reversed his initial opposition to the concept later that year and signed legislation into law in December 2002 creating the Department of Homeland Security (DHS). This effort, constituting the largest reorganization of the federal government in 50 years, still only achieved a partial consolidation of homeland security functions, as many security capabilities remained in other federal agencies and the bulk of our nation's protective assets reside in state and local governments. DHS was charged with attempting to harness its diverse components, and coordinate with states, localities and the private sector, to develop a truly national structure for defending the nation against terrorist attacks and certain non-terrorism harms.

Increased funding for enhanced homeland security flowed freely in the initial months following 9/11 through supplemental appropriations measures and large increases for particular programs, such as transportation security. Creation of the DHS brought greater focus to the question of homeland security funding that became the topic of political discourse between Congress and the executive branch, as well as a dialogue between the federal, state, and local branches of government. With the executive branch required to submit its initial budgets for DHS and Congress required to pass appropriations legislation

for the fledgling department, questions such as "How much should we be spending on homeland security?" and "How should we allocate the available funding?" were squarely presented for the first time.

These issues loomed over both Congress and the executive branch as the capacity of our adversaries to do harm seemed unlimited, our vulnerabilities severe, and the calls for federal spending unending. In October 2004, President Bush boasted that he had tripled federal spending on homeland security, including a $3.5 billion increase in funding for state and local responders since 2001.[3] Nonetheless, just one month earlier, an amendment had been proposed in the United States Senate to add $16 billion to the DHS budget for first responder funding.[4] Although the amendment was voted down, its mere consideration demonstrates the lack of any guiding principles to determine how much to spend on security and how those funds should be allocated.

To answer these questions, it was natural to turn to the field of risk science, which has been developing for decades to guide risk reduction efforts in health, the environment, transportation safety, and a variety of other areas. While there is no agreed-upon definition for the term "risk," in its new publication, *DHS Risk Lexicon*, the department's extended definition of risk is "potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence."[5]

By developing tools to make mathematical calculations of these factors, risk science can provide a means of assessing the risk reduction value of a given policy, program, or budgetary investment. Even in fields where risk science is well developed, such as environmental protection, results of risk analysis are still only tools that inform decision making and cannot dictate policy results or replace the need for judgment.

Political dialogue in the years immediately following 9/11—where it appeared that every identification of a potential gap in our security led to proposals for a new program and new spending—made it clear that the government should not promise and could not deliver absolute security from terrorism. Eventually, this reality began to be reflected in the rhetoric of our political leaders, who began to speak in terms of reducing and managing risk. In April, 2002, Tom Ridge noted that "as a free and open and welcoming society, we will always be at risk. We can never totally eliminate it—but we are working every day and using every resource at our disposal to reduce it."[6] In 2005, this concept was adopted as the official doctrine of the Department of Homeland Security by then-Secretary Michael Chertoff, who stated, "we need to adopt a risk-based approach in both our operations and our philosophy…. [r]isk management must guide our decision making as we examine how we can best organize to prevent, respond, and recover from attack."[7]

"Risk management" is defined by DHS as the process by which society attempts to reduce risk "to an acceptable level at an acceptable cost."[8] Identifying risk management as a core principle guiding DHS activities made a great deal of sense.

What is the DHS Risk Lexicon?

In September 2008, the Department of Homeland Security produced the first *DHS Risk Lexicon*. The *Lexicon* initiative is part of the department's Integrated Risk Management Framework to improve its capability to make risk-informed strategic decisions using systematic and structured assessments of homeland security risk. The *Lexicon* supports the Risk Management Framework by defining a single language for DHS Risk management.

The *Lexicon* is the product of the Intra-Departmental DHS Risk Steering Committee (RSC). The Committee is chaired by the Under Secretary of National Protection and Programs Directorate and administered by the Office of Risk Management and Analysis. The RSC provides strategic direction for integrating risk management approaches across DHS by creating working groups to execute special efforts or initiatives. One of those groups was the Risk Lexicon Working Group (RLWG).

The goals of the *Lexicon* initiative were to:

- Promulgate a common language to ease and improve communications for DHS and its partners
- Facilitate the clear exchange of structured and unstructured data, essential to interoperability amongst risk practitioners
- Garner credibility and grow relationships by providing consistency and clear understanding with regard to the usage of terms by the risk community across DHS and its components

Yet, putting this concept into practice in the homeland security domain has proven to be a daunting task. From the earliest days after creation of the department, many placed faith in the idea that we could develop a formula or matrix that could answer the questions such as, "How much should we be spending to keep us safe?" or "Should we be spending more money on chemical detectors on subways or new anthrax vaccine?"

In 2004, the then-chairman of the Select Committee on Homeland Security, Christopher Cox, called on then-Secretary Ridge to conduct a "complete risk assessment to establish 'more concrete goals to make the country safer' and 'deter irresponsible binge spending.'"[9] The deep desire for a methodological way to identify priorities is reflected in this 2003 exchange between Representative Loretta Sanchez and DHS Assistant Secretary for Infrastructure Protection Robert Liscouski:

> **Sanchez:** Can you tell me, does there exist a single document that comprehensively assesses the nation's critical infrastructure risks and serves as a guide for us and for you in our efforts and as far as the spending program? And if not, when do you think that document is going to be ready?
>
> **Liscouski:** I would be surprised, frankly, if we had that done in the next five years. It is going to be an ongoing process. That is sort of peeling away the layers of the onion. The more you learn, the more you realize you do not know.... I am sorry to say we are not going to have that list in that period of time, but clearly we will have our processes in place so we can begin to move. We are doing that work now, but that will be an ongoing process. I do not think that will ever end.
>
> **Sanchez:** What do you think are the most vulnerable infrastructure sectors and how do you make that determination? Do you do it asset-by-asset, regionally? Are you looking at it sector-by-sector? Can you give us some indication? I am sure you probably have this in writing somewhere and you will let us take a look at it.[10]

Key Risk Definitions (From *DHS Risk Lexicon*)

Risk: potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk analysis: systematic examination of the components and characteristics of risk.

Risk assessment: product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Risk management: process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost.

Congress' desire for the department to articulate a risk based set of principles for allocating homeland security spending has not abated. At a hearing on DHS's research priorities in 2007, Representative David Wu told a DHS official that "I am concerned ... about the lack of a strategic plan based on risk assessment that should be the basis for research priorities within DHS.... I strongly encourage you to carry out a detailed, systematic, scientific risk assessment soon so that we know whether our investments are in the right place."[11]

In 2008, Representative Sheila Jackson-Lee echoed the past calls for "a risk management strategy that will help us make rational investment decisions with our homeland security dollars."[12] And in response, DHS Under Secretary for National Protection and Programs Robert Jamison lamented that "while we have made significant progress in our efforts to build an integrated, effective, and harmonized architecture for risk management at the department, we are still in the early stages of a long journey."[13]

The calls for improved risk management have not only emanated from Congress. The 9/11 Commission was among the first of many expert panels to raise the topic, concluding that homeland security funds should be allocated "based on an assessment of threats and vulnerabilities."[14] In 2007, the Government Accountability Office convened an expert panel to identify and address risk management challenges.[15]

In 2008, on the seventh anniversary of 9/11, the Homeland Security Advisory Council listed improving risk management among the top challenges for DHS. The Council concluded:

> Determining the risks to Homeland and using a risk management approach to allocate resources, make decisions, and communicate threats, readiness and protective actions has not been perfected. This will require establishing and improving performance metrics for measuring risk and building a framework for risk-informed decision-making.[16]

Obstacles to Applying Strategic Risk Management to Homeland Security

While the need to apply strategic risk management principles to homeland security is well-founded and compelling, it is important to understand the difficulties of applying this well-established methodology to the new and evolving discipline of homeland security. Identifying these difficulties is essential to establish reasonable expectations as to what can be achieved and chart a rational course for the future.

Practical and Theoretical Difficulties

From the example on page 16, one can begin to grasp the enormity of the task of developing a unified, comprehensive risk assessment that can be used to guide DHS's budget allocation decisions. All the factors that comprise threats are enormously difficult to calculate. Threats (not only from terrorism, but natural disasters and unintentional accidents) are extensive, varied, and uncertain. The scale of estimating the vulnerabilities in our complex, diversified, and densely populated country are massive. And calculating the consequences of a possible event is complicated by the interconnected nature of our economy, where small impacts in one area could have spiraling ripple effects throughout the economy.

Furthermore, we have been using risk science to attempt to inform decision making in areas like environmental protection and workplace safety for decades, but are just beginning to develop methods for quantifying the elements of risk with respect to homeland security.[21] We have well established models to predict how changes in policy will affect the level of air pollution on the population, but these models just don't exist for predicting terrorist attacks.[22]

Given the size of our economy, the resources needed to analyze vulnerabilities across just one sector—transportation, for example—are enormous. As Henry Willis has pointed out, to incorporate risk management into homeland security decision making processes, we will need to ensure that data collection and analytical requirements are "technically and economically feasible."[23] Even estimating the economic consequences will require substantial baseline research that does not now exist.

On top of the foregoing analysis, we need to take into account that homeland security (at least in its counterterrorism aspects) is a qualitatively different subject matter than other disciplines to which risk analysis has been applied in the past. In general, social policy problems that involve dynamic human systems are inherently more complex and difficult to solve than more definable linear scientific problems.[24] These problems involve multiple stakeholders whose interests may be irreconcilable. Social policy problems are rarely "solved," but rather one stage of a solution inevitably leads to new aspects of the same problem, and unintended consequences not only occur, but they are inevitable. Addressing social policy problems does not require selection of the single "right" answer, but rather the application of "judgment based on political and other relevant factors."[25]

Social problems vary in difficulty based on the uncertainty, complexity and social intricacy they present. Homeland security issues rank high on each of these factors.[26]

There is a great degree of uncertainty as to when, where, and how terrorists will attack. Moreover, terrorists are adaptive adversaries. Any action we take to prevent a particular type of attack will lead to a change in the terrorists' strategy and tactics that may render the protective action moot.[27] Take, for example,

A Simple Example of Strategic Risk Management in Homeland Security

The difficulty of developing methodologies to manage the full range of security risks for which DHS is responsible is best explained through a simplified example: How should DHS decide whether to spend an available $5 million on security improvements to the Lincoln Tunnel in New York or on bio-protection suits for first responders in Los Angeles?

Improvements on the Lincoln Tunnel would be important because:

- Terrorists have struck in New York before and therefore are likely to do so again
- The tunnel has vulnerabilities that could be exploited by a terrorist attack to damage it
- If the tunnel is damaged, a large number of people could be killed and there would be severe economic consequences to the local and regional economies

Spending on bio-protection suits in Los Angeles could also be justified because we know that:

- Terrorists have expressed interest in bioterrorism and we believe they are capable of executing a bioterrorist attack
- Biological pathogens can be manufactured and spread throughout large population centers to make people ill
- If there is a bioterrorist attack, having trained and well equipped emergency first responders could save lives

Strategic risk management is a discipline that provides tools that begin to help us make these types of decisions. The concept of "risk" is helpful because it ties together the variables reflected in the example above by defining "risk" as the function of threat, vulnerability, and consequence (R = T x V x C).[17] In this formula, threat equals the likelihood that an attack could occur (which has two components—what the terrorists' intentions are, and their capability to execute such an attack).[18] Vulnerability reflects the likelihood that an attack, if launched, would be successful.[19] Consequences are the total impact that an attack would cause, including both tangible (deaths, damage to property, economic losses) and non-tangible impacts (such as effects on consumer confidence or national pride).[20]

Applying these concepts to the example above, we could attempt (in this grossly simplistic way) to apply risk scores to the two attack scenarios. On a scale of 1 to 10, we might apply a 7 to the threat of a bomb attack on the Lincoln Tunnel, we could say that the bomb terrorists are capable of delivering to that target has a 50 percent likelihood of breaching the tunnel wall, and then estimate that the total consequences of such an attack in terms of lives lost, property and economic damage, and psychological tolls are $2.0 billion. This would give the bomb scenario a risk score of 7 billion. Whereas we could score the threat level of the bioterror attack in Los Angeles as a 5, the likelihood that such an attack would infect 100,000 people at 25 percent, and estimate the consequences of such an attack would be 1,000 deaths and 25,000 long-term illnesses at a cost of $5 billion, for a total risk score of 6.25 billion.

To answer our question about the relative value of the two proposed expenditures, we would need to estimate how each intervention would impact the overall risk. If the hardening of the tunnel wall would reduce the vulnerability from 50 percent to 25 percent, that would lower the tunnel risk score to 3.5 billion. If buying protective suits for first responders would reduce the consequences from $5 billion to $1 billion—that would reduce the risk score of the bioterror attack to 1.25 billion. Under this crude analysis, we lower the overall risk to the nation more with the expenditure on bioterror suits than hardening the Lincoln Tunnel. The concept of risk gives us at least some way to inform comparative judgments across dissimilar domains.

chemical plant security. Intelligence might suggest that terrorist organizations intend to infiltrate a plant and detonate an explosive. In response, we invest millions installing surveillance cameras and otherwise improving perimeter security. Yet, having observed our build-up in perimeter security, the terrorists merely switch tactics to highjacking a rail chemical container in transport.

Measuring risk is also uncertain because we do not know how populations and governments will respond when attacks occur:

- Will there be mass panic, causing huge consequences, or will a response be orderly and effective?
- Will governments respond in a manner proportionate to the risk, or will they overreact and inflict unnecessary harm on economy or the social fabric of society?

We also have to take into account that not only are these risks objectively uncertain, but individuals will have varying subjective evaluations of risk levels (which helps to explain why some people evacuate when a hurricane is approaching and others go surfing).

Homeland security issues are also highly complex. After 9/11 it became more difficult to enter the United States from many Middle Eastern countries on a student visa—which seemed wise after the highjackers came here to study at flight schools. But this policy negatively impacted our colleges and universities and, many argued, deprived us of a strong tool for providing at least some Arab youth a positive image of the United States. The policy has led more Arab students to attend universities in Europe, where radicalization of Muslim youth is more prevalent. Estimating the risk reduction value of the visa tightening policy is therefore extremely complex.

Finally, homeland security problems often involve multiple stakeholders who have varied interests. Take, for example, the issue of screening cargo in foreign ports—which seems to be a commonsense security measure. Any decision regarding these foreign inspections, however, implicates diplomatic relations with the other countries, multiple corporate stakeholders, unknown and unpredictable impacts on the global supply chain, government employment issues, protection of proprietary information, data integrity issues, and customs collection matters to name but a few of the stakeholders and interests.

Strategic Risk Management Is a Process, Not a Formula

All of these difficulties make analyzing homeland security risks an especially "wicked" problem. Such problems are not amenable to solutions based on simple risk formulas, but rather require discourse-based, multi-party, conflict resolution techniques.[28] In an ideal world, DHS would be able to produce a list of our top five security priorities with a scientific formula explaining how the ranking was developed and how federal spending will systematically reduce the societal risk our nation faces. But this notion is entirely unrealistic.

The International Risk Governance Council has developed a framework for analyzing risk management problems. Judgments regarding "simple risk problems" merely require discourse between agency staff and the directly affected groups.[29] Risk problems with major ambiguities, however, like homeland security, "need to be open to public input and new forms of deliberation."[30] Such forms of deliberation require "participative discourse," that is, "a platform where competing arguments, beliefs and values are openly discussed."[31]

This framework demonstrates the inadequacies of the crude scoring system used in the example above comparing the benefits of reinforcing the Lincoln Tunnel against bio-protection suits for first responders in Los Angeles. The problem of resource allocation across threat scenarios and geographic locations is not only an analytic problem, but rather a complex issue of governance that calls for public input, participation of multiple stakeholders, candid open debate, and discussion of tradeoffs. Homeland security is such a new, and, frankly, poorly understood subject, that we are only at the very beginning of developing a process for communicating the concept of risk to the public and infusing the concept of risk into policy decisions.[32] President Bush's statement that "our government will take every possible measure to safeguard our country and our people" established an impossible standard and communicated an unrealistic message to the American people. Former Secretary Chertoff's insistence that the task of the

Figure 1: GAO Risk Management Cycle

government is to "manage" risk, rather than attempt to eliminate it, is a step in the right direction. Yet, efforts to communicate this concept to the public, establish a means of engaging in a national dialogue on the topic, and base policy decisions on the concept of risk management are still in their infancy.

Not only is it important to understand that risk management is a process of governance, but also that risk management is a continuous cycle. The Government Accountability Office has developed a risk management cycle representing the ongoing nature of this process. As the diagram below indicates, the first step is developing strategic goals based on inputs from the intelligence community concerning threats, the existing legal and policy framework, the availability of technology to address the identified risks, and public input.[33] This is followed by a process of assessment, whereby the causes of the risks are identified, possible means for mitigating risk are evaluated, and the cost and benefits of the courses of action are calculated. Policymakers must then select a course of action, which entails assigning responsibilities and providing resources. The policy is then implemented and, importantly, evaluated. These evaluations then inform the revision of the strategic goals, and the process begins anew.

As a participative, continuous process of governance, the application of risk management principles will not provide definitive, static answers to resource allocation issues in homeland security. It will, however, have a number of important benefits:

- Use of risk management will help to educate the public and policy makers about the tradeoffs that are implicit in homeland security policy and budgeting decisions. Risk management that is rigorous and well executed will identify possible costs and benefits of a course of action that may not have been initially apparent to the policy makers and force them to consider the opportunity costs of not pursing alternative solutions.
- Risk management will provide analytic rigor to a process that otherwise seems random and open to political influence.
- A participatory process of developing priorities and making choices will help build long term public support for the homeland security enterprise. This is critically important. In the immediate aftermath of the September 11 attacks, the public was willing to spend taxpayer funds and bear inconveniences to enhance security and preparedness. As time passes and other pressing needs compete for scarce resources, public support may wane. An effective risk management system that explains the security risks in comparison to other risks Americans face and justifies budget expenditures in these terms may build and sustain public support for necessary long term security initiatives.

Strategic Risk Management at the Department of Homeland Security

Despite the theoretical difficulties of applying strategic risk management principles to the topic of homeland security, the imperative remains for DHS to justify its expenditures. Whether the concept is labeled "return on investment" as did one congressional staff member we interviewed, or "prioritizing spending," as called for by the House Appropriations Committee,[34] DHS must demonstrate that the investments being made by the American taxpayer are reducing the risks our nation faces and the funds are being spent according to a rational, defensible plan.

Although risk management is not a silver bullet that can provide answers to all questions, continued long term public support for the concept of homeland security and the viability of DHS depends on its ability to demonstrate a capability to strategically manage risk.

This section describes the efforts DHS has taken to date to develop this capability, assesses their strengths and weaknesses, and proposes steps that should be taken to improve DHS's performance in this regard.

Risk Management at the Tactical, Operational and Strategic Levels

Risk management activities are needed and are taking place at DHS at several levels:

- **Tactical risk management** refers to the process for selecting among alternative courses of action that are permitted within a given policy. An example of tactical risk management at DHS is the Coast Guard's process for determining the place of refuge for a distressed vehicle when it needs to enter a port for repairs.[35]
- **Operational level decisions** require selection among policy options to achieve a stated objective. So, for example, the Transportation Security Administration is using risk management techniques to select among the various options for providing enhanced aviation security.[36]
- **Strategic risk management** is the process through which these decisions are informed by the concept of risk. This paper is focusing on decision making at the strategic level—where the entire agency establishes goals, sets policy to meet those goals, and then allocates resources to implement policy.

Risk Management Through Strategic Planning

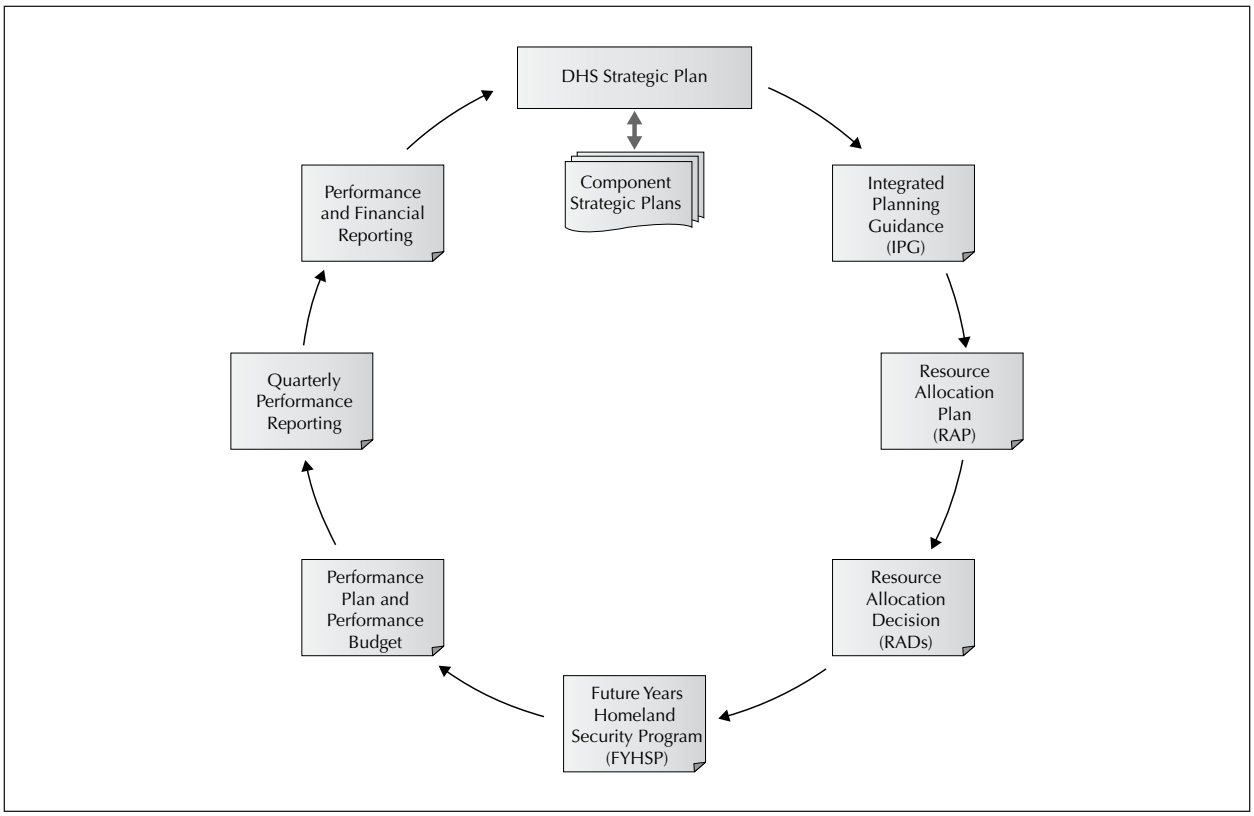
Developing a risk management approach requires the infusion of risk management principles at all levels of DHS's planning process. As Figure 2 on page 20 indicates, the strategic plan ultimately drives the budget process and the allocation of resources to specific programs.

DHS's Strategic Plan for fiscal years 2008-2013 establishes five goals for the agency:

- Protecting the nation from dangerous people
- Protecting the nation from dangerous goods
- Protecting critical infrastructure
- Strengthening preparedness and emergency response capabilities
- Strengthening and unifying DHS operations and management[37]

Within each goal, there is a list of sub-goals and a set of indicators to be used to measure whether the

Figure 2: DHS Strategic Planning



Source: *Department of Homeland Security Strategic Plan, 2008-2013, p. 33.*

goals are being met. Although the strategic plan discusses the importance of risk management, there is little evidence that the goals and objectives set forth in document are the product of a process that considered risk and evaluated tradeoffs. Indeed, these five goals appear to be more of listing of DHS's responsibilities, than a description of how DHS intends to use its resources and authorities to reduce the risks that the country faces. Nor is there any indication in the strategic plan of the priorities that DHS places on the four substantive goals. Is it more important, for example, to prevent dangerous people from entering the country or to protect critical infrastructure? Both goals, of course, are important, but nothing in the Strategic Plan speaks to whether investments in critical infrastructure are more likely to reduce our overall risk than investments in border security. The same lack of prioritization pervades details of the document. For example, within the critical infrastructure goal the plan appears to give equal weight to all infrastructures, and within transportation, to give equal weight to each part of the transportation system.[38]

The failure of the strategic plan to identify priorities or evaluate tradeoffs renders the document practically of limited use as a risk management exercise. The mere listing of DHS's responsibilities is neither a strategy nor a plan. A strategic plan should articulate the risks our nation faces for which DHS is (at least partially) responsible for addressing and demonstrate how DHS will apply resources to reduce these risks to an acceptable level to the extent we are able to do so. While doing so with mathematical precision is impossible for the reasons described in the previous section, at this stage in DHS's development, Congress and the public are entitled to at least a general plan of what risks DHS perceives to be of greatest urgency and how this agency will contribute to our national effort to reduce them.

Strategic Risk Management Through Budgeting

Only recently have efforts been made to apply risk management techniques to the DHS budgeting process. DHS's early budgets were, in essence, a combination of budgets from its legacy components plus

budgets from new components designed to start programs and build capabilities as quickly as possible. There is no evidence that efforts were made in the early days of DHS to systematically assess risks and allocate funds according to a strategic plan to reduce these risks as cost effectively as possible. Of course, this is understandable in light of the way DHS came into being—moving from a presidential proposal to authorizing legislation to swearing in of the first secretary in about seven months. DHS's first budget—for fiscal year 2004—was submitted before employees had even been transferred to the new agency.

It is also important to note that DHS was born into a highly charged political atmosphere. Homeland security had been a divisive issue during the 2002 congressional elections, and the 2004 presidential election was only 18 months away when DHS was formally stood up. There was extreme pressure for programs to be initiated, for security gaps to be being addressed, and for the agency to demonstrate the capability to provide security during a period of perceived high threats. Programs were established, some of them with a substantial cost, without a clear understanding of DHS's strategic goals or how the programs contributed to reducing risk.

Subsequent budget debates demonstrated, however, that there were risks that the DHS budget did not address. The lack of a program to screen air cargo carried on passenger planes and regulations to increase security at chemical plants, for example, became controversial and the subject of congressional debate. Members of Congress defending the administration's budgets were forced to begin speaking in terms of priorities and risk management to explain why DHS did not have a program to cover every conceivable risk to the nation.

Frustration mounted during the annual appropriations process when DHS presented a budget, but did not have a satisfactory explanation for the allocation of spending based on a conception of agency priorities or the goal of reducing risk. In the report on the fiscal year 2007 DHS budget, the House Appropriations Committee chided DHS, stating, "Without a relative risk scale ranking the greatest dangers to society, decision making can become arbitrary and lead to the use of resources for the most frightening threats rather than ones most likely to harm us." The committee complained that the budget "offers no details on how risk assessment was used in its formulation or even which DHS agency was tasked with prioritizing risks and assigning them resources."[39]

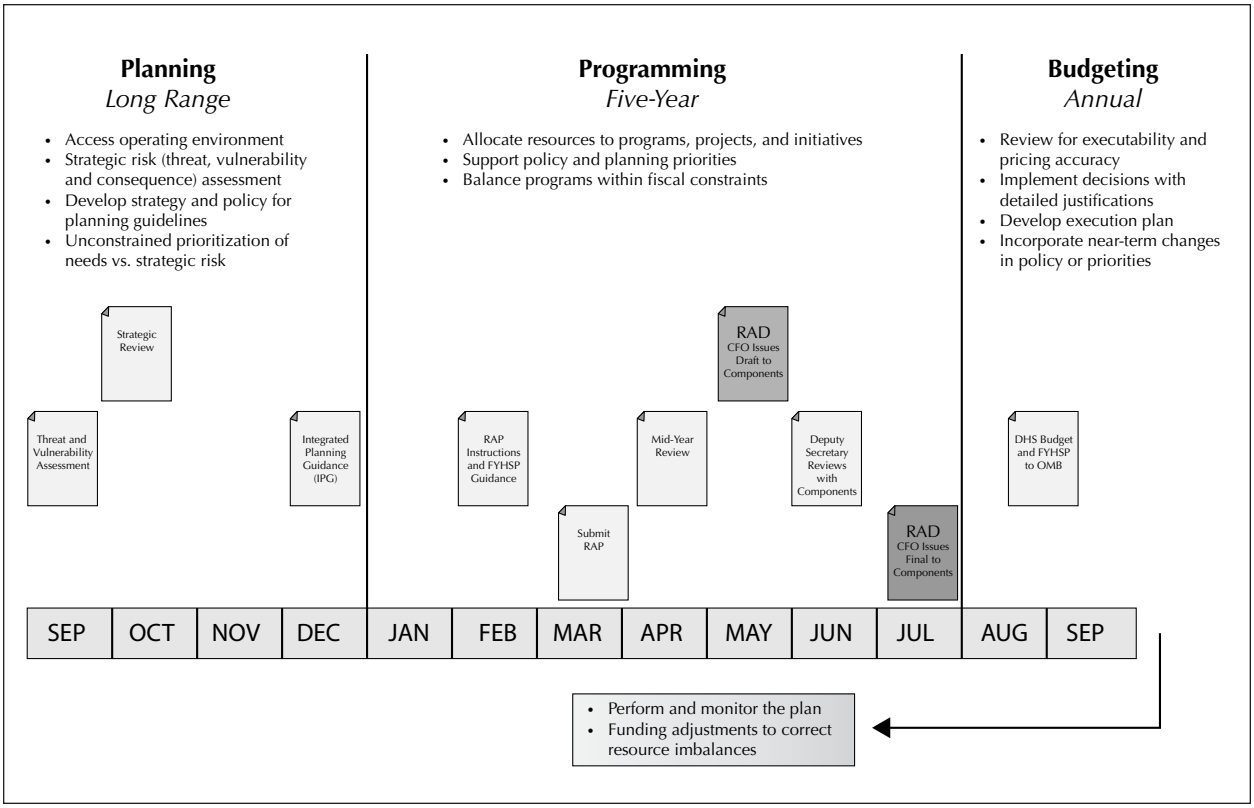
This pressure from Congress and Secretary Chertoff's endorsement of risk management principles led to the beginning of efforts to incorporate risk management into the annual budgeting process. Whereas DHS's early budgets were built principally from the bottom up by the components based on their own risk assessments, DHS has developed a Planning, Program, Budgeting, and Execution (PPBE) process, which, in theory, enables the department leadership to set risk based priorities and impose them on the sub-agencies and components so that the DHS secretary's priorities are ultimately reflected in the budget. (Figure 3).

As Cindy Williams describes in her paper for the IBM Center for The Business of Government, the annual budgeting process is supposed to begin with a threat assessment presented by the DHS Office of Intelligence and Analysis to identify emerging and declining threats.[40] The planning process culminates in the preparation of the Integrated Planning Guidance, a memo from the secretary to DHS's components that discusses strategic goals, describes policy priorities, and provides fiscal guidance.

Our research confirmed Williams' conclusion that the front end of the PPBE process "remains weak."[41] The comprehensive threat assessment was not included as part of the planning process until the 2008 to guide development of the fiscal year 2010 budget. During that budget cycle, cross-component leadership meetings were held to review these threat assessments and establish departmental wide priorities. These priorities were communicated to the components whose budgets are supposed to be responsive to the guidance produced during the cross-component meetings.[42] Guidance from these cross-component meetings, however, was considered to be "one input among many."[43]

In addition to these steps, DHS is developing a decision tool to attempt to inform the DHS resource allocation process—known as Risk Assessment Process for Informed Decision-Making (RAPID). This program is being implemented by the Office of Risk Management and Analysis, created in April 2007 to develop a common framework across DHS to analyze

Figure 3: Planning, Programming, Budgeting, and Execution (PPBE) Overview



Source: *Department of Homeland Security Strategic Plan, 2008-2013, p. 34.*

and manage homeland security risk.[44] This small office, located within the National Protection and Programs Directorate, was initially formed outside of the normal budget cycle with limited resources.

RAPID has identified 85 risk reduction areas (such as screening cargo for nuclear material) and mapped them against the priority goals identified in the DHS strategic plan. DHS's programs were then surveyed to identify the risk reduction areas that each program addressed. This tool is intended to provide a means to identify gaps in programming and allocate resources to programs when new strategic goals are developed or strategic priorities are shifted. It also provides a framework for program managers to justify their budgets in terms of how they contribute towards DHS risk reduction areas and strategic objectives. Although the program has been in development for over two years, it is not currently delivering quantitative results that can be used to influence the strategic planning or budgeting process.

Strategic Risk Management Through Evaluation

One aspect of the risk management process that is given too little attention is program evaluation. There is often an assumption that the development of a new program, a change in policy, or expenditure of funds will reduce risk in the manner intended. One security function that has been rigorously evaluated is the effectiveness of airport screeners, and we have learned, over time, that increased professionalism, training efforts and technological improvements have not reduced the rate of illicit materials entering security efforts to the degree that policymakers expected or desired.[45]

The vast majority of DHS security programs, however, have had no or virtually no rigorous, independent evaluation to determine effectiveness. One DHS official noted that the agency was "at a prototype stage on the way to a pilot stage" for developing measurements of program effectiveness. The RAPID program, for example, uses subject matter experts to opine on program effectiveness because

program evaluations (and even the means to evaluate such programs) are lacking.

The inability of DHS to measure comprehensively the baseline requirements and the effectiveness of its programs is a major hindrance to effective strategic risk management. It is virtually impossible to allocate resources based on reducing potential harms from security risks unless it can be determined that programs in which resources are being invested will actually work. Furthermore, the evaluations must include both the technical and human elements of the programs. The best technology cannot be effective if it cannot be understood, adopted, and implemented by the program staff and the citizens it is designed to protect. So, for example, DHS has expended huge amounts of resources on attempting to detect airborne bioterrorism agents. Program evaluations would test not only the efficacy of the technology, but also consider a number of other questions that bear on the effectiveness of the technology in actually reducing risk, such as whether the number of collection points is sufficient, whether the protocols for analyzing samples gives sufficient early warning to take effective action, whether the technology fits into the existing monitoring and reporting process, and whether risk levels are being properly communicated to the public.

Based on such evaluations as described above, DHS may decide to continue or expand the program, allocate resources to another means of finding an early warning of an airborne bioterrorism attack or shift resources to enhancing response capabilities. Without effective evaluations, however, these strategic decisions cannot be truly "risk informed."

Impact of Congress on DHS's Strategic Risk Management Efforts

Most discussions about DHS's difficulties developing strategic priorities and mapping resources against those priorities focus on deficiencies at the agency itself. It is important to recognize, however, that Congress plays an integral role in shaping the internal operations of DHS, allocating resources, and establishing legal mandates that DHS must meet, regardless of their risk reduction value. To better align DHS's resource allocations with their risk reduction value, therefore, Congress must be a risk manager as well.

Legislative Activities

DHS's inability to tailor its budget allocations to a set of risk based priorities is not caused solely by factors internal to the agency. Legislative mandates—requirements put in place through statute by the Congress—dictate a least a portion of DHS spending. These mandates can be quite expensive, extremely difficult to implement, and come with strict deadlines that may be difficult or even impossible for the agency to meet.

Because these mandates are written into law, DHS must allocate resources toward meeting their goals, regardless of whether DHS believes that these expenditures are reducing the risks our society faces or expenditures on other programs would achieve greater levels of risk reduction. DHS officials and congressional staff interviewed for this study consistently pointed to congressional mandates as a significant obstacle to DHS allocating its resources based on risk.

A recent example of this phenomenon is the mandate enacted in 2007 requiring that by 2012, all foreign cargo containers must be screened for radiation before being shipped to the United States.[46] This provision was enacted as part of legislation to implement the recommendations of the 9/11 Commission, although the 9/11 Commission never made this specific recommendation. No hearings were held on this proposal prior to passage of the bill by the House of Representatives and there were no studies in existence (nor are there to this day) that analyze the cost of meeting this mandate, the expected risk reduction benefits of compliance, and potential alternative policies for achieving these security benefits.[47] By enacting this mandate, Congress directed that significant resources be spent on this single method for increasing cargo security without evidence that this policy would effectively reduce overall risk levels compared to other policies or investments, or, indeed, that the policy would reduce risk at all.

There is no requirement, nor should there be, that Congress may only enact protective legislation if there is proof that the policy will result in overall reduction in societal risk. The legislative process is complex and impacted by many factors –including politics, interest group pressure, public opinion and the interests of individual lawmakers. Homeland

security, however, is an area that is particularly vulnerable to influences that could result in legislative mandates that do not conform to risk management principles. Because this is such a new area, compared to, for example, workplace safety or environmental protection, we do not have the historical references and well developed analytical frameworks to evaluate what policies will most effectively reduce risk.

Heightened public sensitivity to the threat of terrorism, even many years after 9/11, also creates pressure on lawmakers to take action whenever gaps in our homeland security are revealed and publicized in the media. Actions that are easy to explain and have intuitive public appeal—such as screening 100 percent of cargo in foreign ports—carry great appeal to legislators eager to demonstrate they are taking steps to protect their constituents from potential danger even if, in practice, they provide little or no actual risk reduction benefit. Legislation in response to high profile incidents and anecdotes is prevalent in many areas—but homeland security is especially vulnerable to such legislative activity.

Oversight Activities

The controversy over congressional oversight of homeland security began the moment Congress began considering creation of the new department. For as anyone that has studied Congress well understands, congressional jurisdiction is the coin of the realm in Congress because jurisdiction equals power—the power to shape policy, influence personnel decisions, and direct the distribution of resources. Indeed, many strong lawmakers (especially chairmen and ranking members) initially lined up against the creation of DHS because they knew that this governmental reorganization could threaten their jurisdiction over agencies and programs scheduled to be transferred into the new department. In the alternative, they argued that even if DHS came into being, their committees should retain jurisdiction over the parts of DHS that had historically fallen within their domain.

In response to the creation of DHS in 2003, the appropriations committees in both the House and Senate created new subcommittees dedicated exclusively to funding DHS. There was little change, however, in the jurisdiction of the authorizing committees—that is, the committees with authority to establish law and policy. The only significant action was the House's establishment of the Select Committee on Homeland Security, which was given virtually no formal jurisdiction over legislative issues. A white paper issued in 2004 concluded that 86 congressional committees and subcommittees had some responsibility relating to DHS oversight.[48]

The issue of jurisdictional overlap came to prominence in 2004, when the 9/11 Commission included in its recommendations that each body of Congress should create a single authorizing committee to exercise jurisdiction over the Department of Homeland Security. In 2005, at the beginning of the next Congress, the House created a new standing Committee on Homeland Security and provided it with substantial new jurisdiction relating to DHS operations and policy, border and port security, customs, domestic preparedness and response, research and development and transportation security.[49] The Senate gave new authority to a re-named Committee on Homeland Security and Governmental Affairs as well.

These modest reforms, however, failed to divest other committees of their claims to jurisdiction. Thus, while some consolidation did occur, DHS is still required to answer to numerous congressional committees, provide witnesses for frequent congressional hearings, and respond to large volumes of congressional inquiries and requests for information. According to DHS statistics, in 2007-2008, DHS officials provided 4,922 congressional briefings, testified in 377 hearings, and reported to 108 congressional committees and subcommittees.[50]

The state of affairs has led to a virtual cottage industry of task forces and studies calling for further consolidation of jurisdiction.[51] Congress' failure to do so, the analysts claim, requires DHS to be responsive to too many congressional masters and cripples its ability to set priorities and execute a strategic plan based on risk management principles. DHS will not be able to manage risk effectively, they claim, until Congress reorganizes and provides the homeland security committees with the same level of exclusive jurisdiction as the armed services committees enjoy with respect to the Department of Defense.

Overlapping congressional oversight jurisdiction, however, is not the root cause of DHS's failure to articulate its risk management priorities. DHS has a

single source to interact with Congress with respect to its funding priorities—the homeland security subcommittees for the appropriations committees in the House and Senate. If DHS had the ability to allocate its resources based on risk management concepts, it could have done so through the appropriations process. The appropriators, however, have been the most consistent critics of DHS's failure to establish priorities and submit budgets that address those priorities.

DHS's failure to set priorities, develop a meaningful strategic plan, and evaluate the effectiveness of its programs—in short, its own institutional weakness—has resulted in the overbearing congressional oversight that DHS is experiencing. In the absence of a strong institutional identity, members of Congress have moved into the void, asserted their authority, and pulled the agency in multiple directions. Relieving jurisdictional overlap will not cure DHS's difficulties improving strategic risk management. But it is unlikely that a stronger agency will be able to emerge under the current conditions.

The congressional free-for-all that currently exists over DHS needs to be effectively managed to reduce the oversight burden and potential mixed messages that result from duplicative congressional oversight. In the foreseeable future, this will probably not be achieved by streamlining all oversight jurisdiction into one committee, as has been done with the Department of Defense, for several reasons. Primarily, achieving changes to committee jurisdiction is exceptionally difficult. Congress made some modest reforms in 2005 in response to 9/11 and the recommendations of the 9/11 Commission. It would take another crisis to move Congress to take up this topic again.

There is also an argument that such extreme jurisdictional consolidation may not even be desirable. Unlike the concept of national defense, homeland security is an amalgam of different disciplines—law enforcement, public health, emergency management, engineering, intelligence, to name a few—all attempting to coordinate their activities and work as a coherent whole. As such, it may make sense for multiple committees in Congress to have a say in the development of our homeland security policies. In fact, it would make very little sense for homeland security committees to be establishing policies regarding, for example, preparedness for a pandemic flu outbreak, without the input of the health committees, and vice versa. Creating a single committee with exclusive jurisdiction over all homeland security matters may push DHS toward becoming its own isolated domain, which is entirely contrary to the reasons the department was created in the first place.

The challenge will be to develop a jurisdictional and oversight regime that reflects the multi-disciplinary nature of DHS, while controlling the oversight burden and protecting the agency from overbearing congressional activities that divert the agency from its core priorities.

Findings and Recommendations

Improving strategic risk management for homeland security will require coordinated and increased efforts by the White House, DHS, and Congress. The recommendations presented below will not "solve" the problem or resolve the best way to allocate scarce resources to address homeland security threats.

The following set of recommendations are intended, however, to move the government toward organizational structures and a process that infuses the concept of risk into our strategic decisions concerning homeland security and, hopefully, provide the American public with a clearer justification for the expenditure of taxpayer funds for homeland security programs.

To the Executive Office of the President

Finding One: The concept of homeland security has not been clearly defined.
DHS was formed in response to a single incident—the 9/11 attacks—during a time of great national concern about security. Its immediate mission was to close the security gaps that had been exploited by the 9/11 hijackers and address immediate threats to our safety and security. In the almost-eight years since 9/11, and the six years since the creation of DHS, however, no one has clearly defined the concept of homeland security, the long term missions of DHS, or the role of DHS vis-a-vis other agencies with counterterrorism and homeland security responsibilities. This lack of clarity was most recently apparent during the H1N1 flu outbreak, where both the secretary of DHS, as well as leaders from the Department of Health and Human Services, were making public announcements regarding the public health emergency, but it was entirely unclear how responsibilities were being divided and what the specific role the DHS was playing in the crisis. Without a clear sense of mission and purpose, it is impossible to execute a strategic risk management program and drive resource allocations toward risk reduction.

Recommendation One: The president should issue an executive order that defines the homeland security mission and allocates responsibilities across agencies.
As time passes since 9/11, it is time to evaluate what the domestic security needs of the country are and determine which agencies are best equipped to provide these protections. This hard work of defining the mission, assigning lead responsibilities, and deconflicting agency roles must be done by the president through the assistant to the president for homeland security and counterterrorism.

An executive order that defined these roles would be the first step toward setting priorities that could be used to inform a risk management process across all agencies, but especially in DHS. The Bush administration's Homeland Security Presidential Directive 10 on biodefense provides a possible model for how issues can be appropriately divided and leadership roles assigned to various agencies and sub-agencies.

Finding Two: The federal government lacks a cross-department risk reduction strategy.
While DHS plays a lead role in a number of homeland security areas, for example, aviation security, it shares responsibility and plays a subordinate role in many others, for example, food security. While DHS is struggling to create a risk management process to

allocate its resources effectively, the same is true for the government as a whole, especially with respect to homeland security. Not only do agency responsibilities overlap, but at present there is no mechanism to establish government-wide priorities for homeland security and coordinate the allocation of resources across agencies to address these priorities.

Recommendation Two: The president should establish a cabinet-level working group on domestic risk management to coordinate approaches toward risk.
A cross-government strategic approach is necessary so the government as a whole can properly define the scope of homeland security and identify its highest risk management priorities to develop a coherent, explainable approach toward mitigating those risks. A coordinated approach will help reduce redundant efforts and verify that gaps in our security are appropriately filled. Such an approach would allow for resources to be allocated based on global risk assessments that reflect societal needs rather than local assessments that consider only the threats within a particular agency jurisdiction. For example, it does not make sense for DHS to increase its resource allocation to reducing vulnerabilities toward food-borne illnesses if other agencies like the Department of Agriculture and the Food and Drug Administration have reached contrary conclusions and are investing their resources toward other priorities.

Even though DHS's own strategic risk management processes are still developing, creating a cross agency panel to share information, identify best practices, and at least begin the process of coordinating priority identification and resource allocation decisions is necessary. Without a strategic, long-term, cross-governmental approach, our approach toward the long term risks the country faces will continue to be reactive, with funding allocations aimed responding more to the latest crisis or incident, instead of making investments that effectively reduce overall risks over the long term.

Finding Three: Efforts to explain risk management principles to the public have been weak.
Although former Secretary Chertoff often spoke about risk management principles and how they applied to DHS, far more work needs to be done in this area. The nation faces continuous threats from terrorism, natural disasters, and infectious disease. While policymakers generally understand that it is impossible to drive these risks down to zero and prohibitively expensive to bring them even close to zero, public expectations for governmental protection from harm resulting from these threats remains quite high. Presidents and members of Congress are normally in the habit of telling the public what government will do for them, not what its limitations are. Yet, strained budget resources and the limits of policy dictate that many risks cannot be fully addressed. There are many security gaps that terrorists could exploit to attack again, the government will not be able to provide immediate food, shelter and medical assistance to all victims of a natural disaster, and people will get sick and die during an outbreak of infectious disease. These realities have not been explained to the American public.

When the response after Hurricane Katrina was perceived to be inadequate, this led to a severe drop in confidence in DHS and the federal government across the board. The consequences could be even more severe if there is another successful terrorist attack, we experience an even greater natural disaster, or if a pandemic flu like H1N1 hits the country hard.

Recommendation Three: The president should discuss risk priorities with the American people.
Before the country faces another large scale or catastrophic domestic event, the president needs to engage with the public about the government's strategy and resource allocation decisions. The president needs to be candid with the American people about why we need homeland security and what it can reasonably achieve. The H1N1 emergency provides an excellent launching off point for this discussion. Americans need to understand the investments that the government has made, but also the risks that the government has chosen to accept. Facing this hard truth will help to stimulate a public debate on what the "acceptable" level of risk may be to a set of potential threats. This debate can then send signals to policymakers to inform their resource allocation judgments.

A public dialogue should also engage community leaders, experts, and policy makers at the federal, state, and local levels to identify the most pressing risks and develop strategies for mitigating them. These strategies will all involve tradeoffs and sacrifices, but

they are necessary to deal with the risks we face today and prepare the nation for the risks we are likely to face decades from now. A consistent, mature message on this subject will help to build long-term public support for security programs and help to reduce disillusionment with the concept of homeland security resulting either from the sense that resources are being wasted because incidents are not occurring or when serious harm occurs despite our investments.

To the Department of Homeland Security

Finding Four: The budget process provides few opportunities for cross-agency deliberation on priorities.

Efforts to promote cross-agency deliberations over budget priorities are in their infancy at DHS. The Office of Intelligence and Analysis provided a threat briefing to a meeting of all DHS leadership during the development of the fiscal year 2010 budget, which led to some discussion and reallocation of resources. While in theory there should be opportunities for cross-agency assessment of budgeting priorities informed by risk analysis, the institutional arrangements to achieve this objective are weak. Budgeting is still principally a bottom-up process where managers attempt to justify increases from their current budgets instead of demonstrating how their programs effectively reduce risk. This needs to change.

DHS has been developing the RAPID tool to help in comparing the full range of risks DHS has been tasked with addressing, but this tool is still in its early stages of development and has many theoretical obstacles to overcome. Although cross-agency analytic programs like RAPID may eventually provide insight about how to produce a more risk-informed budget, it cannot serve as a substitute for judgment based on deliberation.

Recommendation Four: The secretary should establish a budget process that requires cross-agency deliberation over budget priorities.

The secretary should chair an annual risk management board of DHS leaders that meets for extensive briefings and deliberation to set priorities and discuss cross-agency tradeoffs. These meetings should provide an opportunity for DHS leaders to interact with intelligence analysts, risk management specialists, and program officials to both set risk management goals and ensure that programs are geared toward meeting them. Operational programs that cannot be justified in terms of risk reduction (excluding support functions like training and education) should be critically scrutinized.

Administrative procedures need to be developed through the PPBE process to impose the risk management guidance issued by DHS leadership on the components. One possible mechanism would be to require all budget justification documents submitted to Congress to contain statements explaining how a program contributes toward risk reduction and why it is superior to other possible interventions. We also recommend that budgets be presented to Congress in a format that would demonstrate how resources are being allocated across issue areas based on priorities in addition to the traditional component-by-component, line-by-line presentation.

We recognize that much of the budget is allocated to fixed costs and on-going programs, so that it is unrealistic to expect large re-allocation of funding in response to risk management efforts. Over the long term, however, we believe that incorporating this type of cross-agency deliberations will result in more effective homeland security efforts that increase the value of taxpayer funded security investments.

Finding Five: The DHS strategic planning process does not sufficiently incorporate risk management principles.

The process for developing the DHS Strategic Plan for 2008-2013 was not sufficiently rigorous, resulting in a document that was bland, set no priorities, and failed to weigh and evaluate tradeoffs. This draft was compiled by reviewing DHS component plans and policies and other Executive Branch directives to develop a list of goals. Then working groups of DHS officials reviewed the results to validate the approach. The process did not incorporate intelligence officials, risk management analysts, or program experts.

The first Quadrennial Homeland Security Review (QHSR), required by the 9/11 Implementation Act, provides an opportunity for DHS to engage in risk informed strategic planning.[52] Yet, it appears that

this report is being produced with a skeleton staff that will be disbanded immediately after the report is issued. Only $1.65 million is being allocated for this two year effort, to be supplemented through detailees from within DHS.[53] This level of effort is unlikely to produce a robust review that sets a strategic course for DHS's future.

Recommendation Five: The assistant secretary for policy should use risk management principles to inform strategic planning.
Strategic planning needs to be a far more analytic process. Goals should be developed in reference to the latest intelligence reports and a survey of stakeholder needs. Priorities need to be established through a consultative process with agency components, stakeholders, elected officials within the different levels of government, and representatives of other agencies with homeland security responsibilities. Risk management analysts should participate in the process to help quantify values across threats, to the extent practical, to give the ultimate decision makers at least some basis for making comparative judgments and assessing tradeoffs.

DHS should use the QHSR to establish a risk informed strategy for DHS. This vehicle provides the Obama administration with a platform for developing an approach toward homeland security based on risk, analyze the extent to which resources are aligned against risk informed priorities, locate gaps, and make appropriate resource allocation adjustments.

The QHSR report will represent a unique opportunity for the Obama administration to think strategically about homeland security and take a fresh look at the entire homeland security enterprise without any need to justify decisions of the past. Given the importance of this undertaking, it needs to be properly staffed and resourced. Congress should provide the administration additional time to issue the report if necessary. It would also be wise to build at least a small permanent staff to monitor implementation of the QHSR recommendations and bolster DHS's strategic planning resources.

Finding Six: DHS lacks core analytic capability to execute risk management.
Seven years into its existence, DHS continues to suffer from the circumstances of its creation—principally that it was created without increasing the size of agency staff and without core, central functions to help pull the agency together. The agency's analytic capability is one of the core functions that need to be strengthened. Although DHS draws on outside expertise to support its analytic activities, such as the university centers of excellence and FFRDCs, these resources are no substitute for full time, in-house expertise to conduct the analyses necessary to implement risk management.

Recommendation Six: The under secretary for management, the under secretary for science and technology, and the assistant secretary for policy should propose budgets that build DHS's analytic capabilities for risk management. In addition, the department should clarify the roles and responsibilities between the DHS units which undertake strategic risk management.
Although DHS bolstered its risk analysis capabilities by creating the Office of Risk Management and Analysis (RMA, now located in the National Protection and Programs Directorate), it still lacks the analytic capabilities in key areas necessary to move toward risk informed budgeting. Additional risk management capabilities should be added in the offices responsible for strategic planning (Office of Policy) and budget review (Office of Policy, Analysis and Evaluation in the Directorate for Management). Expertise in risk analytics methodology, especially methodologies related to conducting threat assessments of adaptive adversaries, should also be developed in the Directorate for Science and Technology.

Finding Seven: DHS does not systematically evaluate its programs.
DHS does not have any institutionalized procedures for evaluating the effectiveness of many of its programs. We do believe that many major programs have not been subjected to an independent, rigorous program evaluation. Entities such as the DHS Inspector General and the Government Accountability Office often review DHS programs, conduct audits, and make recommendations for improved performance. But these reviews are sporadic and are often conducted in response to a specific incident or media attention. They cannot substitute for a systematic, institutional mechanism for program evaluation.

Recommendation Seven: The under secretary for management should require that program evaluations be incorporated into all major program budgets.
DHS should rigorously and continuously assess its programs for effectiveness. A set of best practices for needs assessments and program evaluation, including experimental design, as appropriate, should be implemented to accurately determine the requirements and effectiveness of any program from both a technical and human systems perspective.

In fields other than homeland security, Congress has a long tradition of setting aside a percentage of funds for program evaluation. For example, in the fiscal year 2008 consolidated appropriations law, Congress inserted statutory language setting aside millions of dollars for evaluations of programs aimed at preventing drug abuse, violence against women, juvenile crime, teen pregnancy and other social problems.[54] By statutorily requiring that evaluation work be conducted, Congress assures that the government is making investments to learn what works so to better inform policy and budgeting decisions. In the immediate aftermath of 9/11, there was a strong emphasis on getting projects started and immediately addressing vulnerabilities. For the long term, however, it is imperative that at least a modest percentage of program funding be dedicated specifically to independent, rigorous evaluations of DHS programs.

Evaluating programs aimed at preventing low probability, high consequence events such as a large scale terrorist attack or catastrophic earthquake present methodological challenges. Research efforts are needed to develop analytics for assessing such programs.

To the Congress

Finding Eight: Congress has enacted legislation imposing mandates on DHS without evidence that they reduce risk.
DHS must comply with the law by addressing legislative mandates, regardless of whether the mandated programs and activities actually reduce risk. In many instances, Congress has enacted homeland security legislation without analysis or studies demonstrating that the requirements imposed will effectively reduce risk compared to other policy alternatives. The mandate for 100 percent cargo screening at foreign ports is most frequently cited as an example of this phenomenon. Such legislative mandates reduce DHS's flexibility to allocate its resources in response to changing circumstances and may require large investments that provide few security improvements.

Recommendation Eight: Congress should enact legislation requiring risk management impact statements to accompany all homeland security legislation.
Congress has imposed analytic requirements on itself in other areas to ensure that it legislates with at least some understanding of the potential impacts of its actions. For example, the Congressional Budget Act of 1974 requires that congressional committees include in their reports on legislation the impact a bill will have on federal spending levels. The Unfunded Mandates Reform Act requires an analysis of whether proposed legislation imposes mandates on state and local government without providing funding for their implementation. A similar type of requirement is needed on homeland security legislation to provide Congress with information on whether the bill effectively reduces overall risk.

This type of analysis could be conducted by the Congressional Budget Office and should require not only analysis of the direct impact of the proposed new policy, but also comparative analysis of alternative risk reduction measures. The purpose of these studies would not to be to attempt to assign a precise numeric value to specific policies because, for the reasons stated earlier in this paper, such analytic precision is neither possible nor desirable. These studies would, however, provide an objective assessment of whether Congress' view that the measure will provide significant risk reduction benefits is true, identify potential unintended consequences, and evaluate alternative courses of action. Such a requirement would have the added benefit of building the analytic capacity of the Congressional Budget Office to help improve security budgeting practices and legislation over the long term.

Finding Nine: Congress is frustrated that DHS has not articulated a risk-informed set of priorities.
Our research indicated that Congress is frustrated with DHS's inability to articulate its strategic priorities

and present a coherent and well justified spending plan to Congress. The imperative to develop such a justification will only grow as federal budget deficits increase.

Recommendation Nine: The chairmen of the Senate and House Appropriations Committees should convene an annual risk management summit between DHS and key congressional homeland security leaders.
A summit meeting at an appropriate point in the budget cycle between DHS and bipartisan congressional homeland security leaders would serve a number of purposes. First, if the summit took place sufficiently early in the budget process, it would provide a forum for congressional leaders to provide input on what they believe DHS priorities should be and how they would deal with tradeoffs implicit in establishing core priorities. As noted in this paper, strategic risk management is a deliberative process—a regular risk management summit would be part of this deliberative process by involving public representatives in the risk management process.

A second purpose of the summit would be to attempt to identify shared goals for DHS, which, hopefully, would then guide and restrain congressional oversight efforts. Congressional leaders will be less likely to forge their own path, and pull the agency away from its core mission, if it has had the opportunity to work in partnership with DHS to establish its top priorities and risk management strategy.

Finally, a risk management summit properly executed would help to educate congressional leaders on the concept of risk so they can better analyze the efficacy of governmental interventions. A risk management summit would force DHS to demonstrate how each DHS program serves its strategic risk reduction goals, which, in turn, would aid Congress in making funding and policy decisions.

Finding Ten: Duplicative and excessive oversight from congressional committees presents difficulties for DHS.
For the reasons set forth earlier in this paper, we disagree with the claim that overlapping legislative jurisdiction over DHS is inappropriate and harmful to the agency. Nonetheless, oversight activities by dozens of congressional committees and subcommittees places a burden on DHS operations, pulls the agency in multiple directions, and contributes to DHS's inability to set strategic priorities.

Recommendation Ten: The Speaker of the House and Senate Majority Leader should coordinate congressional oversight of DHS.
Congressional leaders in each body of Congress should develop a working group to coordinate oversight activities with respect to DHS. The group should consist of the chairman and ranking members of the key committees that have jurisdiction issues over DHS. This group should meet regularly at both the member and staff level to discuss issues and ensure that different committees are not pulling DHS in conflicting directions. The working group should also plan legislative strategy and resolve jurisdictional conflicts before they adversely affect the legislative process.

Congressional leaders should require the committees to eliminate redundant hearings and streamline congressional requests for information. The Speaker of the House should use the power over referrals of legislation to force these committees to cooperate with each other. The Senate Majority Leader has less power than the Speaker to shape committee activities because aggrieved committee chairs can block legislation on the Senate floor, but nonetheless, a coordinating committee should help to delegate responsibilities among the committees and reduce excessive oversight activities.

Appendix: Methodology

Research for this paper was conducted by an extensive review of the literature on the application of strategic risk management to homeland security, attendance at conferences on this topic, and semi-structured interviews with government officials and policy experts. Strategic risk management in homeland security is an emerging field, so the literature was obtained from sources other than books and scholarly journals.

A key source was the paper of an experts' forum on the topic convened by the Government Accountability Office in 2007. Other sources were government reports, congressional testimony, papers published by think tanks and other research organizations, and presentations delivered at conferences. One author attended two major conferences on the topic, the Second Annual National Conference on Security Analysis and Risk Assessment (May 2008), organized by the Security Analysis and Risk Management Association, and Risk Informed Decision Making for Homeland Security Resource Allocation (April 2009), organized by the Military Operations Research Society. The authors also attended relevant presentations at the DHS University Network Summits in 2008 and 2009.

Original research was conducted through semi-structured interviews with Department of Homeland Security officials, current and former congressional staff, and policy experts. The authors developed a standard questionnaire script for the interviews and a set of lead materials that included informed consent information and a description of the study. The script and the lead materials were reviewed by an outside expert, rehearsed by the authors, refined, and distributed to respondents as part of the recruiting process for the interviews.

In-person, confidential semi-structured interviews were conducted using the script as a guide with five officials at DHS with responsibilities in this area, five congressional staff, and one policy analyst with the Congressional Research Service. Interviews ranged from 45 minutes to 90 minutes. Two informal interviews were held by phone with academic experts in the risk management field. Hand written notes were recorded by the authors and coded to identify common themes and key points. These themes and key points were incorporated into the analysis in the final paper. Drafts of the paper were provided to all interviewees and their comments were incorporated into the final paper.

Endnotes

1. George W. Bush, "Remarks by the President at the Signing of H.R. 5005 the Homeland Security Act of 2002," November 25, 2002, available at http://www.whitehouse.gov/news/releases/2002/11/20021125-6.html.
2. United States Constitution, Preamble.
3. White House, "Providing the Resources to Protect America," October 18, 2004, available at http://www.whitehouse.gov/news/releases/2004/10/20041018-1.html.
4. Department of Homeland Security Appropriations Act, Congressional Record, September 9, 2004, p. S8996-97 (Amendment of Senator Dodd). The Senate failed to waive a point of order under the Budget Act by a 41-53 vote.
5. Department of Homeland Security Risk Steering Committee, "DHS Risk Lexicon," September 2008, p. 24.
6. Tom Ridge, Remarks to the American Society of Newspaper Editors, April 21, 2002, available at http://www.dhs.gov/xnews/speeches/speech_0050.shtm.
7. Remarks by Secretary Michael Chertoff, U.S. Department of Homeland Security, George Washington University Homeland Security Policy Institute, March 16, 2005, available at http://www.dhs.gov/xnews/speeches/speech_0245.shtm.
8. Department of Homeland Security Risk Steering Committee, "DHS Risk Lexicon," September 2008 at 27.
9. Rucker, Terri, "Lawmakers Want Full Assessment of Terrorism Risks," *National Journal's Technology Daily,* Feb. 12, 2004, available at www.govexec.com/story_page_pf.cfm?articleid=27651.
10. Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection, the Electric Grid, Critical Interdependencies, Vulnerabilities and Readiness, Hearing before the Select Committee on Homeland Security, Subcommittee on Cybersecurity, U.S. House of Representatives, September 17, 2003.
11. Rep. David Wu Holds Hearing on the Department of Homeland Security's Research and Development Priorities for Fiscal Year 2008, Mar. 12, 2007, available at http://www.accessmylibrary.com/coms2/summary_0286-29947799_ITM.
12. Goodyear Explosion And Homeland Security Risk Management Framework, Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, United States House of Representatives, June 24, 2008, Statement of Rep. Sheila Jackson-Lee.
13. Ibid., Statement of Robert D. Jamison, Under Secretary, National Protection and Programs Directorate, Department of Homeland Security.
14. Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition (2004), p. 396.
15. Government Accountability Office, Highlights of a GAO Forum: Strengthening the Use of Risk Management Principles in Homeland Security, GAO-08-627SP (April 2008).
16. Homeland Security Advisory Council, Top Ten Challenges for the Next Secretary of Homeland Security, p. 13, (2008) available at http://www.dhs.gov/xlibrary/assets/hsac_dhs_top_10_challenges_report.pdf.
17. Department of Homeland Security Risk Steering Committee, "DHS Risk Lexicon," September 2008 at 24 (extended definition).
18. Id. at 33-34.
19. Id. at 34-35.
20. Id. at 16-17.
21. Henry H. Willis, RAND Corporation, "Risk Informed Resource Allocation at the Department of Homeland Security," Testimony before the House Appropriations Subcommittee on Homeland Security (Feb. 2007), p. 3.
22. Id.
23. Id.
24. Robert G. Ross, Risk and Decision-Making in Homeland Security (2006).
25. Id.
26. Id.
27. Erim Kardes, Randolph Hall, "Survey of Literature on Strategic Decision Making in the Presence of Adversaries," CREATE Report 05-006, (March 15, 2005), available at http://create.usc.edu/research/50765.pdf.

28. Ortwin Renn, "White Paper on Risk Governance: Toward an Integrative Approach," International Risk Governance Council (2005), p. 15-16.

29. Id. at 52.

30. Id.

31. Id.

32. Homeland security is such an undeveloped field that a consensus has not yet developed on how to define the term "homeland security." See Christopher Bellavita, "Changing Homeland Security: What is Homeland Security?." *Homeland Security Affairs,* IV, No. 2 (June 2008), available at http://www.hsaj.org/?article=4.2.1.

33. Government Accountability Office, "Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security," GAO-08-627SP (April 2008), pp. 41.

34. Homeland Security Appropriations Act for Fiscal Year 2007, H. Rep. 109-476, Title IV, pp. 118.

35. Commandant Instruction 16451.9, United States Coast Guard, Department of Homeland Security (July 17, 2007) available at: http://www.uscg.mil/directives/ci/16000-16999/CI_16451_9.PDF; Commander Andrew Tucci, "Place of Refuge: Development and Application of a Risk Informed Process," available at www.nrt.org/production/NRT/RRT3.nsf/Resources/powerpoint3/$File/POR_Presentation_RRT.ppt.

36. Cathleen Berrick, "Testimony before the Subcommittee on Aviation, Commerce and Transportation Committee, House of Representatives: Transportation Security Administration has Strengthened Planning to Guide Investments in Key Aviation Security Programs, But More Work Remains," GAO-08124T (July 824, 2008).

37. U.S. Department of Homeland Security, One Team, One Mission, Security of the Homeland, Strategic Plan, 2008-2013 (Sept. 16, 2008).

38. Id. at p. 15 ("We will improve the resilience and security of the domestic and intermodal transportation sectors including air cargo, passenger aviation, rail, transit, highways, maritime, and pipeline modes.")

39. Homeland Security Appropriations Act for Fiscal Year 2007, H. Rep. 109-476, Title IV, pp. 117-18.

40. Cindy Williams, "Strengthening Homeland Security: Reforming Planning and Resource Allocation," IBM Center for the Business of Government (2008), pp. 16-18.

41. Id. at 20.

42. Field Interviews, July 23, 2008

43. Id.

44. "Improving Use of Risk Informed Decision Making in DHS," U.S. Department of Homeland Security, Report to Congress in Response to House Report 109-476 (March 2007).

45. Gregory D. Kutz, Testimony Before the Committee on Government Oversight and Reform, U.S. House of Representatives, "Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process," GAO 08-48T, Nov. 15, 2007; Thomas Frank, "Most Fake Bombs Missed by Screeners," *USA Today,* Oct. 22, 2007; Matthew L. Wald, "Airport Screening Still Falls Short," *The New York Times,* September 24, 2004.

46. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. Law 110-53, Aug. 3, 2007. §1700.

47. A 2005 study of screening 100 percent of cargo in domestic ports concluded that adopting such a policy was "not viable because of restrictions on land and personnel." Susan E. Martonosi,., David S. Ortiz, Henry H. Willis, "Evaluating the viability of 100 percent container inspection at America's ports," from *The Economic Impacts of Terrorist Attacks* (Harry W. Richardson, Peter Gordon, James E. Moore II, eds.) pp. 218-241 (Edward Elgar Publishing. 2005).

48. "Untangling the Web: Congressional Oversight and the Department of Homeland Security. A White Paper of the CSIS-BENS Task Force on Congressional Oversight of the Department of Homeland Security," December 10, 2004.

49. Rules of the House of Representatives, 109th Congress, Rule X (i).

50. Letter from Hon. Peter T. King to the Hon. Nancy Pelosi, November 12, 2008, available at http://chs-republicans.house.gov/list/press/homeland_rep/rmoversightletter.pdf.

51. "Addressing the 2009 Presidential Transition at the Department of Homeland Security," National Academy of Public Administration (June, 2008); "Homeland Security 3.0," Center for Strategic and International Studies/Heritage Foundation, (September 18, 2008); "Untangling the Web: Congressional Oversight and the Department of Homeland Security," Business Executives for National Security, December, 2004.

52. Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Aug. 3, 2007.

53. U.S. Department of Homeland Security Report to Congress on Quadrennial Homeland Security Review Resource Plan (March 27, 2008), available at http://www.dhs.gov/xlibrary/assets/qhsr-resource-plan.pdf.

54. Consolidated Appropriations Act for Fiscal Year 2008, P.L. 110-61 (Dec. 6, 2007), 112 Stat. 1870 (evaluations of Food Stamp Program); 121 Stat. 1906 (3% of funds for violence against women program may be used for evaluations); 121 Stat. 1912 (10% of funds of juvenile justice funding for evaluation); 121 Stat. 1982 ($250,000 for research on drug control policy); 121 Stat. 2177 ($79 million for drug abuse data collection and evaluation activities); 121 Stat. 2179 ($9 million for child care program evaluations).

References

Legislation

Consolidated Appropriations Act for Fiscal Year 2008, P.L. 110-61 (Dec. 6, 2007).

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53 (Aug. 3, 2007).

Congressional Materials

Amendment of Senator Chris Dodd, Department of Homeland Security Appropriations Act, Congressional Record, September 9, 2004.

Hearing before the Select Committee on Homeland Security, Subcommittee on Cybersecurity, U.S. House of Representatives, "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection, the Electric Grid, Critical Interdependencies, Vulnerabilities and Readiness," September 17, 2003.

Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, United States House of Representatives, "Goodyear Explosion And Homeland Security Risk Management Framework," June 24, 2008 (Statement of Rep. Sheila Jackson-Lee; Statement of Robert D. Jamison).

Hearing Before the Committee on Science And Technology, Subcommittee On Technology And Innovation, U.S. House of Representatives, "The Department Of Homeland Security's Research And Development Budget Priorities For Fiscal Year 2008," March 12, 2007, (Comments of Rep. Wu) available at http://www.accessmylibrary.com/coms2/summary_0286-29947799_ITM.

Homeland Security Appropriations Act for Fiscal Year 2007, H. Rep. 109-476, Title IV.

Jenkins, William O., Testimony before the Subcommittee on Homeland Security, Committee on Appropriations, U.S. House of Representatives, "Homeland Security: Applying Risk Management Principles to Guide Federal Investment," GAO-07-386T, (February 7, 2007).

Katz, Gregory D., Testimony Before the Committee on Government Oversight and Reform, U.S. House of Representatives, "Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process," GAO 08-48T (Nov. 15, 2007).

Letter from Hon. Peter T. King to the Hon. Nancy Pelosi, November 12, 2008, available at http://chs-republicans.house.gov/list/press/homeland_rep/rmo-versightletter.pdf.

Rabin, Norman J., Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, U.S. House of Representatives, "Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security," GAO-08-904T (June 25, 2008).

Rules of the House of Representatives, 109th Congress, Rule X (i).

Willis, Henry H., RAND Corporation, Testimony before the House Appropriations Subcommittee on Homeland Security , U.S. House of Representatives, "Risk Informed Resource Allocation at the Department of Homeland Security," (Feb. 2007).

Willis, Henry H., RAND Corporation, Testimony before the Subcommittee on Oversight and Investigations, Committee on Financial Services and the Committee on Homeland Security, U.S. House of Representatives, "Analyzing Terrorism Risk," (July 25, 2006).

Published Papers

Martonosi, Susan E., Ortiz, David S., Willis, Henry H., "Evaluating the viability of 100 percent container inspection at America's ports," from *The Economic Impacts of Terrorist Attacks,* Richardson, Harry W., Gordon, Peter, Moore, James E., II, eds. (Edward Elgar Publishing, 2005).

Von Wintervelt, Detlof, O'Sullivan, Terrence M., "Should We Protect Commercial Airplanes Against Surface to Air Missile Attacks by Terrorists?," *Decision Analysis,* (June 2006).

Willis, Henry H., LaTourrette, Tom, "Using Probabilistic Terrorism Risk Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative in the Land Environment," *Risk Analysis* (April 2008).

Reports

Center for Strategic and International Studies/ Heritage Foundation, "Homeland Security 3.0" (September 18, 2008).

CSIS-BENS Task Force on Congressional Oversight of the Department of Homeland Security, "Untangling the Web: Congressional Oversight and the Department of Homeland Security," (December 10, 2004).

Department of Homeland Security, "Improving Use of Risk Informed Decision Making in DHS, Report to Congress in Response to House Report 109-476." (March 2007).

Department of Homeland Security, "One Team, One Mission, Security of the Homeland, Strategic Plan, 2008-2013" (Sept. 16, 2008).

Department of Homeland Security, "Report to Congress on Quadrennial Homeland Security Review Resource Plan" (March 27, 2008), available at http://www.dhs.gov/xlibrary/assets/qhsr-resource-plan.pdf.

Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition (2004).

Government Accountability Office, "Highlights of a GAO Forum: Strengthening the Use of Risk Management Principles in Homeland Security" GAO-08-627SP (April 2008).

Homeland Security Advisory Council, "Top Ten Challenges for the Next Secretary of Homeland Security" (2008), p. 13, available at http://www.dhs.gov/xlibrary/assets/hsac_dhs_top_10_challenges_report.pdf.

National Academy of Public Administration, "Addressing the 2009 Presidential Transition at the Department of Homeland Security" (June, 2008).

National Strategy for Homeland Security, October, 2007, available at http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

Renn, Ortwein, "White Paper on Risk Governance: Toward an Integrative Approach," International Risk Governance Council (2005).

Williams, Cindy "Strengthening Homeland Security: Reforming Planning and Resource Allocation" IBM Center for the Business of Government (2008).

Manuscripts

Ross, Robert G., Deputy Director, Office of Comparative Studies, "Risk and Decision-Making in Homeland Security" (2006) (available from author).

Ross, Robert G., "Collaborative Public-Private Risk Assessment in Vessel Traffic Safety: Two Case Studies" (available from author).

Willis, Henry H., "Guiding Resource Allocations Based on Terrorism Risk" Working Paper – WR-371-CTRMP, RAND Center for Terrorism Risk Management Policy (March 2006).

Speeches and Press Releases

Bush, George W. "Remarks by the President at the Signing of H.R. 5005 the Homeland Security Act of 2002" November 25, 2002, available at http://www.whitehouse.gov/news/releases/2002/11/20021125-6.html.

Chertoff, Michael, Remarks at the George Washington University Homeland Security Policy Institute, March 16, 2005, available at http://www.dhs.gov/xnews/speeches/speech_0245.shtm.

White House, "Providing the Resources to Protect America," October 18, 2004, available at http://www.whitehouse.gov/news/releases/2004/10/20041018-1.html.

News Articles

Frank, Thomas, "Most Fake Bombs Missed by Screeners," *USA Today*, Oct. 22, 2007.

Rucker, Terri, "Lawmakers Want Full Assessment of Terrorism Risks," *National Journal's Technology Daily*, Feb. 12, 2004, available at www.govexec.com/story_page_pf.cfm?articleid=27651.

Wald, Matthew L., "Airport Screening Still Falls Short," *The New York Times*, September 24, 2004.

Presentations

Breor, Scott, Deputy Director, Office of Risk Management and Analysis, "Risk Management at DHS," Risk Symposium 2008, (March 11-13, 2008).

Gabbrielli, Tina, Director, Office of Risk Management and Analysis, "Growing Maturity in DHS Risk Management," 2007 Annual Meeting of the Society for Risk Analysis, (December 10, 2007).

Ross, Robert G., "Risk & Homeland Security Decisionmaking: What Do Decision-Makers Need? What Can Risk Analysis Provide?," DHS 2008 University Centers of Excellence Summit (March 20, 2008).

ABOUT THE AUTHORS

David H. Schanzer is an Associate Professor of the Practice at the Sanford School of Public Policy at Duke University and co-director of the Institute for Homeland Security Solutions, a research consortium between Duke, UNC Chapel Hill, and RTI International, focusing on applied social science research in support of the national homeland security mission. He also is an Adjunct Professor of Public Policy at the University of North Carolina. He teaches and writes about counterterrorism strategy, counterterrorism law and policy, and homeland security.

Prior to his academic appointments, Schanzer was the Democratic staff director for the Committee on Homeland Security of the United States House of Representatives from 2003-2005. He also served as the legislative director for Senator Jean Carnahan (2001-2002), counsel to Senator Joseph R. Biden, Jr. (1996-1998) on the staff of the Senate Judiciary Committee, and counsel to Senator William S. Cohen (1994-1996) on the staff of the Senate Governmental Affairs Committee. His positions in the Executive Branch include special counsel, Office of General Counsel, Department of Defense (1998-2001) and trial attorney, United States Department of Justice (1992-94). Schanzer was a law clerk for United States District Judge Norma L. Shapiro (1990-91) and for the Office of the Solicitor General of the United States (1989-1990).

Schanzer is a graduate of Harvard College (BA 1985 cum laude in Government) and Harvard Law School (JD 1989), where he served as an editor of the Harvard Law Review. Schanzer is the author of numerous articles on a range of national security topics and has appeared on national and local radio and television discussing terrorism and homeland security.

Joe Eyerman is the co-director of the Institute for Homeland Security Solutions (IHSS) and the director of RTI's Health Security Program. Dr. Eyerman has more than 17 years of professional experience statistically modeling social behavior and managing data for the analysis of political behavior and conflict. His substantive interest is in the modeling of decision processes related to political behavior, group decision making, multi-agency coordination, and political conflict. His recent methodological work has focused on the relationship between the data collection process and error in population estimates on a variety of bioterrorism, public health, and surveillance studies.

Dr. Eyerman is an adjunct assistant professor at North Carolina State University, where he teaches courses on political violence, terrorism, and applied statistics. Dr. Eyerman holds a PhD in political science from Florida State University and a Masters in International Relations from Miami University.

KEY CONTACT INFORMATION

To contact the authors:

David Schanzer
Sanford School of Public Policy
P.O. Box 90316
Duke University
Durham, NC 27708
(919) 613-9279

e-mail: schanzer@duke.edu

Joe Eyerman
RTI International
3040 Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709-2194
(919) 541-7139

e-mail: eyerman@rti.org

Applying Strategic Risk Management to Allocating Resources for Homeland Security: A Case Example of Port Security

Veronique de Rugy
Senior Research Fellow
Mercatus Center
George Mason University

Introduction

The Need for Increased Use of Strategic Risk Management

International terrorism is often described as the greatest security challenge America faces today. After the attacks on the United States on September 11, 2001, policy makers responded in two ways:

- Going after terrorists abroad
- Improving security against terrorism at home by boosting homeland security funding. Congress and the administration moved to create a Department of Homeland Security and increased total funding for homeland security activities by 2,589 percent between FY2002 and FY2009, from $19.5 billion to $70 billion.[1]

On the issue of homeland security, a key question is whether America is getting the maximum level of benefit in exchange for this increase in spending. This means that homeland security should be about wise choices, not just increased spending. It means that the absolute amount of money spent on homeland security should not be the major criteria on which to evaluate homeland security. Rather, the process that leads to the decision to spend the money should be its focus.

Another name for this process is strategic risk management. Strategic risk management is about assessing odds. It is figuring out which threats are most worth worrying about and spending money on and which threats are better left ignored or given fewer resources. Strategic risk management is about devoting more resources against the threat of the most serious attacks—defined as being very likely or if successful, having devastating effects—and spending less on threats which are have potentially smaller consequence. It is taking a finite security budget and making the best use of it.

A recurring recommendation from the Government Accountability Office (GAO) over the years has been the need to use risk management as an important element in developing a national strategy to fight terrorism and allocate counter terrorism resources.[2]

As explained by David Schanzer and Joe Eyerman in Part I of this report, "Not only is it important to understand that risk management is process of governance, but also that risk management is a continuous cycle." It an ongoing process that follows steps and reassesses itself along the way. Understanding this process will lead to strategic spending, which in turns leads to better security at lower costs for taxpayers.

As the paper will discuss, considering the scope of maritime opportunities for terrorists and the nature of the risks related to ports, strategic spending is clearly needed in the area of maritime security.

Port Security in the United States

The U.S. maritime system includes more than 360 sea and river ports with more than 3,700 cargo and passenger terminals and more than 1,000 harbor channels along thousands of miles of coastline.[3] Maritime shippers have increasingly concentrated their traffic through major cargo hubs (megaports) because of their superior infrastructure.

Approximately 85 percent of all cargo tonnage exchanged in the United States passes though just 50 seaports scattered throughout the country.[4]

Maritime commerce is essential to America's economic vitality. Maritime commerce is the primary mode of transportation for trade goods and is essential to America's economic vitality.[5] Every year approximately nine million cargo containers from all over the world —26,000 a day—arrive at U.S ports.[6] Ships carry more than 95 percent of the nation's non-North American trade by weight, 75 percent by value, and 100 percent of the oil imported by the United States.[7] In 2003, waterborne trade contributed about 7.5 percent of the U.S. gross domestic product.[8] Given the importance of maritime trade to the U.S. economy, disruption of that trade would have immediate and significant economic consequences in the United States and also worldwide.[9]

This tremendous flow of goods creates many kinds of vulnerabilities. Drugs and illegal aliens are routinely smuggled into this country, not only in small boats but also in otherwise legitimate cargoes on large commercial ships.[10] More worrisome, terrorist organizations could exploit these same pathways to smuggle dangerous materials—nuclear weapons for instance—for use in an American city.

The variety and number of U.S. ports makes protecting them even more difficult. Some are multi-billion dollar enterprises while others have very limited facilities and very little traffic. Cargo operations are similarly varied, including containers, liquid bulk (such as petroleum), dry bulk (such as grain), and iron ore or steel.

However, there is one relatively consistent characteristic that makes ports an attractive target for terrorists: most seaports are located in or near major metropolitan areas, where attacks or incidents make more people vulnerable.

Port security is a complex issue that involves numerous key actors:

- The federal government, which has jurisdiction over harbors, interstate and foreign commerce, and state and local governments are the main port regulators
- Port authorities, generally self-financed governmental or quasi-governmental public authorities in charge of creating and supporting economic development within ports
- Private sector businesses
- Organized labor and other port employees

As noted, a key actor is the federal government. The routine border control activities of certain federal agencies, most notably the United States Coast Guard (USCG), United States Customs and Border Protection (CBP), and United States Immigration and Customs Enforcement (ICE) seek to ensure that the flow of cargo, vessels, and persons through seaports complies with all applicable U.S. criminal and civil laws. Also, the USCG, the Federal Bureau of Investigation (FBI), the Transportation Security Administration (TSA), and the Department of Defense (DOD) seek to safeguard critical seaport infrastructure from major terrorist attack.

Rethinking Threat Analysis: Using Risk Analysis Instead of Sector Analysis

Central to strategic risk management is the requirement that policymakers think in terms of the risks to be addressed rather than locations to be protected. In the case of ports, strategic port security requires that policymakers think not of the ports themselves, but of what risks are related to ports.

However, policymakers' current approach to homeland security in general and port security in particular is very localized and discretionary as opposed to strategic and holistic. Policy-makings now allocate security resources between critical security sectors, instead of allocating them to address overall risks.[11] At the national level, for instance, Congress allocates resources for port security, airline security, emergency preparedness, or transportation rather than allocating money to address different risks such as nuclear, bio-terrorism, and so on. Within a given sector, Congress does not now allocate resources based on the risk as it relates to specific sectors, but allocates resources to specific security tasks such as detection, prevention or protection.

As a consequence, rather than designing a strategic solution to a given risk, policymakers ignore the holistic and interconnected nature of such risks and focus instead on a few particulars. For instance, instead of thinking strategically about the best way to prevent terrorists from smuggling a nuclear attack

through one of our ports, a solution that might involve focusing most of our efforts beyond the borders of our ports, policymakers think about what's the best way to engage in perfect detection in a port. Thus, port security resources often spend a great deal of money to address one part of the risk it faces. As a result, we have developed a security system that may now overinvest on low priority threats and underinvest in high priority threats.

A strategic risk management approach to homeland security would:

- First, identify risks that a sector faces
- Second, for each risk, identify the most cost effective solutions to address it
- Third, assess who are the best players or agencies (federal (i.e, DOD, DHS, or DOT), state or local government) to put these solutions in place
- Fourth, allocate scarce resources based on the priority and severity of the threat to agencies that would then implement appropriate security measures

Purpose of this Paper

The goal of this paper is to provide a case example of how strategic risk management can be used to allocate resources across the federal government, including the Department of Homeland Security. Port security has been selected as a case example in strategic risk management to demonstrate how the government might use risk analysis in allocating resources to protect the nation.

Preparing a Risk Analysis: Assessing Current Spending

A key step is examining how the government currently allocates port threat related resources. Most of this spending now goes through the U.S. Coast Guard and U.S. Customs and Border Protection, the federal agencies with the greatest involvement in seaports, but other agencies, such as the Department of Defense and the Department of Energy, also receive funds.[12]

Current Programs and Spending

Nuclear Threat Reduction Programs: $1.9 billion (FY2009)

The U.S. government does try to secure weapons and highly dangerous materials scattered abroad. Most of these materials are located mainly in Russia and other countries of the former Soviet Union. The government's main instrument in this area is the Cooperative Threat Reduction Program—usually referred to as "Nunn-Lugar" after the senators who sponsored the legislation in 1991—but the United States also has dozens of separate programs, in several cabinet departments, that are directed toward keeping nuclear weapons and weapon-usable nuclear materials out of terrorists' hands. Activities in these programs include:

- Securing and accounting for vulnerable nuclear material
- Helping states intercept nuclear smugglers at their borders
- Getting rid of vulnerable caches of bomb material

Table 1 shows funding for nonproliferation and nuclear threat reduction programs in FY2008 and FY2009.

In FY2009, the Department of Defense (DOD), the Department of Energy (DOE) and the State Department is spending $1.874 billion between them to secure and dismantle weapons of mass destruction (WMD) and related materials worldwide.[13] Specific programs include:

DOD's Cooperative Threat Reduction program (CTR) enables the removal of shipment of nuclear warheads from former Soviet republics to Russia—as

Table 1: Change in Nuclear Threat Reduction Funding between FY2008 and F2009 ($Million)

Department	FY2008 Appropriation	FY2009 Requested	$ Change 2008–2009	% Change 2008–2009
Department of Defense	$428	$414	-$14	-3.3%
Department of Energy	$1,660	$1,250	-$410	-24.7%
Department of State	$237	$210	-$27	-11.3%
Department of Homeland Security	$0	$0	$0	0
Total	$2,325	$1,874	-$451	-19.4%

Source: *The Institute for Policy Studies (2008) A Unified Security Budget for the United States FY2009, September.*

well as the safe and secure storage of nuclear weapons and the dismantlement and destruction of nuclear silos. In FY2009, CTR will receive $414 million, a 3.3 percent decrease from the $428 million appropriated in FY2008.[14]

DOE's National Nuclear Security Administration's (NNSA) budget includes $1.25 billion for threat reduction activities in Russia and states of the former Soviet Union, a 24 percent decrease in funding over the previous budget. The request for the Global Nuclear Threat Reduction Initiative (GTRI), an important program that secures and reduces the use of vulnerable fissile material around the world, was $220 million. And the International Nuclear Materials Protection and Cooperation program, a program to convert research reactors and security fissile material in Russia, will receive $430 million. These two programs are crucial since terrorists cannot make a nuclear bomb without fissile material.

The Department of State will spend $210 million on its nonproliferation programs, including funding for the Nonproliferation of WMD Expertise program and the Nonproliferation and Disarmament Fund (NDF).

However, according to the authors of *A Unified Security Budget for the United States FY2009*, the $1.9 billion figure spent on nonproliferation efforts might be misleading since part of this funding will go to programs that directly undermine or complicate nuclear nonproliferation efforts. For instance, in FY2009, out of that $1.9 billion, $550 million is used for efforts to research and develop new nuclear weapon warheads, to manufacture and certify new cores for nuclear weapons, and to resume the reprocessing of nuclear spent fuel.[15] This means that roughly $1.35 billion is left for true nonproliferation efforts, out of which only $650 million goes to protection of fissile material stockpiles overseas.

Container Security Programs: $1.35 billion (FY2009)

Table 2 shows funding for container security funding in FY2008 and FY 2009. Over 80 percent of container security funding is spent by the Department of Homeland Security.

The Department of Homeland Security has put in place a series of counterterrorism measures aimed at protecting the United States from the smuggling of dangerous material into the United States. These measures mainly involve securing cargo containers.

On the front line of that effort is the Domestic Nuclear Detection Office (DNDO) within DHS. It was developed to provide a one-stop accountable organization responsible for developing, acquiring and supporting the deployment of the domestic detection system. The mission of the office addresses a broad spectrum of radiological and nuclear protective measures, but is focused directly on nuclear detection at home.[16] DNDO will receive $553.8 million in FY2009.[17]

DHS also focuses some of its nuclear detection and containment efforts at foreign ports through three additional container security programs:

- **The Container Security Initiative (CSI),** administered by U.S. Bureau of Customs and Border Protection (CBP), addresses the threats posed to the United States and global trade by terrorists using a maritime container to deliver a WMD into the United States. CSI targets high-risk containers at overseas ports prior to their departure

Table 2: Change in Container Security Funding between FY2008 and F2009 ($million)

Department	FY2008 Appropriation	FY2009 Requested	$ Change 2008–2009	% Change 2008–2009
Department of Homeland Security	$1,118	$1,132	$14	1.2%
Department of Energy	$64	$67	$3	5.2%
Department of Defense	$73	$151	$78	107.0%
Total	$1,255	$1,350	$95	7.6%

Note: *Programs under the Department of Homeland Security include NDO, CSI, C-TPAT, ACE and RPMs*

for U.S. ports. It deploys teams of inspectors, special agents, and intelligence analysts to foreign "megaports" and other strategic ports to inspect containerized cargo for weapons of mass destruction before the cargo is ever shipped to the United States. Customs officers in 58 ports overseas monitor containers as they are being loaded.[18] In FY2009, CSI budget will be $149.4 million, a 4 percent decrease over FY2008.[19]

- **The Customs-Trade Partnership Against Terrorism (C-TPAT)** program is the second program DHS and CBP put in place to improve cargo security while facilitating commerce. This program partners with foreign manufacturers and importers. These partners—over 7,800 to date—agree to meet "supply chain" standards for establishing a secure chain of custody for every unit of cargo traded overseas. This practice should make it difficult for potential terrorists to use those shipments for introducing weapons of mass destruction into our ports. C-TPAT will receive $64.4 million in FY2009.[20]
- **The Automated Commercial Environment (ACE)** is the third program at DHS that involves container security. ACE provides tools and enhances business processes by providing intelligence required to target illicit goods, while ensuring the efficient processing of legitimate goods. ACE capabilities have been designed to identify potential risks, analyze information prior to arrival of people and cargo, and provide intelligence in easy-to-use formats. As a web-based system, ACE will provide users from government and the trade community with new, more efficient ways of accessing, processing, and sharing trade-related information. This program will receive roughly $300 million in FY2009.

While these are the formal programs within DHS, a large part of detection efforts rely on the deployment of direct detection systems designed to detect radioactive material within containers in local ports. So far, DHS, through the CBP and the USCG, has spent several hundreds million dollars to install over 1,000 radiation portal monitors (RPMs) at U.S. points of entry.[21] The FY2009 budget requested another $64 million to purchase additional RPMs.[22]

In addition, the U.S. Department of Energy (DOE) and Department of Defense (DOD) have developed their own programs aimed at securing containers and vessels from nuclear smuggling. The DOE has been funding and deploying radiation sensors in many of the world's largest ports through a program called the Megaport Initiative. At the end of 2007, the Megaport Initiative was operational in 12 countries and being implemented at 17 additional ports. The DOD has a counterproliferation initiative that obtains permission from seafaring countries to allow specially trained U.S Navy boarding teams to conduct inspections of a flag vessel on the seas when there is intelligence that suggests that nuclear material or a weapon may be part of the ship's cargo. In FY2009, these initiatives combined will receive over $200 million. [23]

There is also the Secure Freight Initiative (SFI). This is a pilot program, within CBP, working in collaboration with the DOE's Megaport program, designed to test high-volume scanning at six ports in Pakistan, Honduras, Britain, Oman, Singapore and South Korea. Containers arriving at participating ports are scanned with both non-intrusive radiographic imaging and passive radiation detection equipment placed at terminal arrival gates to screen incoming containers. Relay containers—those being transferred from ship-to-ship—would also be scanned. Sensor and image data concerning U.S.-bound containers will be transmitted in near-real-time to the National Targeting Center where it will be combined with other available risk data to improve risk scoring and targeting of high-risk containers. In theory, this initiative will enhance the opportunity to conduct further scrutiny of suspect cargo while still overseas.

Altogether, in FY2009 spending on container security measures will total $1.35 billion.

Direct Threat to U.S. Ports: $ 1.78 billion (FY2009)

Table 3 shows funding for direct protection and detection funding in FY2008 and FY2009. Funding in these areas is spent by the Department of Homeland Security, specifically the United States Coast Guard and the Office of Domestic Preparedness.

The United States Coast Guard and the Department of Homeland Security's Port Security Grant Program (PSGP) are the two main programs tasked with preventing direct threats to U.S. ports.

The Coast Guard performs the largest part of the direct protection of U.S. ports through its ports, waterways and coastal security program (PWCS). PWCS mission has three strategic objectives:

- Prevent terrorist attacks, sabotage, espionage, and subversive acts
- Protect the U.S. Maritime Domain and U.S. Marine Transportation System (MTS)
- Respond to and recover from those terrorist attacks, sabotage, espionage, or subversive acts that do occur

In FY2009, $2.59 billion will be allocated to this program out of the Coast Guard's $9.3 billion budget.[24] According to the Coast Guard, $1.4 billion is directly directed to domestic protection and detection. That is roughly the same amount as in FY2008.

The Port Security Grant Program (PSGP) has a more narrow focus. It concentrates on funding security upgrades— such as new patrol boats, surveillance equipment at roads and bridges, and new command and control facilities—in the hope of mitigating direct attacks on ports.

In 2002, Congress provided the first wave of funding to the Transportation Security Administration (TSA), then part of the Department of Transportation, to enhance the security of ports and other facilities. TSA, along with the Maritime Administration (MARAD) and the U.S. Coast Guard, developed the PSGP, which it continued once it became part of the Department of Homeland Security. In May 2004, the PSGP was transferred to the Office of Domestic Preparedness (ODP) within DHS.

PSGP awards grants to state and local governments and private companies. Eligible applicants in each port area may submit one application for funding, and PSGP selects recipients through a competitive process in which a field review panel and a national review panel evaluates each applicant that meets the requirements of the PSGP guidelines.

In FY2002, the TSA received a total budget of $1.24 billion, of which $92 million was dedicated to the new Port Security Grant Program.[25] In FY2008, the PSGP received $388 million, and will receive another $388 million in FY2009.

A total of nearly $1.8 billion was allocated to port security grants between FY2002 and FY2009.[26] PSGP represents a small portion of port security funding and an even smaller portion of homeland security spending governmentwide, yet it receives a lot of attention from members of Congress.

Table 3: Change in Direct Protection and Detection Funding between FY2008 and F2009 ($million)

Program	FY2008 Appropriation	FY2009 Requested	$ Change 2008–2009	% Change 2008–2009
United States Coast Guard	$1,400	$1,400	$0	0.0%
DHS Port Security Grant Program (PSGP)	$388	$388	$0	0.0%
Total	$1,788	$1,788	$0	0.0%

Source: *Department of Homeland Security Budget In Brief FY2008 and FY2009 and PSGP (http://www.fema.gov/government/grant/psgp/index.shtm)*

Scenario Planning in Strategic Risk Management

We have identified two main risks related to ports:

- A direct attack on a U.S. seaport
- The exploitation of our ports by terrorists to smuggle weapons of mass destruction into the country for use in an American city

Based on these threats, we can say that port security measures should prevent the exploitation or disruption of maritime trade and the underlying infrastructure and processes that support it. Scenario planning allows one to rank threats based on their potential costs.

Developing Scenarios

Scenario One: Nuclear Attack

If terrorists successfully introduced a weapon of mass destruction into the country through one of our ports they could cause damage and disruption costing a minimum of $1 trillion. According to the Council of Foreign Relations (CFR), the blast from a one-kiloton nuclear weapon—such as a crude improvised weapon or a stolen battlefield weapon—in midtown Manhattan during the day would kill more than 200,000 people and injure at least 200,000 more. It would also produce radioactive fallout that could kill half the exposed population as far as three miles away within a few weeks. And it would destroy most buildings and other structures over 11 city blocks as well as seriously disrupt Manhattan's transportation, communications, utilities, and other infrastructure.[27]

Based on the CFR's assumptions, Table 4 shows an imperfect estimate of the direct cost of a successful terrorist attack using a one-kiloton nuclear weapon in selected U.S. cities: lower Manhattan, downtown Chicago, downtown Washington, DC, and downtown Los Angeles. To put this blast yield in perspective, a one-kiloton device has less then 10 percent the yield of the 1945 era "Little Man" weapon used in the bombing of Hiroshima. Based on population density numbers from 2000, such a device would destroy 11 city blocks and kill 200,000 people in Manhattan, 38,160 in Chicago, 27,880 in Washington D.C., and 23,570 in Los Angeles.[28]

According to Aldy and Viscusi (2003), the value of statistical life for 30- to 40-year olds is at least $5 million in 1996 dollars.[29] Using this estimate, the value of life is $5.766 million in 2004 dollars. I therefore estimate the cost of 200,000 lives lost to be $1.1 trillion, the cost of 38,160 to be $217 billion, the cost of 27,880 to be $158 billion, and the cost of 23,570 to be $134 billion.

Estimating the cost associated with the destruction of 11 city blocks in each of the selected cities is also possible. Assuming that the length of 11 blocks equals 1 mile, then an 11 block area is about 0.1 square mile. Most of the buildings destroyed downtown in big cities would likely be office buildings. After September 11, most experts used the New York City comptroller's construction costs estimate to measure the cost of a terrorist attack leading to building destruction. This construction cost is roughly $500 per square feet,[30] which means that the construction cost for 11 city blocks would be $765 million in New York, $26.1 million in Chicago, $91.6 million in Washington, DC, and $18.1 million in Los Angeles.

Thus, a crude estimate of the direct cost of immediate deaths and destruction of 11 city blocks due to the use of a one-kiloton nuclear weapon would be $1.1 trillion in New York City, $217 billion in Chicago, $158 billion in Washington, DC, and $134 billion in Los Angeles.

Of course, though the order of magnitude is correct, this number is a gross underestimate of the total cost as it does not consider indirect costs from cleanup, economic disruption, and injuries after the explosion or treatment for the serious diseases that the people exposed to radiation during the attack would develop eventually. [31] These costs would be huge.

Moreover, according to Nuclear Threat Initiative experts, the costs related to the disruption of economic activities, such as the loss of economic output in the city attacked, would likely total several times the direct cost amount.[32] The New York City comptroller estimated that the weekly output of lower Manhattan was $2.1 billion per week and that of the rest of the city was $6.3 billion per week.[33] In the wake of the envisioned blast, a conservative estimate claims that the output of lower Manhattan would be reduced to zero for two weeks and permanently reduced by one third.[34] That means a loss of over $50 billion per year.

To these figures must be added the immense cost of cleaning up the contamination from the radioactive fallout, which would run into the tens of billions of dollars. In short, in order to encompass the total costs of such an attack, several hundred billion dollars would have to be added to the direct costs given in Table 4.

Scenario Two: Dirty Bomb Attack

Another potential scenario is the detonation of a dirty bomb in a U.S. city. According to the Central Intelligence Agency (CIA), the Al Qaeda terror network is fully capable of building a radioactive "dirty bomb" that it could use to target the United States and other Western nations and "has crude procedures" for producing chemical weapons.[35]

Fortunately, even though the probability of a dirty bomb is much higher than the probability of a nuclear attack, such a weapon is a far cry from an actual nuclear explosive since few, if any, casualties would immediately result from radiation exposure.[36] Yet, a dirty bomb device detonating in New York City would still result in large costs.

The biggest cost of a dirty bomb attack would be the required cleanup. In addition to the damage its explosion would cause, a dirty bomb would spread radioactive materials in the air. The only effective way to clean up radioactive buildings is to tear down them down and rebuild them. While we do not have good numbers of what that cost might be, Zimmerman and Loeb estimate that the consequences of a dirty bomb attack on lower Manhattan might exceed the costs to restore New York City after the September 11 attacks. [37] However, they guess that it wouldn't be tremendously bigger.

The New York City comptroller estimated the economic cost of 9/11 at roughly $94.8 billion.[38] In other words, even the least devastating WMD attack in New York City using a dirty bomb would end up costing at least $95 billion in damage.

Table 4: Estimated Cost of the Blast from a One-Kiloton Nuclear Weapon in Selected U.S. Cities

City	Total ($million)
Lower Manhattan	$1,153,766
Downtown Chicago	$217,026
Downtown Washington, DC	$158,092
Downtown Los Angeles	$134,019

Note 1: *These costs do not include the lost of economic output or the cost of cleaning up the contamination from the radioactive fallout. These costs would add at least several hundred billions to the total.*

Note 2: *These numbers are low estimates but correct as to order of magnitude.*

Scenario Three: Direct Attack on a U.S. Seaport

Finally, terrorists could also attack U.S. seaports directly. Such an attack would result in loss of lives, property, and business; affect the operations of harbors and the transportation infrastructure (bridges, railroads, and highways) within and beyond the port limits; and disrupt the free flow of trade.

For instance, imagine the consequences of a successful attack on twin ports of Los Angeles and Long Beach. These two ports handle 43 percent of the total container traffic flowing in and out of the United States.[39] If a terrorist attack shut down that traffic, it would have an immediate spillover effect, causing gridlock in Hong Kong, Singapore, Rotterdam, and every other major trading port reliant on the world's biggest economy. Key U.S. imports, starting with oil, would become scarce almost immediately. Factories would become idle for lack of raw materials or spare parts. Places like Hawaii, which depend on shipping for almost every consumer need, would quickly run out of food.

Of course, attacks on megaports like Los Angeles and Long Beach would have disproportionately larger consequences than attacks on smaller ports. According to data from the American Association of Port Authorities, the total trade disruption cost of a daily shutdown of the twin California ports would be $600 million.[40] The daily cost of the total shutdown of the megaport of New York/New Jersey would be $277 million, [41] but the daily cost of the total shutdown of a small port like Richmond, Virginia, would be $3 million.[42] The final cost to the country would be much larger because neither of these numbers ($600 million and $277 million) takes into consideration the cost to the economy as a whole that such attacks would have. The megaport of New Orleans, for instance, yields roughly 20 percent of the annual U.S. GDP. Its devastation and shutdown following Hurricane Katrina at the end of August 2005 produced a large loss for our economy.

Scenario Summary

Table 5 recapitulates the estimated cost of three different terrorist attack scenarios on New York City and its port.[43] In order to allow us to compare scenarios, the impact on New York City only is presented in Table 5. Although imperfect, these estimates give an idea of the consequences of the three types of attacks on New York City.

Based on Table 5, we see that the smuggling of dangerous materials through ports for use elsewhere in the country or in the ports themselves is likely to be orders of magnitude more severe than the damage caused by a direct, but conventional, attack on a port. Perhaps this is why WMD attacks figured in two-thirds of the 15 disaster scenarios the Department of Homeland Security uses to measure the country's level of preparedness. Also, we see that a nuclear attack would have more dramatic consequences than a dirty bomb.

However, risk assessment consists not only in evaluating the cost of each type of terrorist attack, but also in assessing the probability that terrorists will be able to carry out an attack successfully.

As explained by Schanzer and Eyerman in their paper, this is one of the many complexities of risk assessment. In this case, while experts agree that a successful nuclear attack would be devastating, they do not agree that such an attack would be likely to happen. In 2005, some national security experts estimated that the risk of a WMD attack in the next decade to be as high as 70 percent.[44] This estimate rests mainly on reports stressing the lack of security around stockpiles of fissile materials scattered around the world and allegations of Al Qaeda's interest in acquiring fully developed nuclear capabilities.[45]

Table 5: Estimated Cost of Three Terrorist Attack Scenarios on New York City

Scenario	Estimated Costs
Scenario One: One-kiloton nuclear bomb in NYC	$1.1 trillion
Scenario Two: Dirty bomb in NYC	$95 billion
Scenario Three: Non-nuclear attack on NYC port ceasing operation for a month	$10 billion

Note: *These estimates are low but correct as to order of magnitude.*

More recently, a report on preventing WMD proliferation and terrorism stated, "Without greater urgency and decisive action by the world community, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013."[46]

On the other side of the debate, experts, like Ohio State University political science professor John Mueller, make the case that there is an "almost vanishingly small likelihood that terrorists would ever be able to acquire and detonate a nuclear weapon."[47] This argument, a popular one in the academic community, rests on the following facts:

- First, it would be extremely difficult to build such a weapon or use one that has been stolen
- Second, nations would almost certainly not give a nuclear weapon to a nonstate group
- Third, most terrorist organizations have no interest in seeking out the bomb

In April 2008 in testimony before the Senate Committee on Homeland Security and Governmental Affairs, Matthew Bunn, of the Carnegie Endowment for International Peace, summed up the issue. "Taking the good news with the bad [about the ability of terrorists to carry a successful nuclear attack], what are the chances of a terrorist nuclear attack? The short answer is that nobody knows." [48] However, he concludes, "even a 1% chance over the next ten years would be enough to justify substantial action to reduce the risk, given the scale of the consequences."[49]

In other words, even if the probability of a terrorist attack with an actual nuclear weapon is lower than the probability of virtually any other type of terrorist attack, the devastation from a nuclear attack relative to other type of attacks would be quite overwhelming leading to an argument that the United States should probably consider this threat one of the greatest dangers it faces.

Analyzing Key Questions in Risk Analysis

After having identified what port related threats exist and their potential costs, this section looks into the best way to address these threats. It means asking two key questions for each threat:

- How should ports be protected?
- Which ports should be protected?

Developing Key Questions

How should ports be protected?

Protection against a direct attack. In ports, as with all stationary targets, the attacker has a natural advantage: He gets to choose where to attack. Terrorists will attack wherever the defenses are weakest. Because of the attacker's advantage of being able to choose the time and place of attack, intelligence gathering and counter-intelligence are often the most cost-effective and best defenses.

The defender's most cost-effective solution is thwarting the attackers before they launch the attack or deploying personnel and equipment exactly where the attack will occur.

The defender's second most cost-effective solution in the face of an attack is to mitigate an attack's damage. Even if the defender doesn't know where or how an attack will occur, the defender can lower the expected damage by developing plans for the aftermath of an attack. For a port, such plans might include evacuating civilians and personnel, placing emergency equipment within easy reach, training personnel to handle emergencies and attacks, and developing business continuity strategies that would allow the port to get up and running quickly after an attack.

The defender's third most cost-effective solution against direct attack is direct prevention. The defender would employ measures such as physical barriers (e.g., fences), surveillance equipment (e.g., closed-circuit television), and access control systems for employees and visitors. However, such direct defenses are only as good as their weakest link. As a result, this solution tends *not* to be cost effective: one has to protect *everything* from *every* possible mode of attack. This gets expensive and is often counter-productive.

So, as with almost all counter-terrorism, an argument can be made to first devote greater focus on intelligence. Second, greater focus could then be given to damage mitigation. Direct prevention should then be only the last resort given this analysis.

Protection against smuggling of WMD. The secrets of nuclear weapon design were revealed long ago. Today, the only significant barrier to building a weapon of mass destruction remains access to fissile (highly enriched uranium and plutonium) and radiological materials. Terrorists have two options. They could either acquire a complete, ready-to-use weapon, or they could acquire the materials and components to build the weapon themselves. While the first scenario cannot be ruled out, the second scenario is more likely.

According to Captain Joseph Bouchard, a retired Navy officer and an expert on nuclear devices, nuclear and radioactive material is considerably more difficult to acquire in the United States than overseas. [50] The rest of the materials required to assemble a bomb, however, could be acquired in the United States. Thus, the most likely scenario is that terrorists would get fissile materials abroad,

smuggle them into the United States and then assemble the bomb here.

According to Stanford University's Lawrence M. Wein, there are 132 of paths that terrorists could use to transport a foreign-built weapon to an American target city once we take under consideration all four likely modes of transportation: commercial planes, cargo airplanes, container ship, and cruise ship. [51] This number increases once we add transportation of a weapon with a vehicle along the thousands of miles of unprotected borders.

Focusing on ports alone, Wein explains that there are 12 paths that terrorists can use to get nuclear material from a foreign nation to an American port. He writes, "Whether by sea or air, the trip could either be direct to the United States or routed through a port in Canada or Central or South America." [52]

In theory, terrorists can be expected to choose the path that gives them the best chance to succeed in bringing it inside the United States. It means that we should maintain an equal protection along each of these paths because if we harden one path, they will just choose an easier one. The cost of this exercise could be spectacularly high.

As we know, law enforcement agencies face an enormous challenge in protecting the country's borders—not just ports—from smuggled goods, whether those goods are drugs, illegal immigrants, stolen goods, or dangerous materials like uranium.[53] Even the fact that they are carrying highly radioactive material does little to enhance their chances of being caught. Experts testified before Congress in July 2005 that terrorists could easily shield highly enriched uranium and avoid detection from radiation detectors.[54]

Considering these factors, the most cost-effective solution to preventing nuclear smuggling might not be to protect every path equally or to engage is detection. The best defense may not come from allocating resources equally across the system.

What is the best defense? For each path (132 of them or 12 port related ones), terrorists first have to acquire the material, and second, they have to transfer it to a foreign port. These two steps represent excellent security bottlenecks.

Hence, we can deduct that by making sure that terrorists do not acquire the materials necessary to build a bomb is the most cost-effective solution in the fight against nuclear smuggling. The most cost-effective way to do this is to keep close tabs on fissile materials. It is easier to monitor a lump of uranium at a known location than to detect it when it is smuggled across a border. In order to keep fissile materials out of terrorists' hands and protect her citizens, the United States might buy foreign stockpiles or help foreign governments protect or destroy their stockpiles.

If terrorists were to acquire dangerous material, our second most cost-effective solution would be to put in place security mechanisms to prevent nuclear devices from arriving in the United States. For instance, the federal government should help officials abroad tighten security at the foreign ports that feed shipments to the United States, by helping to fund systems that bolster foreign countries' abilities to detect nuclear material in their ports or placing U.S. agents on site in foreign ports. A related cost effective strategy of preventing dangerous material from entering U.S. ports would be to create partnerships with foreign manufacturers and importers. Partners would agree to meet "supply chain" standards establishing a secure chain of custody for every unit of cargo traded overseas. This would ensure that their shipment methods repel potential terrorist attempts to use those shipments for introducing weapons of mass destruction into our ports. These partnerships would reduce the need of screening every cargo equally.

Finally, another cost-effective solution is onsite detection at US seaports. This is the least cost effective measure. As explained earlier, for this solution to be truly effective all ports and other points on entry into the US should be equally protected. This would be extremely hard to achieve even if we were to pour massive resources into it. Second, it is hard to detect highly enriched uranium especially if it is shielded. As such, the effectiveness of the detection devices is in doubt. However, even if the detection devices were capable of detecting dangerous material, it would still be riskier than the three other solutions because the stakes are so high: If the system fails, the illicit material ends up inside the country.

Which ports should be protected?

Protection against a direct attack. The objective of counterterrorism is to prevent if possible or minimize expected damage. Expected damage equals the probability of attack times the damage if attacked. Because terrorists usually focus on targets with the greatest potential for damage, the ports facing the greatest probability of attack and the ports where attacks would cause the most damage are one and the same—the megaports, where an attack would stop a significant amount of trade and have a considerable economic impact. Moreover, due to a larger workforce and higher passenger traffic, the death toll at a megaport would likely be higher than at a smaller port. Thus, if the government were to think strategically about port protection, it would allocate the bulk of the counterterrorism money and measures to the big ports, because the consequences and probability of an attack occurring there are significantly larger.

Protection against smuggling of WMD. Unlike direct threats to ports, where larger ports present more attractive targets for terrorists, when it comes to transporting WMD material through a port, terrorists are agnostic: They will exploit whichever port has the most porous security. Spending to thwart admission of WMD materials should therefore seek to make all ports equally secure. Roughly speaking, this will mean that each port's counter-WMD spending should be roughly proportional to its volume. For example, if gamma-ray detectors are used in one port, then they should be used in all ports. Providing these detectors would cost the same per ton of cargo in all ports, so a port with twice the cargo volume would require twice the number of detectors and twice the budget for counter-WMD expenditures.

Bringing Strategic Risk Management and Threat Analysis Together

Figure 1 summarizes our assessment of the two major threats facing port security and actions that can be taken against these threats.

Strategic risk management to port security identifies three security actions to protect against the smuggling of WMDs into the United States, including an analysis of resources currently devoted to each action:

Action One: Stop terrorists from acquiring the fissile material necessary to build a bomb. After all, no fissile material, no bomb. By keeping close tabs on fissile materials around the world, buying foreign stockpiles, and helping foreign governments protect or destroy their stockpiles, the United States would dramatically decrease the risk of nuclear attack and increase the security of its citizens.

> **Current resources:** Most of DOD's and DOE's nuclear threat reduction programs seek to control stockpile of fissile material—a total of $1.3 billion. Of this amount, roughly $650 million goes to the protection of fissile material stockpiles abroad. This funding doesn't include the DOE's Megaports Initiative or the Pentagon's parallel initiative.[56]

Action Two: Recover nuclear material and devices that fall into terrorists' hands. In cooperation with

Who Should Do the Protection?

Economic theory suggests that it is efficient to have the federal government provide public goods and private markets provide non-public goods. [55] A public good means that one person's consumption of the good does not prevent another from consuming the same good. Public goods are also non-excludable: It is hard or impossible to prevent anybody from getting access to and enjoying the public good once it is produced.

Typically, the provision of protection through intelligence is a public good. The intelligence gained could apply to any port, and it would not be cost effective for each port operator to try to infiltrate terrorist networks to discern whether their ports were to be attacked. Given this public-good nature of intelligence, the federal government should fund such activities.

Like intelligence gathering, preventing a nuclear or radiological bomb from going off in the United States is a public good. Espionage, intelligence, and nuclear threat reduction benefit all of the states, so the federal government should make these investments.

But protective measures such as direct prevention via physical barriers, direct surveillance, and access control are not public goods: It costs just as much—if not less—for the port to provide these measures as it would the government. Moreover, in the case of a non-public good such as this, local or private decisionmakers are in a better position to determine local needs and the most effective way to meet them. As a result, spending on direct prevention measures should be local, paid for through taxes and fees charged by the port in question.

Figure 1: Chart of Cost Effective Port Security Spending

	Protection Against Direct Attacks on Ports	Protection Against Smuggling of WMD into the United States
Actions the Federal Government Can Take	1. Intelligence to thwart attacks before they are launched	1. Stop terrorists from acquiring fissile material (i.e., stockpiles protection) to build a bomb
		2. Recover nuclear material and devices that fall into terrorists' hands
		3. Direct detection and protection in ports
Actions State and Local Governments Can Take	1. Mitigate damage after an attack (i.e., emergency equipment, business continuity practice)	N/A
	2. Upgrade security in ports (physical and operational)	

other countries, the United States engage in an international effort to tighten security at foreign ports. For instance, it could help fund systems that bolster nuclear detection abilities in foreign ports and/or place U.S. agents on site in those ports. Partnerships between DHS and foreign manufacturers and importers to ensure that their shipments are protected against infiltration are probably also a good idea and would reduce the need for screening every cargo shipment.

> **Current resources:** In this category, DHS's programs are directed at stopping terrorists from loading a nuclear device in a cargo container in a foreign port. That includes CSI, CTPAC, DoE Megaport Initiative, ACE, and a portion of the Coast Guards' PWCS program: $1.9 billion.

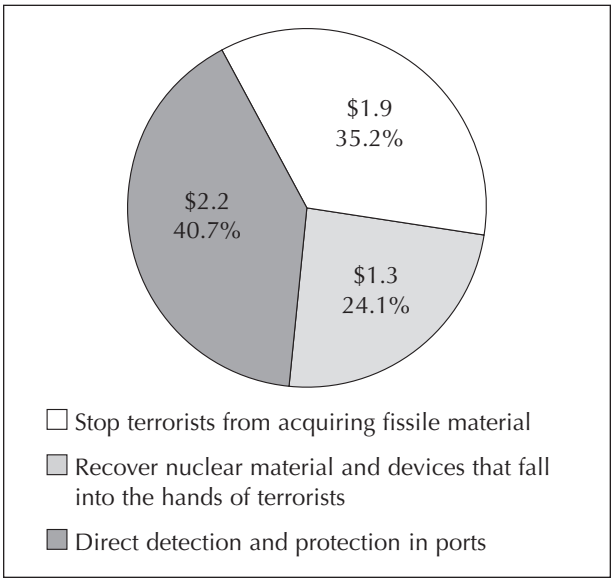
Action Three: Direct detection and protection in ports. This requires the acquisition of detection devices, jersey barriers, and video surveillance cameras. It would also involve mitigation and continuity plans in case of a successful terrorists attackson a port.

> **Current resources:** Programs like the Port Security Grant Program, most of the Coast Guard's Seaport, Waterways and Coastal Security program, the Domestic Nuclear Detection Office, and detection devices installed in domestic ports: $2.2 billion.

Strategic risk management helps weigh each of these actions. For instance, based on the dramatic consequences of a nuclear attack in the US and because Action One would have the highest probability of success, Action One should weigh more than Actions Two or Three. Also, Action Two should weigh more than Action Three. As mentioned earlier, direct detection in ports are only as good as their weakest links and must protect *everything* from *every* possible mode of attack, which makes the least cost effective measure.

Figure 2 shows the allocation of port threats-related appropriations for FY2009.

Figure 2: Port Threats-Related Appropriation for FY2009 and Percentage ($Billions)



Source: *Budget of the United States, FY2009, Department of Homeland Security, Budget in Brief FY2009, A Unified Security Budget for the United States FY2009.*

Note: *While these numbers are estimates and have left out some small programs, the order of magnitude is correct.*

Using Strategic Risk Management to Prepare Resources Allocation Options

Strategic risk management can help inform homeland security resource allocation in regard to port security. Based on the analysis presented in this paper, three options, each of which commands a certain resource allocation, have been identified.

Developing Resource Options

Option One: Increase Allocation to Stop Terrorists from Acquiring Fissile Material

Based on our risk analysis, we found that Action One (stop terrorists from acquiring fissile material) would have the highest probability of success. Hence, this option would direct more resources where there would be the most cost effective.

The first step would consist in increasing resources to stopping terrorists from acquiring fissile material. Figure 2 shows that in FY2009 roughly $1.3 billion will be allocated to nuclear threat reduction programs.[57] It represents nearly 25 percent of the total funding the federal government allocated to port-related threats. The actual protection of global fissile material gets an even smaller share of that funding—$650 million—and those funds only address a fraction of the fissile material in the world. The total funding going to nuclear threat reduction is slightly lower than what DHS spent to secure cargos in foreign ports and much less than what the United States spends on detection in domestic ports.

Today, most of the current fissile material security costs outside the United States are borne by the nations holding those stocks. Whether we can be confident that all nations have the resources, the incentives, and the political will to carry out adequate security on an ongoing basis is a real concern. If they do not, these countries will under-invest in stockpile protection, which will in turn increase the probability that terrorists could acquire dangerous materials.

In 2004, the bipartisan 9/11 Commission reported that it was deeply worried about the U.S. government's commitment and approach to securing the weapons and fissile materials scattered around the world.[58] The commission members reported that the Cooperative Threat Reduction Program in particular was then in dire need of serious expansion, improvement, and resources.[59] In October 2008, former Commission members, regrouped in the Partnership for a Secure America, released a "WMD Terrorism Report Card." It gave the federal government an overall grade of a "C."[60] According to the report card, nonproliferation programs are still limited primarily by lack of interagency coordination, a long-term strategy, and a mismatch of U.S. and foreign expectations.

This is particularly true for non-proliferation programs that minimize the risk of nuclear terrorism by securing vulnerable material at the source. While there can be no doubt that America and the world face a far lower risk of nuclear terrorism today than they would have had these efforts never begun in the 1990s, the $650 million allocated in FY2009, out of a $1.7 billion budget, still falls short of what is really needed to successfully protect stockpiles.[61]

According to Laura Holgate of the *Nuclear Threat Initiative*, there is no good estimate for the total cost of sustainable security for global fissile material stockpiles. However, current spending is nowhere near what would be needed to achieve that task. Mathieu Bunn estimates that $1.5 billion a year—not $650 million—would be necessary to protect all

the stockpiles of fissile material.[62] And the current allocation certainly falls short to the $3 billion a year recommended by Lloyd Cutler and Howard Baker, co-chairs of the Russia Task Force, in their report card on non-proliferation programs back in January 2001.[63]

The urgency of securing stockpiles material around the world has been highlighted numerous times. Without fissile materials, terrorists cannot build nuclear or dirty bombs. However, once they have put their hands on such material, each of the later lines of defense is more desperate and more doubtful. As Bunn, Wire, and Holdren point out, "[I]f defenses against nuclear weapons at the U.S. border or within the United States are ever called into play, this will represent a serious failure of U.S. policy, in failing to intercept the threat earlier in the terrorist pathway to the bomb."[64] Even though DHS is not involved in that effort directly, the department should be highly interested in the success and efficiency of the nuclear threat reduction programs abroad. Their failure exposes the country to great risks and puts more pressure on the other lines of defense put in place by DHS, such as CSI, CTPAC, and direct detection in ports.

Finally, and more importantly, properly securing stockpiles of fissile materials would alleviate much of the pressure on all other lines of defense outside of ports (air, borders, and else). It also reduces the need to spend a lot of money on detection.

Option Two: Increase Allocation to Recover and Detect Nuclear Material

If terrorists ever do put their hands on dangerous material, the second line of defense would prevent them from bringing it anywhere near our ports. This is achieved by spotting suspicious anomalies while cargos are in foreign ports. Because foreign governments, especially those that are very unlikely terrorist targets, have almost no incentive to invest money to tighten security in their ports to protect U.S. ports, the federal government should provide most of the funding.

This second option would increase the level and depth of the investment spent on screening efforts in foreign ports. Currently, the federal government spends $714 million through CSI and C-TAPT, ACE programs, and by installing detection devices to secure cargo coming to the U.S. from foreign ports, in addition to the Coast Guard's budget allocated to recovery.

Under this scenario, DHS would expand its partnerships with foreign ports through CSI. It would also encourage public-private partnerships that adopt sustainable and effective security programs in foreign ports. According to the Unified Security Budget for the United States FY2009, DHS would need to double the current budget for CSI and C-TPAT. But, the report also recommends increasing the resources going to the Coast Guard. In previous years, it priced the additional Coast Guard's budget needed at $500 million. Together, these measures would cost roughly an additional $1 billion.

That being said, critics have charged that added funding for CSI and C-TPAT wouldn't achieve much. In the case of CSI, in large part, the program's targeting is based on the description of contents provided by suppliers. A very small percentage of containers passing through CSI ports ever gets scanned, and even fewer are even opened for inspection. Experts, like Stephen Flynn, for instance, have argued that these programs wouldn't achieve increased security unless foreign ports started screening 100 percent of the containers.

The members of the Hong Kong Container Terminal Operators, a private organization, have put such a system in place in the past few years. Their goal is to enhance container-screening security while at the same time minimizing the effect of the cargo inspection regime on the efficiency of operation and the flow of cargo. Thus far, the system has proven quite successful in not only screening all U.S.-bound cargo loaded in Hong Kong while minimizing the delays when shipments required more thorough inspections, but also doing background checks on the shipping companies that raised a red flag for terrorism risk. The Hong Kong Container Terminal Operators have offered to work with DHS to improve and implement this same system around the world.

Stephen Flynn estimates that deploying a screening system that would run every container through both radiation and gamma-ray density sensors (which would detect shielding efforts on the part of terrorists) and then take a picture of the container's identi-

fication numbers to match against databases for additional screening at every port in the world would cost roughly $1.5 billion.[65]

Advocates of this measure claim that it might not cost that much to the U.S. government. For instance, if destination port operators could offer reduced fees to cargo originating in 100% screening ports of origin or alternatively impose fees for failing to implement a 100% screening regimen, foreign port operators and shippers would soon see a commercial benefit in getting with the program.[66]

It is, however, unlikely that every single foreign government would agree to sustain such a cost without some help from the US government. As we have mentioned earlier, unless every port does it, terrorists will likely decide to go to the weakest link, which means that very little additional security will have been added to the system. In other words, the U.S. government would probably have to foot most of the bill.

Option Three: Increase Allocation to Detection and Protection at United States Seaports

This option would increase dramatically the level of spending dedicated to enhancing security in U.S. seaports. Again, based of the security concept that one's security system is only as strong as its weakest link, we know that for this option to be efficient it should maintain an equal level of protection and detection in each port.

If the goal is to enhance security in our ports, critics have argued that $388 million in PSGP is inadequate. They also argued that the U.S. port infrastructure is so vast that spreading $388 million across the entire nation will not achieve meaningful security either. According to an estimate by the Coast Guard, the cost for enhancing security at America's 361 maritime facilities would be $1.5 billion in the first year, plus an additional $7.3 billion over the next decade.[67]

Criticism of the Port Security Grant Program has come from within the Department of Homeland Security. In January 2005, the DHS Inspector General (IG) questioned the merits of hundreds of projects funded with these grants, based on the review of four rounds of grants. [68] The grant system is meant to be a competitive grant allocation program. In theory, grants are given out based on the merits and the expected security returns of applications submitted by individual ports. However, the IG reports that "[t]he program funded projects despite dubious scores by its evaluators against key criteria, raising questions about the merits of several hundred projects."[69] Given the limited budget available, the funding of such low-priority projects necessarily means that many projects were not funded despite strong support from the field review.

In February 2006, a second review of the grant programs concluded that while some improvements were made to the allocation process, problems remained which raised doubts about the ability of the program to achieve any meaningful security.[70] For instance, the report finds that while the evaluation and selection process was improved, it didn't eliminate funding going to projects such as $326,000 awarded to a port to install some crash-proof barriers at secondary gates that the DHS's field reviewers said "would have no impact on the national priority threat." The IG reports on the Port Security Grant Program underline that the department has little assurance that the program is protecting the nation's most critical and vulnerable port infrastructure and assets. This means that serious reforms of this program may be needed.

As discussed in this paper, the protection of ports or detection in ports are a much less effective means of defending the United States from terrorist attack than securing vulnerable material at the source or investing resources to recover dangerous stolen material. This would be true even if cutting-edge detection technologies were used such as direct detection on site in local ports.[71]

Buying many more radiation portal monitors might, however, not be enough to secure the country against WMD attacks. For one thing, the detection devices have so far proven unreliable. The monitors cannot reliably detect highly-enriched uranium, the crucial element in a nuclear bomb.[72] Terrorists could easily shield the uranium and avoid detection. According to experts, another limitation of the monitoring system is that it lacks the capability to rapidly determine the type of radioactive materials it detects, which leads to higher "nuisance alarm" rates—the number of alarms that must be resolved by further inspection.[73]

To address the situation, a program in the Homeland Security Department's Domestic Nuclear Detection Office calls for the investment of hundreds of millions of dollars to upgrade the country's nuclear detection devices. The development and testing of the monitors has been a continuing source of friction between Congress and the administration over the past couple years. Many experts agree that searching for a technological savior to deliver us from the threat of nuclear terrorism might not be the best use of our resources. [74]

While additional resources can be allocated inside U.S. ports, it may be risky to rely so much on port security at home: If the system fails just once, the illicit material ends up inside the country, making it almost impossible to prevent the worst. If a nuclear bomb blows up at the Port of New York, it would kill some of the New York City's 8 million residents.

With the existence of several practical alternatives to smuggling nuclear material through ports—including smuggling through thousands of unprotected miles of borders—domestic detection in ports will remain difficult.

Conclusion

Table 6 simulates a possible resource allocation for each option. While the numbers are a rough estimate of what each option would cost, it gives us a good idea of the weight that could be assigned to each security action identified through our risk analysis.

As a society, international terrorism is probably the greatest challenge we face today. It is a difficult topic because it is emotionally charged and has so many terrible frightening aspects. This is why the strategic risk management process and its different steps can help make better homeland security decisions that will lead to better spending allocations and enhanced security.

Strategic risk management is a process. It requires taking a series of steps. The first step consists in defining which assets we are trying to protect. In the case of this paper, the assets in question are ports.

We can then identify how much resources are currently devoted to the protection of this particular asset. For this step we can make a list of all the actions taken by the government to protect ports and the agencies responsible for the protection.

The third step consists in identifying the risks to these assets. In the case of ports, we identified two main risks:

- A direct attack on a domestic seaport
- The smuggling of a weapon of mass destruction through a United States seaport

Table 6: Possible Resource Allocation Based on Risk Analysis ($Billions)

Response to Threats	Current Allocation (FY 2009)	Option One: Increase Allocation to Stop Terrorists From Acquiring Fissile Material	Option Two: Increase Allocation to Recover and Detect Nuclear Material	Option Three: Increase Allocation to Detection and Protection at United States Seaports
Action One: Stop terrorists from acquiring fissile material	$1.3 (24%)	$4.3 (54%)	$1.3 (16%)	$1.3 (19%)
Action Two: Recover nuclear material and devices that fall into the hands of terrorists	$1.9 (35%)	$1.9 (24%)	$4.4 (56%)	$1.9 (27%)
Action Three: Direct detection and protection in ports	$2.2 (41%)	$1.8 (22%)	$2.2 (28%)	$3.7 (54%)
Total	$5.4 (100%)	$8.0 (100%)	$7.9 (100%)	$6.9 (100%)

Note: *These numbers are estimate. They are meant to show how differently each option weight the security action identified through our risk analysis.*

The final step consists in assessing the probability and the consequences of a successful terrorist attack as they relate to the asset we are trying to protect. Identifying scenarios and assessing their costs helps in that process. In the case of port security, we have concluded that even though the probability of a nuclear attack is extremely small, its dramatic consequences commands that we make this risk a priority.

The following step in our risk analysis case example identifies security solutions to mitigate the risk. It also asks how well each solution mitigates those risks and at what costs. Based on our risk analysis of port security we identified three security actions. They were the following:

- **Action One:** Stop terrorists from acquiring fissile material.
- **Action Two:** Recover nuclear material and devices that fall into the hands of terrorists.
- **Action Three:** Direct detection and protection in ports.

We found that Action One has the highest probability of success, hence it should probably weigh more than Action Two or Three. Also, Action Two should weigh more than Action Three since direct detection in ports are only as good as their weakest links and must protect *everything* from *every* possible mode of attack, which makes the least cost effective measure.

The last step consists in using our risk analysis to inform the resource allocation. Based on our analysis we identified three options that weigh each security action differently and achieve different security levels.

We find that many of the security measures proposed have enormous tradeoffs, meaning that they have large monetary costs without increasing security much. In fact, risk analysis is rarely about the value or cost of each security measure. Rather, it is about the tradeoffs that each measure requires.

Finally, strategic risk management attempts to ask the important question, "Is a particular security measure worth it?" The answer of course depends on the details of the measure itself and on the context of its implementation. It means that there is not predetermined and standard response to each security scenario. However, it also makes the process of strategic risk management even more important as government strives to achieve the highest level of security at the lowest cost.

Endnotes

1. Author's calculation based on *Department of Homeland Security, Budget in Brief FY2010 (http://www.iaem.com/committees/GovernmentAffairs/documents/DHSBudgetinBriefFY2010.pdf)* and Office of Management and Budget, "Securing the homeland, Strengthening the Nation" http://www.whitehouse.gov/homeland/homeland_security_book.pdf

2. General Accounting Office, "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts," GAO-02-208T, October 31, 2001, p. 2. Also see "Combating Terrorism: Selected Challenges and Related Recommendations," GAO-01-822 September 20, 2001.

3. John Frittelli, "Maritime Security: Overview of Issues," Congressional Research Service, RS21079, February 24, 2003. http://www.boozman.house.gov/UploadedFiles/TRANS%20-%20Maritime%20Security%20Overview%20of%20Issues.pdf

4. US Army Corps of Engineers' Navigation Data Center ranks U.S. ports by dollar value and tons of cargo imported and exported. See http://www.iwr.usace.army.mil/ndc.

5. John Frittelli (2003), "Maritime Security: Overview of Issues," Congressional Research Service, RS21079, February 24. Ibid.

6. Ibid.

7. John Frittelli, "Maritime Security: Overview of Issues," February 24, 2003.

8. John Frittelli, "Maritime Security: Overview of Issues," February 24, 2003.

9. U.S. Department of the Treasury. "US Customs Commissioner Robert Bonner, Speech Before the Center for Strategic and International Studies," Washington DC January 17 2002 and Stephen Flynn, America the Vulnerable: How our Government is Failing to Protect us From Terrorism (New York: Harper Collins, 2004), p. 83.

10. JayEtta Z. Hecker (2002), "PORT SECURITY: Nation Faces Formidable Challenges in Making New Initiatives Successful," Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations House Committee on Government Reform, GAO Report GAO-02-993T, August 5.

11. The federal government has identified thirteen critical sectors that the country needs to protect from terrorism: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal and shipping. Each sector is then broken into sub-sectors. For instance, transportation is separated into aviation, train, freight, etc.

12. Ronald O'Rourke (2005), "Homeland Security: Coast Guard Operations—Background and Issues for Congress," CRS Report for Congress, RS21125, June 30, 2005.

13. The Institute for Policy Studies (2008), "A United Security Budget for the United States, FY2009," p 31.

14. Ibid, p. 31.

15. The Institute for Policy Studies (2008), "A United Security Budget for the United States, FY2009," p 32.

16. Department of Homeland Security (2005), Fact Sheet: Domestic Nuclear Detection Office, April 20. http://www.dhs.gov/dhspublic/display?theme=43&content=4474&print=true

17. Department of Homeland Security, Budget in Brief FY2009, p. 109. http://www.dhs.gov/interweb/assetlibrary/Budget_BIB-FY2006.pdf

18. See http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/csi_in_brief.xml

19. Department of Homeland Security (2008), FY2009 Explanation of Changes, general provisions, p. 27, http://www.dhs.gov/xlibrary/assets/budget_fy2009.pdf.

20. Ibid, p. 27.

21. GAO report Complete

22. DHS, Budget in Brief FY2009.

23. Department of Energy, Nuclear Security Administration, FY2009 Budget request.

24. Department of Homeland Security, Budget in Brief, FY2009, p. 58.

25. Department of Homeland Security, Budget in Brief FY2004, p. 9. See also Department of Homeland Security, Press Release, "Department of Homeland Security Announces $49 Million in Grants to Secure America's Ports," September 13, 2004.

26. The Transit Grant Program for ferry security received an additional $5 million a year on average since FY2005 on top of the PSGP.

27. Council on Foreign relations, "Terrorism: Questions & Answers, Responding to Nuclear Attacks,", http://cfr-terrorism.org/security/nuclear.html

28. See Area and Population Density from 2000 County and City Data Book.

29. Aldy, Joseph E. and W. Kip Viscusi (2003). "Age Variations in Workers' Value of Statistical Life," NBER Working Paper No. 10199.

30. William C. Thompson Jr. (2002), "One Year Later: The Fiscal Impact of 9/11 on New York City," Office of NYC Comptroller, September 4. http://www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf

31. Peter D. Zimmerman and Cheryl Loeb (2004), "Dirty Bomb: The Threat Revisited," Defense Horizons, The Center For Technology And National Security Policy At National Defense University, Number 38, January. http://hps.org/documents/RDD_report.pdf

32. Matthew Bunn, Anthony Wier, and John P. Holdren (2003), "Controlling Warheads and Materials: A Report Card and Action Plan," The Nuclear Threat Initiative, March 2003, http://www.nti.org/e_research/cnwm/cnwm.pdf

33. William C. Thompson Jr. (2002), "One Year Later: The Fiscal Impact of 9/11 on New York City," Office of NYC Comptroller, September 4. http://www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf

34. Matthew Bunn, Anthony Wier, and John P. Holdren (2003), "Controlling Warheads and Materials: A Report Card and Action Plan," The Nuclear Threat Initiative, March 2003, p. 18.

35. National Terror Alert (2004), "CIA Warns Dirty Bomb within Al Qaeda's Capabilities," November 25.

36. Federation of American Scientists Public Interest report (2002), "Dirty Bomb: Response to a Threat," Journal of the Federation of American Scientists, Volume 55, Number 2, March/April.

37. Peter D. Zimmerman and Cheryl Loeb (2004), "Dirty Bomb: The Threat Revisited," Defense Horizons, the Center for Technology And National Security Policy At National Defense University, Number 38, January. http://hps.org/documents/RDD_report.pdf.

38. William C. Thompson Jr. (2002), "One Year Later: The Fiscal Impact of 9/11 on New York City," Office of NYC Comptroller, September 4. http://www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf

39. Stephen Flynn (2004), Stephen Flynn, The Limitations of the Current Cargo Container Targeting, *Written Testimony before the Subcommittee .on Oversight and Investigations of the House Comm. on Energy and Commerce*, 108th Cong., Mar. 31. http://www.cfr.org/pub6907/stephen_e_flynn/the_limitations_of_the_current_cargo_ container_targeting.php.,

40. American Association of Port Authorities, "United States Waterborne Foreign Commerce 2003," http://www.aapa-ports.org/industryinfo/statistics.htm.

41. Ibid.

42. Ibid.

43. The cost of an attack on NYC port is based on the daily cost of $277 million to shutdown of the megaport of New York/New Jersey.

44. Jim Morris (2005), "Don't Worry be Happy: Polls Show Experts More Worried About New Attacks, Americans Less," Congressional Quarterly, June 22.

45. See for instance, Matt Bunn (2008), "The Risk of Nuclear Terrorism – And Next Steps to Reduce the Danger testimony before the committee on homeland security and governmental affairs United States senate, April 2nd. http://belfercenter.ksg.harvard.edu/files/bunn-nuclear-terror-risk-test-08.pdf. But also account by the CIA that Al Qeada has been trying to acquire fissile material, CIA (2003), "Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass destruction and Advanced Conventional Munitions," Attachment A, January. http://www.cia.gov/cia/reports/721_reports/jan_jun2003.htm

46. Bob Graham and Jim Talent and al. (2008), The World at risk, First Vintage Book, December. http://documents.scribd.com/docs/2avb51ejt0uadzxm2wpt.pdf

47. Chris Schneidmiller (2009), "Experts Debate Threat of Nuclear, Biological Terrorism," Global Security Newswire, January 13.

48. Matt Bunn (2008), "The Risk Of Nuclear Terrorism – And Next Steps To Reduce The Danger" Testimony before the Committee on Homeland Security and Governmental Affairs, United States Senate, April 2. http://belfercenter.ksg.harvard.edu/files/bunn-nuclear-terror-risk-test-08.pdf. 8.

49. Ibid, p. 8.

50. Joseph F. Bouchard (2005), "Defense in Depth Against Improvised Nuclear Device or radiological Dispersal Device," Zel Tech Technology presentation, April 26.

51. Lawrence M. Wein (2009), "A Threat In Every Port," The New York Times, Monday June 15, http://www.nytimes.com/2009/06/15/opinion/15wein.html?pagewanted=1

52. Lawrence M. Wein (2009), "A Threat In Every Port," *The New York Times,* Monday June 15, http://www.nytimes.com/2009/06/15/opinion/15wein.html?pagewanted=1

53. According to the U.S. Customs Service, each year 60 million people enter the United States on more than 675,000 commercial and private flights. Another 6 million come by sea and 370 million by land. In addition, 116 million vehicles cross the land borders with Canada and Mexico. More than 90,000 merchant and passenger ships dock at U.S. ports. These ships carry more than 9 million shipping containers and 400 million tons of cargo. Another 157,000 smaller vessels visit our many coastal towns. Amid this voluminous trade, the probability of stopping terrorists from smuggling something into the country is very low.

Drug smuggling illustrates how easy it is to smuggle goods into the United States. According to Barry R. McCaffrey, the former director of the Office of National Drug Control Policy, virtually all of the cocaine and heroin and a majority of the marijuana sold and consumed in this country is produced abroad and then smuggled into the country. In 2000, the total amount of cocaine and heroin consumed in the United States was 259 metric tons, roughly equivalent to 300 pickup trucks full of drugs. Contrast that number with the fact that in 2002 the Drug Enforcement Administration seized 59.1 metric tons of cocaine and heroin. The amount of successfully smuggled drugs dwarfs the amount of captured drugs. Clearly, determined smugglers have no difficulties permeating the U.S.'s porous borders.

Based on these numbers, determined smugglers with a nuclear device would have little trouble circumventing the nation's border protection and control, particularly because they would be able to leverage the techniques used successfully by drug smugglers.

54. See Congressional Quarterly. Congressional Transcripts, Congressional Hearings, June 21, 2005, House Homeland Security Subcommittee On Emergency Preparedness, Science And Technology Holds Hearing On Effectiveness Of Nuclear Weapons Detection Technology.

55. See for example Gold (1999) for a good review of the literature and a discussion of defense as a public good.

56. DoE's Megaport initiative installs radiation detectors to screen cargo containers at the largest foreign ports

57. This number is made of nonproliferation and nuclear threat reduction spending ($1.9 billion) minus $550 million for programs that undermine or complicate nuclear non proliferation efforts, minus the funds allocated the Megaport Initiative and the Pentagon's deployment of radiation portal monitors in foreign ports, $200 million.

58. The 9/11 Commission report, "Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, p.381.

59. The 9/11 Commission report, "Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, p.381.

60. Partnership for Secure America (2008), "WMD Report Card," September. http://www.psaonline.org/downloads/ReportCard%208-25-08.pdf

61. Matthew Bunn (2008), "Next Steps To Strengthen The National Nuclear Security Administration's Efforts To Prevent Nuclear Proliferation, Testimony before the Subcommittee On Energy And Water Appropriations United States Senate April 30, 2008. p. 2-3.

62. Mathieu Bunn (2000), "The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material," Carnegie Endowment for International Peace. http://www.ciaonet.org/wps/bum01

63. Lloyd Cutler and Howard Baker (2001), A Report Card on the Department of Energy's Non Proliferation Programs with Russia', 10 January. This figure is often used to stress the lack of appropriate resources spent on this effort. Yet we must remain somewhat caution with this figure. First it is a guess, with no analytical back-up. Second, it leaves out nuclear security issues outside of Russia.

64. Matthew Bunn, Anthony Wier, and John P. Holdren (2003), "Controlling Warheads and Materials: A Report Card and Action Plan," The Nuclear Threat Initiative, March 2003, p. 31.

65. Stephen Flynn (2006), "The Limitations of the Current U.S. Government Efforts to Secure the Global Supply Chain against Terrorists Smuggling a WMD and a Proposed Way Forward," Testimony Before the Senate Homeland Security Committee, March.

66. Robert W. Kelly (2007), "Containing the Threat: protecting the Global Supply Chain Through Enhanced Cargo Container Security," The Reform Institute, October. http://www.reforminstitute.org/uploads/publications/Container_Security_Final_10-02-07_(in_template).pdf

67. John Frittelli, "Maritime Security: Background and Issues for Congress," CRS Report for Congress, RL31733, May 27, 2005.

68. Richard Skinner, Office of Inspector General, Department of Homeland Security, "Review of the Port Security Grant Program," OIG-05-10, January 2005. http://www.dhs.gov/interweb/assetlibrary/OIG_05-10_Jan05.pdf

69. Ibid, p. 4.

70. Richard Skinner, Office of Inspector General, Department of Homeland Security, "Follow Up Review of the Port Security Grant Program," OIG-06-24, February 2006.

71. To make matters worse, the current radiation portal monitors used by DHS, the Pentagon and the Department of Energy have been highly criticized for their lack of effectiveness. See Vayl Oxford, "Detecting Nuclear Weapons and Radiological Materials: How Effective is Available Technology?" Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, June 21 2005.

72. See Congressional Quarterly. Congressional Transcripts, Congressional Hearings, June 21, 2005, House Homeland Security Subcommittee On Emergency Preparedness, Science And Technology Holds Hearing On Effectiveness Of Nuclear Weapons Detection Technology.

73. Vayl Oxford, "Detecting Nuclear Weapons and Radiological Materials: How Effective is Available Technology?" Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, June 21.

74. Thomas Cochran (2008), Before the Senate Homeland Security and Homeland Security Governmental Affairs Committee, September 25. See http://homeland.cq.com/hs/display.do?dockey=/cqonline/prod/data/docs/html/transcripts/congressional/110/congressionaltranscripts110-000002966079.html@committees&metapub=CQ-CONGTRANSCRIPTS#speakers

ABOUT THE AUTHOR

Veronique de Rugy is a senior research fellow at the Mercatus Center. Her research interests include the federal budget, homeland security, tax competition, and financial privacy issues.

Ms. de Rugy was previously a resident fellow at the American Enterprise Institute, a policy analyst at the Cato Institute, and a research fellow at the Atlas Economic Research Foundation. She also directed academic programs for the Institute for Humane Studies-Europe in France.

Ms. de Rugy has testified on Capitol Hill on several occasions, most recently before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, of the U.S. House of Representatives. De Rugy presented her research addressing the "midnight regulations" phenomenon and discussed effective ways to curb this endemic problem. She has also testified before the Federal Financial Management Subcommittee of the Senate Homeland Security, Government Affairs and International Security Committee about the inefficiencies of the 7(a) loan program at the Small Business Administration and whether the program is contributing to the growth and health of the nation's small business community.

Ms. de Rugy is the coauthor of *Action ou Taxation*, published in Switzerland. Her work has appeared in the *Wall Street Journal, The Los Angeles Times, Reason* magazine, and numerous other publications. She is a frequent guest on PJTV and Reason TV, and has appeared on CNN, ABC 20/20, MSNBC and Fox News. She is a contributor to The Corner at *National Review Online*.

She is currently on the board of directors of the Center for Freedom and Prosperity.

Ms. de Rugy earned an MA in economics from the University of Paris IX-Dauphine and a PhD in economics from the University of Paris-Sorbonne.

KEY CONTACT INFORMATION

To contact the author:

Veronique de Rugy
Senior Research Fellow
Mercatus Center
George Mason University
3301 North Fairfax Drive
Suite 450
Arlington, VA 22201
(703) 993-4934

e-mail: vderugy@gmu.edu

REPORTS from The IBM Center for The Business of Government

For a full listing of IBM Center publications, visit the Center's website at *www.businessofgovernment.org*.

Recent reports available on the website include:

Collaboration: Networks and Partnerships

*Designing and Managing Cross-Sector Collaboration: A Case Study in Reducing Traffic Congestion*s by John M. Bryson, Barbara C. Crosby, Melissa M. Stone, and Emily O. Saunoi-Sandgren

Integrating Service Delivery Across Levels of Government: Case Studies of Canada and Other Countries by Jeffrey Roy and John Langford

Contracting

The Challenge of Contracting for Large Complex Projects by Trevor L. Brown, Matthew Potoski, and David M. Van Slyke

Success Factors for Implementing Shared Services in Government by Timothy J. Burns and Kathryn G. Yeaton

E-Government/Technology

Creating Telemedicine-Based Medical Networks for Rural and Frontier Areas by Leonard R. Graziplene

The Role and Use of Wireless Technology in the Management and Monitoring of Chronic Diseases by Elie Geisler and Nilmini Wickramasinghe

Financial Management

Managing a $700 Billion Bailout: Lessons from the Home Owners' Loan Corporation and the Resolution Trust Corporation by Mark K. Cassell and Susan M. Hoffmann

Strengthening Government's Ability to Deal with the Financial Crisis by Thomas H. Stanton

Human Capital Management

Federated Human Resource Management in the Federal Government by James R. Thompson and Rob Seidner

Innovation

Transforming Government Through Collaborative Innovation by Satish Nambisan

Managing for Performance and Results

Moving Toward Outcome-Oriented Performance Measurement Systems by Kathe Callahan and Kathryn Kloby

Organizational Transformation

Launching a New Mission: Michael Griffin and NASA's Return to the Moon by W. Henry Lambright

Transforming Information Technology at the Department of Veterans Affairs by Jonathan Walters

Presidential Transition

Transformation of the Department of Defense's Business Systems by Jacques S. Gansler and William Lucyshyn

Performance Management Recommendations for the New Administration by Shelley H. Metzenbaum

Social Services

US and UK Routes to Employment: Strategies to Improve Integrated Service Delivery to People with Disabilities by Heike Boeltzig, Doria Pilling, Jaimie C. Timmons, and Robyn Johnson

About the IBM Center for The Business of Government

The IBM Center for The Business of Government connects public management research with practice. Since 1998, we have helped public sector executives improve the effectiveness of government with practical ideas and original thinking. We sponsor independent research by top minds in academe and the nonprofit sector, and we create opportunities for dialogue on a broad range of public management topics.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value. For more information visit www.ibm.com.

For additional information, contact:
Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
1301 K Street, NW
Fourth Floor, West Tower
Washington, DC 20005
(202) 515-4504, fax: (202) 515-4375

e-mail: businessofgovernment@us.ibm.com
website: www.businessofgovernment.org